Overview Report:
Literature on Money Laundering and Real Estate
& Response from Real Estate Industry

TABLE OF CONTENTS

1. INTRODUCTION

1. This overview report attempts to provide a summary of the academic literature and media reporting on the subject of money laundering in the real estate industry, and responses to those academic and media reports from the real estate industry, and from governments in BC.

2. This overview report is divided into two parts: 1) literature from entities studying money laundering in real estate; and 2) response to that literature from industry.

3. In the first part, the report will first set out domestic and international governmental reports on the state of money laundering in real estate, including from FATF, FINTRAC, and the EU. Second, this part sets out academic literature from various experts in Canada and internationally. Third, this part reviews media reporting in Canada, with a focus on reporting in BC, on the topic of money laundering and real estate. Fourth, this part sets out a brief overview of the findings reached by government-commissioned reports that form part of the Commission's Terms of Reference.

4. In the second part, the report first sets out perspectives expressed by industry advocacy groups, including the BC Real Estate Association ("BCREA") and the Canadian Mortgage Brokers Association – BC ("CMBA-BC"). Next, the report summarizes conversations Commission Counsel had with local real estate boards, followed by a review of measures the quasi-governmental regulatory body, the Real Estate Council of BC, has taken to respond to concerns of money laundering in the real estate industry.

5. This overview report takes no position on the truth of any of the perspectives advanced. Rather, the overview report seeks to provide insight into the state of the discourse between various actors in the real estate industry at the time the Commission began its work. Commission counsel are not relying on the assertions recounted in this overview report, nor in the reports cited in this overview report, to establish the truth of the assertions. Instead, where we intend to rely upon a particular assertion made in any of the reports cited in this report, Commission counsel will obtain and present additional evidence.

6. Commission counsel see this overview report as a useful general introduction to the topic of money laundering in real estate and expect that all participants would benefit from hearing about at the outset of the real estate hearings.

PART 1: THE LITERATURE

2. GOVERNMENTAL & INTERGOVERNMENTAL ASSESSMENTS

A. FATF

7. On June 29, 2007, the Financial Action Task Force ("FATF") released its report on Money Laundering & Terrorist Financing through the real estate sector (the 2007 FATF Report).[1] The report aggregated case studies and used those case studies to identify the following typologies of money laundering in real estate:[2]

a. Use of complex loans or credit finance.

b. Use of non-financial professionals.

c. Use of corporate vehicles.

d. Manipulation of the appraisal or valuation of a property.

e. Use of monetary instruments.

f. Use of mortgage schemes.

g. Use of investment schemes and financial institutions.

h. Use of properties to conceal money generated by illegal activities.

8. The 2007 FATF Report provides, within each typology, conclusions on particular methods, and provides case studies. For example, under "use of non-financial professionals" FATF noted the use of gatekeepers, such as real estate agents, concluding:

---

[1] **Appendix 1**, FATF, *Money Laundering and Terrorist Financing Through the Real Estate Sector*, FATF (June 29 2007), online: <https://www.fatf-gafi.org/documents/documents/moneylaunderingandterroristfinancingthroughtherealestatesector.html> ("FATF 2007"). For more on FATF, please refer to "Overview Reports: FATF Records" introduced into evidence as exhibit 4.

[2] *Ibid*, at 7.

9. Professionals working with the real-estate sector are therefore in a position to be key players in the detection of schemes that use the sector to conceal the true source, ownership, location or control of funds generated illegally, as well as the companies involved in such transactions.[3]

10. The 2007 FATF Report also discussed the use of lawyers, notaries and other professionals to structure transactions to obscure ownership and identity. Shell companies and transfer of funds between offshore vehicles featured in many of the typologies.[4] Secrecy was highlighted as an enabling feature in many typologies.[5]

11. One Canadian example involved the conviction of an individual who had provided false information on multiple mortgage applications, and used nominee purchasers (family members), in order to purchase five properties.[6] Both the individual and all nominees paid more toward the properties than could be supported by their income as declared to CRA. The individual was later convicted of drug trafficking as well as money laundering.[7]

12. FATF concluded that:

> The use of real estate to launder money seems to afford criminal organisations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and even obtaining tax advantages (such as rebates, subsidies, etc.). [8]

13. The 2007 FATF Report also presented approximately 45 red flags identified from cases and other information, stating that these indicators "may help in identifying suspicious activity that should be reported to competent national authorities according to AML/CFT legislation."[9] However, in providing these indicators, FATF noted that the presence of indicators does not mean the transaction is necessarily linked to money laundering, but rather: "It needs to be borne in mind that money laundering always aims to disguise itself as a "normal" transaction. The criminal nature of the activity derives from the origin of the funds and the aim of the participants."[10] The 2007 FATF Report's authors emphasized that real estate agents are well placed to detect suspicious

[3] *Ibid*, at 10.
[4] *Ibid*, at 12, 13, 14.
[5] *Ibid*, at 12, 13, 14.
[6] *Ibid*, at 25.
[7] *Ibid.*
[8] *Ibid*, at 27.
[9] *Ibid*, at 34.
[10] *Ibid*, at 28.

activity or identify red flags because they generally know their clients better than other parties to the transaction.[11]

14. In 2013, FATF released a report titled "Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals" (the "2013 FATF Report").[12] The 2013 FATF Report identifies real estate as a vulnerability for money laundering by legal professionals. It also outlines reasons real estate is attractive to money launderers: it provides a location to live and conduct business, it is an appreciating asset, and the sale of real estate appears as a legitimate source of funds.[13] The 2013 FATF Report notes:

> The types of assets acquired by criminals with the proceeds of their crime are evidence of the laundering methods utilised and highlight areas of potential vulnerability. Real estate accounted for up to 30% of criminal assets confiscated in the last two years, demonstrating this as a clear area of vulnerability.[14]

15. This 2013 FATF Report discussed the use of trust accounts as a mechanism of obscuring source of funds in the purchase of real estate,[15] and noted that cash is sometimes used, but "increasingly, [purchase of real estate] is seen as part of the layering process, where the funds have been accumulated in one or more bank accounts and the property purchase is wholly or predominantly funded through private means rather than a mortgage or loan."[16]

16. The FATF 2013 report includes a series of red flag indicators, and a schedule of case studies.[17] Many of the indicators with a real estate component are the same as those identified in the FATF 2007 report. Some of the Canadian case studies involving real estate include:

a. Case 15 – a career criminal deposited cash into his parents' bank account, then purchased a home registered to his parents using a mortgage that was paid off in less than 6 months.[18]

---

[11] *Ibid*, at 29.
[12] **Appendix 2**, FATF, Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (Paris: FATF, June 2013), online: <www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf> ("FATF 2013").
[13] *Ibid*, at 44.
[14] *Ibid*, at 24.
[15] *Ibid*, at 37, 39, 41. See also Stephen Schneider, "Money laundering in Canada: A quantitative analysis of RCMP cases" (July 2004) 11:3 J Financ Crime, online: <doi: 10.1108/13590790410809220>, at 282.
[16] FAFT 2013, s*upra* note 12, at 44.
[17] *Ibid*, at 77-82; 96-148.
[18] *Ibid*, at 49.

b. Case 67 – a BC man used proceeds from sale of various illicit drugs to purchase homes in BC, by way of regular cash deposits of $4,000-5,000 to his lawyer. Many of the homes would be used as grow-ops.[19]

c. Case 95 – a law firm acting on behalf of known drug traffickers incorporated shell companies and used trust accounts to conduct real estate transactions.[20]

17. In 2018, FATF released a report entitled "Professional Money Laundering" ("2018 FATF Report"),[21] which reviews techniques favoured by professional service providers that specialize in money laundering services. The report includes some commentary on real-estate focused money laundering, including Project OROAD, a Canadian investigation into an organized crime drug trafficking ring in which 10 nominees were hired to establish 25 shell companies in various industries, including the real estate sector.[22] The operation appeared to be an example of trade-based money laundering, with nominees in China, Panama and the US, in addition to Canada.[23]

18. Another example involved a BC network with connections to criminal organizations in Mexico, Asia, and the Middle East, which is said to have laundered $1 billion per year.[24] The model involved moving money from China to Canada in order to gamble in Canada, but using an informal value transfer system rather than actually moving the funds. Gamblers would receive cash in casino parking lot, purchase chips, and obtain a "BC casino cheque" which could then be deposited into a Canadian banking account. Some of the funds were reportedly used for real estate purchases in Canada.[25]

19. The standing FATF recommendations, known formally as the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations", were updated in June 2019 (the "FATF Recommendations").[26] With respect to real estate, they provide:

---

[19] *Ibid*, at 116.
[20] *Ibid*, at 131.
[21] **Appendix 3**, FATF, *Professional Money Laundering* (Paris, France: FATF, July 2018), online: < https://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html#:~:text=Paris%2C%2026%20July%202018%20%2D%20Professional,countries%20identify%20and%20dismantle%20them> ("FATF 2018").
[22] *Ibid*, at 31.
[23] I*bid.*
[24] *Ibid*, at 34.
[25] *Ibid.*
[26] **Appendix 4**, FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Paris, France: FATF, October 2020), online: www.fatf-gafi.org/recommendations.html ("FATF 2020").

> The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:
>
> (b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.[27]

20. Recommendation 10 provides that entities be required to undertake customer due diligence (CDD) for all customers, when:

a. establishing business relations;

b. carrying out transactions above USD/EUR 15,000; or involving wire transfers in some cases;[28]

c. there is a suspicion of money laundering; or

d. the identity data provided is inadequate, or there are doubts about its veracity.[29]

21. The recommendations suggest the CDD measures should include:

a. Identifying the customer using reliable documentation;

b. Identifying and taking reasonable measures to verify the identity of the beneficial owner, including understanding ownership and control of legal persons;

c. Understanding the purposes and nature of the business relationship; and

d. Ongoing due diligence on future transactions to ensure transactions are consistent with customer's business and source of funds. [30]

22. Additionally, Recommendation 10 provides:

23. Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business

[27] *Ibid*, at 18.
[28] I.e. wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16 issued by FATF.
[29] FATF 2020, *supra* note 26 at 12.
[30] *Ibid*, at 12.

relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.[31]

24. The remaining recommendations provide:

> 11. That records be kept for 5 years, including customer due diligence, identification documents, and analysis undertaken;[32]
>
> 12. Entities should be required to conduct additional due diligence for foreign politically exposed persons including establishing the source of wealth and funds;[33]
>
> 15. Entities should identify and assess money laundering risks arising from new products or new business practices, including virtual assets;[34] and
>
> 17. When relying on third parties for customer due diligence, entities should ensure that the third party is regulated and has measures in place for due diligence that adhere to standards in Recommendation 10, ensure information is obtained immediately and documentation will be available without delay.[35]

25. In September 2016, the FATF released its Mutual Evaluation Report for Canada "), Anti-money laundering and counter-terrorist financing measures – Canada" (the "Canada MER").[36] The key findings of the Canada MER with respect to real estate were as follows:

a. The real estate sector in Canada is "highly vulnerable" to money laundering, including international money laundering.[37] The sector is exposed to high risk clients, including PEP's from Asia, and foreign investors from locations of concern.[38] Certain real estate products, such as mortgage loans were considered high-risk.[39] The main typologies identified in reviewing real estate-related STRs submitted to FINTRAC ranged from the use of nominees by criminals, structuring of cash deposits, to sophisticated schemes involving loans, mortgages, and the use of a lawyer's trust account.[40] FATF commented that the existence of a memorandum of understanding between the RCMP and the People's Republic of

---

[31] *Ibid*, at 13.
[32] *Ibid*, at 13.
[33] *Ibid*, at 14.
[34] *Ibid*, at 15.
[35] *Ibid*, at 16.
[36] **Appendix 5**, FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures - Canada*, Fourth Round Mutual Evaluation Report (Paris, France: FATF, September 2016), online: www.fatf-gafi.org/publications/mutualevaluations/documents/mer-canada-2016.html ("FATF 2016").
[37] *Ibid,* at 16.
[38] *Ibid.*
[39] *Ibid,* at 79.
[40] *Ibid.*

China was important, but noted that "no assistance with this country was reported in the province of British Columbia, despite the fact that it appears to be at greater risk of seeing its real estate sector misused to launder POC generated in China."[41]

b. Supervision of real estate sector is not commensurate to the AML risks in that sector; more supervision is necessary.[42]

c. Real estate agents are not aware of their AML obligations.[43] Real estate agents are not familiar with basic customer due diligence processes, and particularly are noncompliant with the third-party determination rule.[44]

d. Real estate agents "consider that they face a low risk because physical cash is not generally used in real estate transactions…[and] are overly confident on the low risk posed by "local customer," as well as non-resident customer originating from countries with high levels of corruption."[45] Further, "detection of suspicious transactions is mainly left to the "feeling" of the individual agents, rather than the result of a structured process assisted by specific red flags."[46]

e. STRs have gradually increased but remain very low in real estate.[47]

f. More dialogue is necessary with the real estate industry.[48] [FINTRAC] "needs to further develop its sector-specific expertise and increase the intensity of supervision of DNFBPs, particularly in the real estate sector and with respect to DPMS, commensurate with the risks identified in the NRA."[49] FINTRAC should update ML/TF typologies and specific red flags to assist in detection of suspicious transactions.[50] FINTRAC does not provide enough sector-specific compliance guidance and typologies especially in the real estate sector.[51]

---

[41] *Ibid,* at 112.
[42] *Ibid,* at 4.
[43] *Ibid,* at 5.
[44] *Ibid,* at 82.
[45] *Ibid,* at 80.
[46] *Ibid,* at 85.
[47] *Ibid,* at 7, 41.
[48] *Ibid,* at 5.
[49] *Ibid,* at 8.
[50] *Ibid,* at 78.
[51] *Ibid,* at 99.

B. FINTRAC

26. On November 14, 2016, FINTRAC released its operational brief "Indicators of Money Laundering in Financial Transactions Related to Real Estate," which lists its purpose as assisting reporting entities involved in real estate transactions to appropriately report suspicious transactions (the "2016 Indicators Brief").[52] In the 2016 Indicators Brief, FINTRAC advised that filings of suspicious transaction reports ("STR's") regarding real estate were "minimal," but nonetheless the STR's that were received exhibited the same indicators of money laundering reported internationally.[53] FINTRAC stated:

27. FINTRAC, through its compliance examinations, has observed deficiencies in most aspects of the real estate sector's compliance programs that render it more vulnerable of being used by criminals to launder illicit funds.[54]

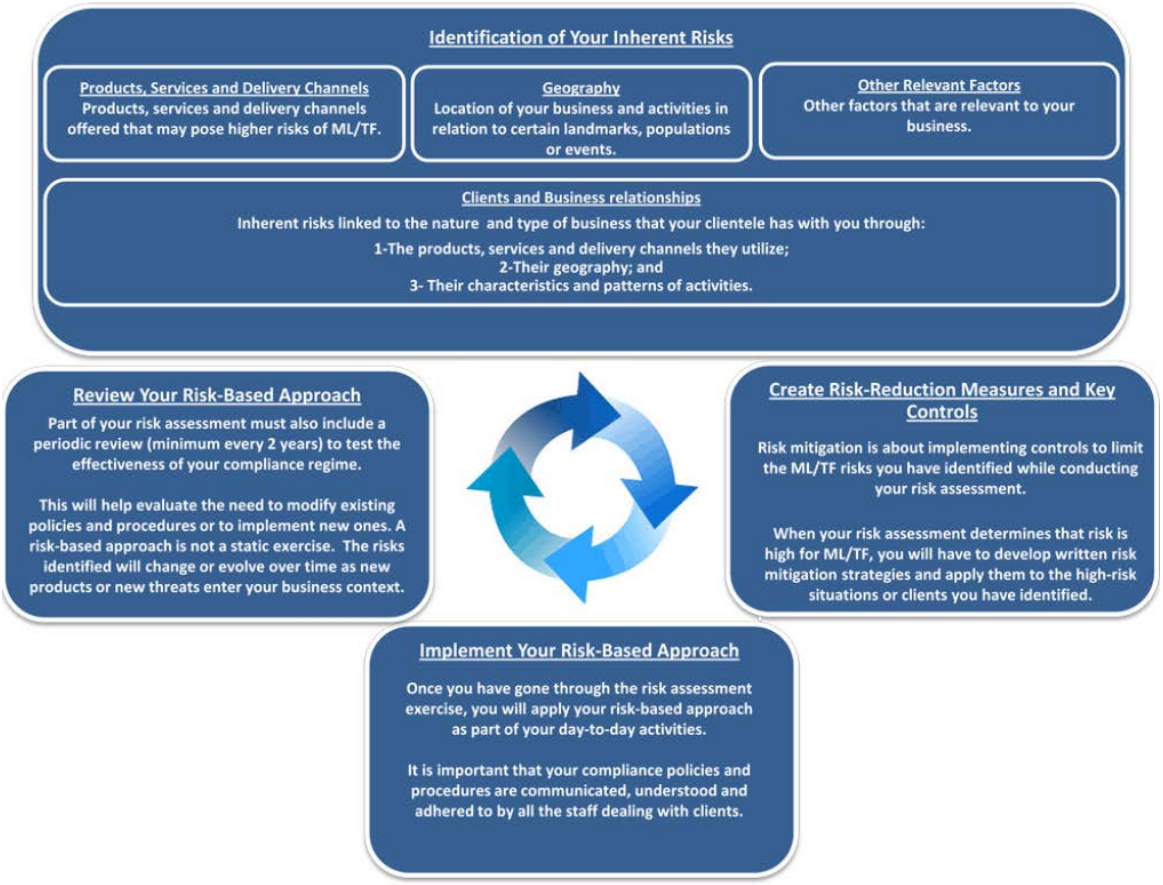
28. The 2016 Indicators Brief describes how money laundering may occur in real estate, and the impact it may have, including artificially inflating the housing market.[55] The 2016 Indicators Brief describes the obligation to report by real estate agents, and the opportunity for non-reporting entities to submit voluntary reports.

29. On the level of suspicion required to submit a report, FINTRAC described the threshold as "more than a "gut feel" or "hunch", but not as high as having evidence that money laundering is actually occurring."[56] Rather, reporting entities should look for transactions that stand out as unusual (such as if a customer is unconcerned with the quality of the property or if a suspicious mortgage is involved) recognizing that suspicion may only arise with accumulation of more information over time.[57] The 2016 Indicators Brief presents 32 indicators and 12 themes that real estate reporting entities should consider in whether to report a suspicious transaction. Those themes are: anonymity, flipping, transaction speed, loan, renovations, income generating, flow through, structuring, geography, inconsistency, defaulting, and direct.[58]

---

[52] **Appendix 6**, Financial Transactions and Reports Analysis Centre of Canada, *Operational Brief: Indicators of Money Laundering in Financial Transactions Related to Real Estate* (Ottawa: FINTRAC, 2016), online: https://www.fintrac-canafe.gc.ca/intel/operation/real-eng.pdf ("FINTRAC 2016").
[53] *Ibid*, at 1.
[54] *Ibid,* at 2.
[55] *Ibid*.
[56] *Ibid*, at 3.
[57] *Ibid*, at 3-4.
[58] *Ibid*, at 4-6.

30. In December 2018, FINTRAC released guidance on its website for the real estate sector entitled "Risk-based approach workbook Real estate sector" ("Risk-based Guidance").[59] The guidance is presented as a workbook to assist in development and implementation of the risk-based approach, since assessing and documenting risk is required under the PCMLTFA. FINTRAC noted the use of this workbook was not mandatory.[60] The Risk-based Guidance depicts the risk-based approach cycle accordingly:



31. FINTRAC provided greater detail for each of the bubbles of the cycle chart in the Risk-based Guidance, for example.[61] The Risk-based Guidance also includes two worksheets, a

[59] **Appendix 7**, Financial Transactions and Reports Analysis Centre of Canada, "Risk-based approach workbook: Real estate sector", online: <https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-res-eng>, accessed October 14, 2020 ("FINTRAC 2018").
[60] *Ibid.*
[61] *Ibid.*

"Business-based risk assessment worksheet," and a "Relationship-based worksheet" both of which are tables that set out scenarios and describe how each scenario could be low or high risk depending on certain factors. FINTRAC is careful to say that these classifications are not universal or exhaustive, and may change depending on the business' specific circumstances. A page of further instructions is provided for each worksheet in the annexes to the Risk-based Guidance. Both of the worksheets encourage reporting entities to come up with their own categories of risk, and strategies for mitigating high-risk situations.

32. In January 2019, FINTRAC released further guidance, entitled "Money laundering and terrorist financing indicators – Real estate," which is stated to be the culmination of a three-year FINTRAC review of money laundering/terrorism financing cases, review of international literature from FATF and the Egmont Group, and consultation with reporting entities (the "2019 Indicators Brief").[62] This document appears to be an evolution of the November 14, 2016 operational brief. The indicators are grouped into topic areas: identifying the person or entity; client behaviour; person/entity financial profile; atypical transactional activity; transactions structured below the reporting or identification requirements; transactions that involve non-Canadian jurisdictions; indicators related to use of other parties (use of a third party, nominee, or gatekeeper); terrorist financing; indicators specific to real estate agents and developers; and indicators specific to real estate brokers and sales representatives.

33. In 2014, FINTRAC commissioned Grant Thornton LLP to prepare a report evaluating the risk of reporting entity sectors, "Reporting entity sector profiles – money laundering terrorist and financing vulnerability assessments" (the "Grant Thornton Report").[63] Overall, the Grant Thornton Report found the real estate sector to be comparatively high risk, in part because the sector was "apparently unengaged…in AML compliance, and other sectors (eg banking and securities) are not sufficiently viewing this sector as one with higher risk transactions, meaning that higher degrees of scrutiny are not being applied."[64]

34. The Grant Thornton Report found that "larger commercial real estate firms are aware of the AML regulations and reportedly have strict regimes in place including customer identification,

---

[62] **Appendix 8**, Financial Transactions and Reports Analysis Centre of Canada, "Money laundering and terrorist financing indicators - Real estate", online: <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/real_mltf-eng>, accessed October 14, 2020 ("FINTRAC 2019").
[63] **Appendix 9**, Grant Thornton LLP, *Reporting Entity Sector Profiles – Money Laundering Terrorist and Financing Vulnerability Assessments* (Toronto: Grant Thornton LLP, March 31, 2014) ("Grant Thornton").
[64] *Ibid*, at 7.

training and reporting of suspicious transactions…larger firms tend to be risk averse"[65] but "at the smaller end of the market there is often no quality and ethics infrastructure in place for these sectors," i.e. the real estate and money service business sector.[66] Further, the Grant Thornton Report found that at the smaller end of the market, there continued to be a high number of cash transactions.[67]

35. Purchase of Canadian real estate assets with offshore money and/or by offshore persons was noted as a significant risk factor."[68] The Grant Thornton Report also found the use of corporate vehicles to purchase real estate was a higher risk factor,[69] as was private lending,[70] and the use of lawyers' trust accounts to "knowingly or unknowingly provide legitimacy and/or obscure the source of illegally sourced funds."[71]

C. EU

36. In February 2019, the European Parliamentary Research Service released a briefing report titled "Understanding money laundering through real estate transactions," which describes how real estate is used for money laundering, sets out typologies including providing some case studies, and provides suggestions for combatting money laundering.[72] The report repeats many of the indicators articulated by FATF and set out in the academic literature.[73] As with the FATF reports, the EU report indicates "real estate plays a role (mainly) in the third and final stage of the money-laundering cycle, after the placement and the layering phases."[74] The report discusses the need to understand normal conduct of business in order to spot money laundering as an unusual transaction, including familiarity with customer risk, transaction risk, and geographical risk.[75]

---

[65] *Ibid*, at 17.
[66] *Ibid*, at 5.
[67] *Ibid*, a. 7.
[68] *Ibid*, at 23.
[69] *Ibid*, at 25.
[70] *Ibid*.
[71] *Ibid*, at 7.
[72] **Appendix 10**, European Parliament, "Understanding money laundering through real estate transactions" (European Union, 2019), online: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/633154/EPRS_BRI(2019)633154_EN.pdf> ("European Parliament 2019").
[73] *Ibid*, at 2.
[74] *Ibid*.
[75] *Ibid*, at 3-4.

37. The report also comments on the impact of money laundering in real estate in the EU, and globally – reviewing past attempts at quantifying the extent of money laundering, including by the World Bank, OECD, and United Nations Office on Drugs and Crime.[76] Following this, the report details the impact of money laundering in the EU.[77]

38. Additionally, the report makes reference to several examples in Canada, including Transparency International Canada's 2016 report on transparency in real estate ownership,[78] and the introduction of the speculation tax in BC.[79]

3. ACADEMIC LITERATURE

39. In addition to the intergovernmental and FINTRAC publications reviewed above, there is considerable academic and quasi-academic literature describing the allure of real estate as a money laundering vehicle. The use of real estate by criminals, particularly organized criminals, as a means of offloading and laundering proceeds of crime is well-documented as occurring all over the world, with documented occurrences in Europe, Southeast Asia, Japan, South and Latin America, the United Kingdom, the United States, Australia, and Canada.[80] One study of 52 Dutch criminal cases found that in 30-40% of money laundering cases, money was invested in real estate.[81]

---

[76] *Ibid*, at p 6.
[77] *Ibid*, at 7-9.
[78] **Appendix 11**, Transparency International Canada, *No Reason to Hide: Unmasking the Anonymous Owners of Canadian Companies and Trusts,* (Ottawa: Transparency International, 2016), online: <https://static1.squarespace.com/static/5df7c3de2e4d3d3fce16c185/t/5dfb8a955179d73d7b758a98/1576766126189/no-reason-to-hide.pdf>, ("TI 2016").
[79] Sep 30 2016, Has Vancouver found the solution to a super-heated housing market?
[80] Louise Shelley, "Money Laundering into Real Estate" in Michael Miklaucic and Jacqueline Brewer, eds, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, D.C.: National Defense University Press, 2013) ("Shelley"); AUSTRAC, *Strategic Analysis Brief: Money Laundering through Real Estate*, (Australia: AUSTRAC, 2015), online: <https://www.austrac.gov.au/sites/default/files/2019-07/sa-brief-real-estate_0.pdf> ("AUSTRAC"), at 5.
[81] Joras Ferwerda and Brigitte Unger, "Detecting Money Laundering in the Real Estate Sector", in Brigitte Unger and Daan van der Linde, eds, *Research Handbook on Money Laundering* (Northampton: Edward Elgar, 2013), at 269, citing J. Meloen, R. Landman, H. de Miranda, J. van Eekelen, and S. van Soest (2003), *Bui ten Besteding: Een Empirisch OnderZoek Naar de Omvang, de Kennerken en de Besteding van Misdaadgeld,* Den Haag: Reed Business Information.

40. Like the governmental and intergovernmental reports above, some academic literature has attempted to identify indicators of money laundering in real estate. An examination of Netherlands-focused literature led to the following list of 15 indicators:[82]

a. Financier is from abroad;

b. Financier is a person, not a company;

c. Financing is unusual compared to appraised value;

d. Financing is not used (no mortgage);

e. Financing is provided by the owner (same person);

f. Owner is from abroad;

g. Owner is a person with an unusual number of objects or transactions;

h. Owner is a company with a particular exploitation;

i. Owner is a company just established;

j. Owner is a company without employees;

k. Owner is a "world citizen" (unknown to the tax administration;

l. Real estate object is involved in multiple transactions;

m. Real estate is in a very bad or a very good neighbourhood; and

n. Purchase amount is unusual compared to appraised value or previous purchase amount.

The study applied the indicators to the real estate of two Dutch cities, and found that while one or two flags per property was common, the presence of five or more flags was "quite exceptional," suggesting the use of indicators remains a useful methodology for identifying potentially suspicious real estate transactions.[83]

[82] Ferwerda and Unger, at 272-275.
[83] Ferwerda and Unger, at 276.

A. Cash and money laundering in real estate

41. In reviewing money laundering in real estate around the world, Professor Louise Shelley observed that real estate is used at all three phases of the money laundering cycle.[84] She describes those phases as:

42. Placement involves the introduction of dirty money into the system. Layering occurs when the money is already in the system and the audit trail is deliberately obscured. Integration occurs when the money is already functioning within the system.[85]

43. While purchases of real estate with physical cash occurs in some "developing nations," in the "developed world," there are usually barriers to purchasing real estate with cash.[86] In developed nations, purchasing real estate with cash is suspicious, such that financial institutions become the initial entryway (or placement stage) for proceeds of crime entering real estate.[87] However, real estate is involved in the latter two phases of the money laundering cycle, layering and integration, in developed and developing nations. Professor Shelley describes real estate's role in these two phases:

44. Transactions in the layering stage are intended to obscure any financial (traceable) links between the funds and their original criminal sources. In this stage, laundering typically occurs by moving funds in and out of offshore bank accounts. Overseas, the money may be used for real estate investments or may assume the form of a foreign bank loan to buy a house, when the loan is in reality the purchaser's own money parked overseas. Finally, the goal of integration is to create a "history" showing that funds were acquired legally. In the integration phase, the criminal places money in the real estate sector and is not interested in trading in real estate but in investing.[88]

---

[84] Shelley, *supra* note 80*,* at 132; per Professor Brigitte Unger: "To sum up, the real estate sector is by its very nature complex and prone to criminal abuse." Brigitte Unger et al., *Detecting Criminal Investment in the Dutch Real Estate Sector* (Dutch Ministry of Finance, Justice and Interior Affairs: January 2010) ("Unger at al"), at 202–203; Fabian Maximilian Johannes Teichmann "Real estate money laundering in Austria, Germany, Liechtenstein and Switzerland" (2018) 21:3 *Journal of Money Laundering Control* ("Teichmann"), at 371.
[85] Shelley, *supra* note 80, at 140; see also Ferwerda and Unger, at 269.
[86] *Ibid.*
[87] *Ibid.*
[88] *Ibid, at* 132; Unger et al, *supra* note 81.

45. It is worth noting here that there is sometimes confusion between real estate purchases made with literal, physical cash, and "all-cash purchases" of real estate; the latter term refers to real estate purchases made without a mortgage or other financing, but does not involve the transfer of physical cash.[89]

B. Types of real estate subject to laundering

46. Experts agree that both commercial and residential real estate are vulnerable to money laundering.[90] Significant examples of laundering in commercial real estate include: the *yakuza* in Japan prior to the long term recession,[91] laundering using cattle ranches in Colombia,[92] property purchases in the red light district of Amsterdam,[93] hotel purchases in tourist areas in Spain and Turkey,[94] and the establishment of Las Vegas.[95]

47. Residential examples abound.[96] While attention has often focused on the use of lavish, high-end real estate by criminal organizations, low-end real estate is also subject to use for money

---

[89] Transparency International Canada, Opacity – why criminals love Canadian real estate (and how to fix it) (Ottawa: Transparency International, 2019), online: <https://static1.squarespace.com/static/5df7c3de2e4d3d3fce16c185/t/5dfb8cf8f8effb79c8bdf415/1576766716341/opacity.pdf >, ("TI 2019"), at 14; the Maloney Report refers to "cash purchases" of real estate at 150; the Second German Report refers to same at 52, 67.

[90] Shelley, *supra* note 80, at 134; TI 2019, *supra* note 86, at 21.

[91] Shelley, *supra* note 80, at 135; Peter B.E. Hill, *The Japanese Mafia: Yakuza, Law, and the State* (Oxford: Oxford University Press, 2003), ("Hill"), at 185, 177–247; Shared Hope International, *Demand: A Comparative Examination of Sex Tourism and Trafficking in Jamaica, Japan, the Netherlands and the United States* (Shared Hope, July 200), online: < https://sharedhope.org/wp-content/uploads/2012/09/DEMAND.pdf>, at 113–141; David Kaplan and Alec Dubro, *Yakuza: Japan's Criminal Underworld, expanded edition* (Berkeley and Los Angeles: University of California Press, 2003), 196–220.

[92] Shelley, *supra* note 80, at 136; Francisco Thoumi, T*he Political Economy & Illegal Drugs in Colombia* (Boulder, CO: Lynne Rienner, 1995), 60, and 237–238; International Crisis Group, *War and Drugs in Colombia, Latin America Report: Latin America Report No. 11* (International Crisis Groups, January 27, 2005), online: <https://www.crisisgroup.org/latin-america-caribbean/andes/colombia/war-and-drugs-colombia>, at 26.

[93] Shelley, *supra* note 80, at 138; Unger et al. *supra* note 81; Brigitte Unger and Joras Ferwerda, Money Laundering in the Real Estate Sector: Suspicious Properties (Massachusetts: Edward Elgar, 2011).

[94] Shelley, *supra* note 80, at 136.

[95] Shelley, *supra* note 80; Howard Abadinsky, *Organized Crime*, 7th ed. (Belmont, CA: Wadsworth/Thomson Learning, 2003), 235–236.

[96] Shelley, *supra* note 80, at 134-140; TI 2019, *supra* note 86, at 16, 23, 24, 28, 29, 30; TI 2016, *supra* note 78, at 31; United States Senate Permanent Subcommittee on Investigation, *Keeping foreign corruption out of the United States: Four case histories* (4 February 2010), online: <https://www.hsgac.senate.gov/imo/media/doc/FOREIGNCORRUPTIONREPORTFINAL710.pdf>; United States Department of Justice, "Press Release" (July 20 2016), online: <www.justice.gov/opa/pr/united-states-seeks-recover-more-1-billion-obtained-corruption-involving-malaysian-sovereign>; also see:

laundering. Examples of the latter include Arizona,[97] rural Ohio, and central Tokyo.[98] In some cases, property is purchased but left vacant, and "[s]uch decay may be allowed so the criminal investors can subsequently buy neighboring properties at depressed costs, thereby increasing their territorial influence."[99] In Austria, Germany, Liechtenstein and Switzerland, money launderers were noted to prefer to buy property in large metropolitan areas where they can maintain anonymity.[100]

48. Additionally, money launderers may become landlords and rent out residential property as a way to integrate illicit funds into the licit economy. The owner may provide illicit funds to the tenant to pay rent, or in some case, the owner may even become the tenant and rent the property out to themselves. The method allows the criminal to legitimize their illicit funds.[101]

49. In a study of money laundering through real estate in the Netherlands, Kruisbergen, Kleemans and Kouwenberg found that the type of property used by money launders differed depending on the predicate offence. For those who engaged in criminal activity like drug trafficking, human smuggling, and illegal arms trade, 45% of the property acquired was for residential use while 18% was for commercial use (such as hotels and casinos). In comparison, only 24.5% of the property acquired by those who engaged in fraud and money laundering was residential, while 69.9% was for commercial use. The remaining difference for both types of criminal groups was "Other/Unknown". [102]

C. Advantages of real estate as a money laundering tool

50. A number of practical benefits of real estate to money launderers are repeatedly cited, such as:

---

www.justice.gov/archives/opa/page/file/877166/download; December 21, 2016 'Brazil' 'Carwash' probe yields largest-ever corruption penalty';

[97] Shelley, *supra* note 80, at 140.

[98] *Ibid,* at 134.

[99] *Ibid*, at 135-6.

[100] Teichmann, *supra* note 81, at 372.

[101] AUSTRAC, *supra* note 80, at 9; Ilaria Zavoli & Colin King,"New development: Estate agents' perspectives of anti-money laundering compliance—four key issues in the UK property market" (2020) 40:5 *Public Money & Management* ("Zavoli"), at 418; Teichmann, *supra* note 81, at 372.

[102] Edwin W. Kruisbergen & Edward R. Kleemans & Ruud F. Kouwenberg "Profitability, Power, or Proximity? Organized Crime Offenders Investing Their Money in Legal Economy". (2015) 21:2*European Journal on Criminal Policy and Research* ("Kruisbergen"), at 243-245.

a. enjoyment of the property, both in terms of residing/conducting business on the property, and as a display of one's success;[103]

b. the benefit of having a location at which to conduct criminal activity;[104]

c. a large amount of money can be laundered with a single transaction, due to the high value of real estate relative to other goods;[105]

d. the relatively low transaction costs, as compared to other methods of money laundering, and the perception of real estate as a safe investment;[106]

e. the potential for income generation via rental income or the appreciation of property;[107]

f. opportunity for further laundering via the real estate, such as by construction on the property;[108]

g. taking out a mortgage to pay for real estate provides an opportunity to use illicit funds to partially service the debt;[109] and

h. the ability to develop influence and power at a local level, such as in cases where a large real estate portfolio is owned in a small town or neighbourhood.[110]

51. In addition to these practical benefits, structural and regulatory factors are cited as incentives for using real estate to launder funds:

---

[103] Shelley, *supra* note 80, at 134; Ferwerda and Unger, at 268; Sean Hundtofte and Ville Rantala, "Anonymous Capital Flows and U.S. Housing Markets" (2018), University of Miami Business School Research Paper No. 18-3 ("Hundofte amd Rantala"), at 10; European Parliament 2019, *supra* note 72, at 2.
[104] Shelley, *supra* note 80, at 134; AUSTRAC, *supra* note 80, at 9; Ferwerda and Unger, at 269.
[105] Shelley, *supra* note 80; Unger et al., *supra* note 81, at 14; Ferwerda and Unger, at 268; TI 2019 *supra* note 86, at 20; Hundtofte and Rantala, *supra* note 100, at 10; Kruisbergen, *supra* note 99, at 243.
[106] Shelley, *supra* note 80, at136: "many forms of laundering cost launderers 10 to 20 percent of the sums they seek to clean, this rule does not always apply in the real estate sector;" see also Kruisbergen, *supra* note 99, at 243, 252; Teichmann, *supra* note 81, at 374.
[107] Shelley, *supra* note 80, at 136; Ferwerda and Unger, at 269; European Parliament 2019, *supra* note 72, at 2; Teichmann, *supra* note 81, at 372-373; see also Kruisbergen, *supra* note 99, at 243, 252; Teichmann, *supra* note 81, at 374.
[108] Shelley, *supra* note 80; Unger et al., *supra* note 81, at 14; Hill, *supra* note 88, at 96; TI 2019 *supra* note 86, at 20; Tecihmann, *supra* note 81, at 372-373.
[109] AUSTRAC, *supra* note 80, at 7.
[110] Kruisbergen, *supra* note 99, at 248.

i. pressure on financial institutions to avoid doing business with potential money launderers has led to reforms that have encouraged launderers to seek alternate means of laundering;[111]

j. ability to manipulate price of real estate;[112]

k. ease of maintaining privacy due to lack of transparency in public corporate and land registries (see more below);[113]

l. conflict for real estate professionals between performing due diligence re: source of funds and attracting clients;[114]

m. minimal reporting of suspicious transactions on the part of the opposite party to the sale, or on the part of real estate professionals;[115] and

n. poor enforcement and insufficient sanctions for facilitating money laundering in real estate.[116]

D. Transparency/beneficial ownership

52. Some commentators, notably Transparency International and Transparency International Canada, point to the availability of mechanisms to disguise ownership as a key attraction for money launderers.[117] These commentators propound that the dearth of data collected by corporate and land registries (i.e. the collection of legal titleholder information but not information on beneficial owners) impedes investigation by law enforcement, prevents real estate

[111] Shelley, *supra* note 80, at 132; TI 2019 *supra* note 86, at 20.
[112] TI 2019 *supra* note 86, at 20; Hundtofte and Rantala, *supra* note 100, at 10; AUSTRAC, *supra* note 80, at 8.
[113] TI 2019 *supra* note 86, at 20-21; Transparency International, "Doors Wide Open: Corruption and Real Estate in Four Key Markets" (Transparency International, 2017), online: <https://images.transparencycdn.org/images/2017_DoorsWideOpen_EN.pdf, ("TI 2017"); TI 2016, *supra* note 78; Shelley, *supra* note 80, at 141; Hundtofte and Rantala, *supra* note 100, at 2; Kruisbergen, *supra* note 99, at 243.
[114] Shelley, *supra* note 80, at 132; TI 2017, *supra* note 111, at 19; Zavoli, *supra* note 98, at 416.
[115] TI 2017, *supra* note 111, at 24, 29-30; Mohammed Ahmad Naheem, "Money laundering and illicit flows from China – the real estate problem" (2017) 20:1 *Journal of Money Laundering Control* ("Naheem"), at 23.
[116] Shelley, *supra* note 80, at 132; TI 2019 *supra* note 86, at 20; TI 2017, *supra* note 111, at 31, 32; TI 2016, *supra* note 78.
[117] TI 2016, *supra* note 78, and TI 2017, *supra* note 111, at; see also Shelley, *supra* note 80, at 141

professionals from conducting due diligence, and obscures insight into the flow of funds or into networks of individuals who may be laundering money.[118] In sum, they propound that the opacity afforded by land and corporate registries "make[s] trafficking into real estate a very viable option for laundering significant sums."[119]

53. In an attempt to better understand the influence of opacity (particularly the use of shell companies) in proceeds of crime entering real estate, two U.S. academics, Sean Hundtofte and Ville Rantala, studied the impact of a Geographic Targeting Order issued by the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the US Department of the Treasury.[120]

54. FinCEN has the authority to issue an order that imposes certain recordkeeping and reporting requirements on certain entities in a geographic area.[121] This is known as a Geographic Targeting Order ("GTO"). In 2016, FinCEN issued GTO's that required reporting of beneficial ownership information of companies that had purchased real estate. Specifically, the GTO required title insurance companies to identify the beneficial owners of LLC's that purchased luxury real estate.[122] Initially, on January 13, 2016, FinCEN issued GTO's that applied to Manhattan and Miami-Dade County.[123] On July 27, 2016, FinCEN expanded the order by issuing GTO's to 12 additional counties in California, Florida, and Texas.[124]

55. Professors Hundtofte and Rantala describe the ability to make all-cash[125] purchases of residential real estate by using a limited liability company ("LLC") was perceived as a key loophole in US anti-money laundering regulations.[126] By using an LLC, all-cash purchasers of real estate could avoid triggering the banking system's "know your customer" requirements, and could avoid identifying themselves to law enforcement authorities.[127]

---

[118] *Ibid* .
[119] Shelley, *supra* note 80, at 141; Naheem, *supra* note 113, at 021-22; Teichmann, *supra* note 81, at 327.
[120] Hundtofte and Rantala, *supra* note 100, at 3.
[121] See 31 U.S.C. § 5326(a); 31 C.F.R. § 1010.370; and Treasury Order 180-01
[122] Hundtofte and Rantala, *supra* note 100, at 8.
[123] *Ibid,* at 7
[124] *Ibid.*
[125] Again, this reference to "all cash" here means the purchase was unfinanced, not that it involved physical currency.
[126] Hundtofte and Rantala, *supra* note 100, at 2.
[127] *Ibid*. Note that "all-cash" does not mean the physical transfer of cash, but rather that the real estate was purchased without a mortgage or other bank financing. Obtaining a mortgage or other new financing would trigger US banks' "know your customer" requirements, putting those purchasers outside of this loophole. See Hundtofte and Rantala, at 9, and speech of Jamal El-Hindi, Deputy Director of FinCEN, at the Institute of International Bankers Annual Anti-Money Laundering Seminar on May 16, 2016, online: <https://www.fincen.gov/news/speeches/jamal-el-hindi-deputy-director-financial-crimes-enforcement-network>.

56. Professors Hundtofte and Rantala examined the rate of all-cash purchases of real estate before and after the introduction of the GTO's. They found that all-cash purchases by corporate entities comprised 10% of the dollar volume of housing purchases prior to the GTO's.[128] This figure fell by 75% upon the introduction of a GTO.[129] The authors concluded that the availability of anonymity was a key incentive for all-cash purchases of real estate by LLC's, suggesting that these LLC's were being used as shell corporations: "The evidence on the whole suggests that anonymity-preferring buyers made up the majority of corporate cash purchases in the US prior to the policy change."[130]

57. Professors Hundtofte and Rantala also found declines in the luxury home markets where the GTO had been implemented; such declines were not observed in comparable jurisdictions in which no GTO applied.[131] After the GTO's were introduced, the prices of high-end house in targeted counties dropped by 4.2% more than prices in other counties.[132]

E. Foreign Capital

58. There is a substantial body of literature focusing on the role of foreign capital in driving housing prices in the Lower Mainland of BC.[133] This phenomenon has created a 'de-coupled' housing market where housing prices and local income levels are not closely aligned.[134]

59. Until recently, there was insufficient data on foreign ownership of property, making it hard to connect the rise in housing prices in the Lower Mainland with foreign capital. However, in 2018,

---

[128] *Ibid,* at 18
[129] *Ibid.*
[130] *Ibid,* at 19
[131] *Ibid,* at 5, 20-21.
[132] *Ibid,* at 20
[133] Richard Wozny, "Low Incomes and High House Prices in Metro Vancouver", *Site Economics* (2017), online: <http://siteeconomics.com/wp-content/uploads/2017/04/High-House-Prices-and-Low-Incomes-April-2017.pdf>; Penny Gurstein and Andy Yan, "Beyond the Dreams of Avarice?" in Penny Gurstein and Tom Hutton, eds, *Planning on the Edge: Vancouver and the Challenges of Reconciliation, Social Justice, and Sustainable Development* (UBC Press, 2019), at 215; Joshua Gordon, "Solving Wozny's puzzle: Foreign ownership and Vancouver's 'de-coupled' housing market." Released through the *Center for Public Policy Research*, School of Public Policy, Simon Fraser University. June 18, 2019 ("Gordon 2019"); David Ley, "A regional growth ecology, a great wall of capital and a metropolitan housing market." *Urban Studies* (2020), online: <doi: 10.1177/0042098019895226;> TI 2016, *supra* note 78; TI 2019 *supra* note 86, at 26, 29.
[134] Joshua C. Gordon, "Solving puzzles in the Canadian housing market: foreign ownership and de-coupling in Toronto and Vancouver" (2020), *Housing Studies*, DOI: 10.1080/02673037.2020.1842340 ("Gordon 2020"), at 2-3.

the Statistics Canada-led project Canadian Housing Statistics Program (CHSP) began releasing data on 'non-resident ownership' in British Columbia.[135] This data has made it possible to link foreign ownership to rising prices and the de-coupling of the Lower Mainland's housing market.[136] The CHSP data has also revealed that a disproportionate amount of 'low-income ownership' is occurring in British Columbia's most expensive neighbourhoods. This points to the possibility that households that earn income in foreign jurisdictions are avoiding paying Canadian income tax.

60. Some of this literature links the influx of foreign capital to money laundering, suggesting the pathways used to ensure anonymity and/or evade capital export restrictions are also subject to abuse by money launderers, or at least those actors seeking to siphon proceeds of crime into BC.[137] As described by Professors Ferwerda and Unger, "although it is often mentioned in the literature that many criminal investments in the real estate sector are financed with money from abroad, we cannot, of course, conclude that all real estate transactions financed from abroad are suspicious. However, we can label them unusual and conclude that the more unusual characteristics a transaction has, the more it should arouse suspicion."[138]

61. The use of real estate as a means for overseas-based crime groups to conceal assets from their home jurisdiction has also been the subject of reports in the United States, Australia, New Zealand, and the United Kingdom.[139]

4. MEDIA REPORTS

62. Money laundering occasionally garnered media attention in Canada throughout the last three decades,[140] but not until 2014 did it become a recurring focus. In spring 2014, several

---

[135] *Ibid,* at 11.
[136] *Ibid,* at 15-21.
[137] TI 2016, *supra* note 78; TI 2017, *supra* note 111, at; Stephen Punwasi, "A Brief History of Foreign Buying of Vancouver Real Estate"
(Better Dwelling, 2017), online: < https://betterdwelling.com/city/vancouver/a-brief-history-of-foreign-buying-of-vancouver-real-estate/#_>; Stephen Punwasi, "China's Capital Controls Could Crash Vancouver Real Estate" (Better Dwelling, 2017), online: <https://betterdwelling.com/city/vancouver/chinas-capital-controls-could-crash-vancouver-real-estate/>.
[138] Ferwerda and Unger, at 270
[139] AUSTRAC, *supra* note 80, at 4; Naheem, *supra* note 113, at 16-19.
[140] For an overview, see Schneider's Literature Review https://cullencommission.ca/data/exhibits/6%20-%20Money%20Laundering%20in%20BC%20-%20A%20Review%20of%20the%20Literature.pdf

Canadian news outlets reported on money laundering issues in BC casinos.[141] Other reports pointed to investment in Canadian real estate as a means for overseas buyers to launder money.[142] News reports documenting alleged money laundering began to proliferate. The interplay between money laundering and British Columbia real estate featured repeatedly in these reports.[143]

63. In September 2015[144], October 2015[145], February 2016,[146] March 2016,[147] April 2016,[148] September 2016[149], and again in February 2018[150], the Globe and Mail published a series of in-depth investigations by journalist Kathy Tomlinson into money laundering in BC real estate. These investigations documented allegedly shady conduct by real estate firms and banks in the sale of BC real estate, including sale to offshore nominees, purchases by real estate agents personally for the purpose of flipping, manoeuvres to accept foreign funds while skirting currency restrictions, and real estate sales to persons and entities that had no apparent sources of funds to match the price of the real estate.

64. A February 16, 2018 article documented a practice of issuing loans secured by a mortgage on residential real estate owned by the borrower.[151] The Globe and Mail reported that 17 lenders, with either a criminal record or reported criminal ties, and only some of whom were identified, had engaged in private lending. The loans were alleged to have been given in cash, and the mortgages bore interest rates of up to 39.5%. The article implicated 45 properties in the

---

[141] April 9, 2014 - https://bc.ctvnews.ca/suspected-money-laundering-rampant-at-b-c-casinos-report-1.1769342 ; Oct 16, 2014, $27M in suspicious money flowed through 2 B.C. casinos in 3 months; Jun 28, 2014, RCMP charge 11 in investment scam
[142] July 14, 2014 https://financialpost.com/personal-finance/mortgages-real-estate/secret-path-revealed-that-allows-wealthy-chinese-to-transfer-billions-overseas-buying-pricey-property-in-vancouver-new-york-and-sydney
[143] July 14, 2014 https://financialpost.com/personal-finance/mortgages-real-estate/secret-path-revealed-that-allows-wealthy-chinese-to-transfer-billions-overseas-buying-pricey-property-in-vancouver-new-york-and-sydney ; August 24, 2015, Real estate bought with offshore cash raises money laundering concerns; August 24, 2015, Cash buys and illicit money: Federal audit probes Vancouver's real estate industry for money-laundering; August 25, 2015 Chinese money laundering in Canadian real estate?; September 16, 2015, Inside the world of B.C.'s top realtor: A deep pool of buyers, a dead fraudster and a forfeited licence; January 27, 2016 Follow the money: Evidence submitted at fraud probe points to concerns about Vancouver real estate market
[144] September 8, 2015 Canadian banks helping clients bend rules to move money out of China; September 10, 2016 Out of the shadows.
[145] October 6, 2015 Foreign investors avoid taxes through Canadian real estate.
[146] February 2, 2016 The Real Estate Technique Fueling Vancouver`s Housing Market.
[147] March 17, 2016 Vancouver housing market 'vulnerable' to money laundering.
[148] April 8, 2016 Tricks of the trade: Inside a B.C. real estate firm that has home sellers crying foul.
[149] September 14, 2016 Canadian banks' mortgage guidelines favour foreign home buyers.
[150] February 16, 2018, B.C. vows crackdown after Globe investigation reveals money-laundering scheme.
[151] *Ibid.*

Vancouver area which secured loans totaling $47 million CAD, plus interest, to these criminal-affiliated lenders. The borrowers were reported to be wealthy Chinese newcomers or tourists and their children, with wealth in China that was difficult to transfer to BC. Tomlinson linked at least one of the borrowers, and the loans he took out, to large-scale gambling activities in BC casinos.

65. In-depth reporting was also conducted by Global News' Sam Cooper (previously The Province and Vancouver Sun) into money laundering in BC real estate. One article describes efforts by the People's Republic of China to repatriate alleged money launderers in order to prosecute them in China.[152] Another article investigated the use of unlicensed wholesaling in BC, and its potential as a tool for money laundering.[153] The article describes an unlicensed agent approaching homeowners with unsolicited offers, and later assigning the contract to a background investor at a marked-up price. The article points to offshore buyers seeking to enter the Lower Mainland real estate market, and suggests the model often succeeds due to elderly and unsophisticated sellers. In January and February 2018, Mr. Cooper provided an in-depth review of the RCMP's E-Pirate investigation into Silver International, an alleged underground money service business and money laundering operation, including examining the potential links to real estate and questionable lending practices.[154]

66. Coverage of the "Vancouver model," a term coined by Australian professor John Langdale and popularized after a report given to AUSTRAC and other Australian intelligence in November 2017, began circulating in spring 2018.[155] Similarly, the release of a C.D. Howe institute report estimating the amount of money laundered in Canada at $5-100 billion, and the release of Transparency International's "Doors Wide Open" report (described above), garnered media coverage.[156]

67. In November 2018, Mr. Cooper ran a series of articles on the trafficking and consumption of fentanyl in BC,[157] including connections to organized crime, including the Big Circle Boys,[158]

---

[152] March 3, 2015 Chinese police run secret operations in B.C. to hunt allegedly corrupt officials and laundered money.
[153] March 7, 2016 Former 'wholesaler' lifts lid on a dark side of Vancouver's red-hot real estate market.
[154] January 12, 2018 Chinese developer took $2.68-million cash loan in Richmond coffee shop, legal filings allege; February 02, 2018 Huge B.C. money-laundering investigation pivots to drugs and guns.
[155] April 19, 2018, How Chinese gangs are laundering drug money through Vancouver real estate.
[156] September 6, 2018, Hidden ownership loopholes make Canada a 'pawn in global game of money laundering' report says.
[157] November 26, 2018 An introduction to Fentanyl: Making a Killing.
[158] November 27, 2018 Fentanyl kings in Canada allegedly linked to powerful Chinese gang, the Big Circle Boys.

money laundering, and real estate,[159] origins of fentanyl in China,[160] and one particular alleged transnational drug trafficking ring.[161]

68. Mr. Cooper, Ms. Tomlinson, and several news outlets also reported on other facets of the link between money laundering and BC real estate not discussed above, including: FATF's conclusion that Canadian real estate transactions are at risk for money laundering,[162] a FINTRAC-commissioned report by Grant Thornton that similarly concluded real estate is at risk for money laundering;[163] and statements that FINTRAC's compliance department was "unhappy" with the Vancouver real estate industry due to deficiencies in reporting.[164] Other news reports detailed specific examples of allegedly suspicious conduct that may have enabled money laundering in BC and Canada.[165]

69. In 2019, the number of news reports on the topic of money laundering rose dramatically.[166] The Commission was struck on May 15, 2019.[167] Prior to that date, the media reported on more examples of suspected money laundering,[168] including connections to casinos[169] and Paul King

[159] November 26, 2018, Secret police study finds crime networks could have laundered over $1B through Vancouver homes in 2016.
[160] December 1, 2018 China won't stop flood of fentanyl into Canada, sources say.
[161] November 29, 2018 High-roller targeted in RCMP's probe of alleged 'transnational drug trafficking' ring.
[162] September 16, 2016, Vancouver real estate used for money laundering, international agency says.
[163] August 25, 2015; August 24, 2015 Cash buys and illicit money: Federal audit probes Vancouver's real estate industry for money-laundering.
[164] August 24, 2015 Cash buys and illicit money: Federal audit probes Vancouver's real estate industry for money-laundering; November 18, 2016 Money-laundering watchdog cites 'significant' deficiencies at 100-plus B.C. real estate firms.
[165] September 16, 2015 Inside the world of B.C.'s top realtor: A deep pool of buyers, a dead fraudster and a forfeited licence; July 24, 2016 Meet the mysterious tycoon at the centre of half-a-billion in B.C. property deals; July 24, 2016 Mysterious wheeler-dealer at centre of a web of B.C. real estate deals; May 25, 2017 Valley board warns offshore clients seek to misuse realtor accounts; September 30, 2017 Whale gamblers ID'ed by BCLC also placed big bets on B.C. real estate; May 10, 2017, Millions in suspected Russian crime proceeds flowed through Canadian banks, companies; June 13, 2017 Crime group allegedly laundered millions through B.C. casinos; June 6, 2018, 'High roller' suspected of laundering $855M arrested in B.C., ordered deported;
[166] A google search for "money laundering" and "BC" and "real estate" limited to January 1, 2019 – May 15, 2019 yielded 15 pages of results. The same search, limited to January 1, 2014-December 31, 2018, yielded 9 pages of results (searches both conducted on September 29, 2020).
[167] Order in Council 238/2019 https://www.bclaws.ca/civix/document/id/oic/oic_cur/0238_2019
[168] January 18, 2019 B.C. civil forfeiture case alleges drug money laundered in real estate; February 13, 2019 Cosmetics company allegedly connected to casino money laundering scheme, police say; March 15 2019 Investigation: Dozens of money transfer/exchange businesses operating out of Metro Vancouver condos, houses.
[169] April 3, 2019 Man arrested in money-laundering probe had stacks of $100 bills in his pocket, court documents say.

Jin;[170] RCMP arrests of alleged money launderers in Montreal and BC;[171] attempts at quantifying the extent of money laundering in BC;[172] and political friction between BC and Canada over information sharing.[173]

70. The collapse of the RCMP E-Pirate investigation[174] and another similar investigation[175] attracted significant media attention. As described above, the RCMP's E-Pirate investigation centred around Silver International Investment Ltd., which was alleged to have been laundering hundreds of millions of dollars a year in Richmond, BC.[176] The Crown laid charges on September 26, 2017, but proceedings were stayed on November 22, 2018, due, according to some news sources, to the RCMP's inadvertent disclosure of unredacted files to defence counsel.[177] The charges were reportedly stayed because the disclosure put a confidential informant at risk of serious harm.[178]

71. Other frequent topics of news reports included:

a. Money laundering as a driver of housing unaffordability;[179]

b. lack of transparency in BC and Toronto real estate;[180]

---

[170] February 3, 2020 $1.2M mortgage called on B.C. home allegedly tied to money laundering
[171] February 11, 2019 RCMP arrest 17 in alleged international money laundering scheme; February 12, 2019 RCMP says dismantled network laundered tens of millions in drug money; April 3, 2019 Man arrested in money-laundering probe had stacks of $100 bills in his pocket, court documents say;
[172] February 19, 2019 Size of money laundering problem in B.C. not clear; estimates in the billions
[173] January 18, 2019 B.C. minister fears money laundering involves billions of dollars, cites reports;
[174] November 28, 2018 David Eby won't rule out public inquiry after collapse of casino money-laundering case; December 17, 2018 Crown disclosure problems revealed in failed high-profile money laundering case;
January 9, 2019 EXCLUSIVE: Crown mistakenly exposed police informant, killing massive B.C. money laundering probe; March 22 2019 B.C. civil forfeiture office suing key target of province's biggest money laundering case
[175] January 16, 2019 REAL SCOOP: Second major organized crime case dropped
[176] October 18, 2019 E-Pirate money-laundering investigation: Leadership problems, missteps proved fatal.
[177] *Ibid*.
[178] January 9, 2019 EXCLUSIVE: Crown mistakenly exposed police informant, killing massive B.C. money laundering probe.
[179] February 19, 2019 Diane Francis: Money laundering by foreigners is what's really destroying housing affordability in Canada; April 2, 2019 Real estate experts blame government policies for dismal March home sales; April 24, 2019 How A Little Money Laundering Can Have A Big Impact On Real Estate Prices.
[180] March 21, 2019 Toronto's real-estate market risky for money laundering, with $28B in opaque investments: Report.

c. the announcement of reports on money laundering by Dr. German and the Expert Panel;[181]

d. calls for a public inquiry into money laundering, from BC mayors and the public;[182]

e. the release of a US State Department report which lists Canada as a "major money laundering jurisdiction;[183]

72. A timeline of events leading to the announcement of a public inquiry was provided by the Vancouver Sun.[184]

73. With much of the media reporting centring on the impact of overseas funds on BC real estate values, and allegations that some of BC's fentanyl supply originates in China,[185] some journalists have raised concerns about anti-Asian racism infiltrating BC's money laundering discourse, as well as conflation of disparate issues.[186] In particular, some of these journalists decry a failure to distinguish money laundering from the transfer of legitimately earned funds from overseas.[187]

---

[181] May 8, 2019 Money laundering funded $5.3B in B.C. real estate purchases in 2018, report reveals; May 8, 2019 BIV Talks: Expert panel on money laundering in B.C. with Dr. Peter German; May 9, 2019 Homemakers buying multiple homes, layers of shady mortgages and other signs of dirty money in B.C. real estate; May 9, 2019 Report finds $5B laundered through B.C. real estate in 2018; May 9, 2019 Money laundering drove up B.C. real estate prices by 5%: reports;

[182] January 21 2019 BCGEU, B.C.'s largest public-sector union, wants inquiry into money laundering, drugs; Febraury 24, 2019 B.C. mayors want inquiry into links between fentanyl, money laundering and real estate; February 27 2019 British Columbia's money laundering is an emergency. The public deserves an inquiry; May 13 2019 Rob Shaw: Attorney general wants to name names in a public inquiry on money laundering.

[183] April 2, 2019 U.S. deems Canada 'major money laundering country' as gangs exploit weak law enforcement; United Sates Department of State, "International Narcotics Control Strategy Report: Volume II - Money Laundering" (March 2020), online: <https://www.state.gov/wp-content/uploads/2020/03/Tab-2-INCSR-Vol-2-508.pdf>.

[184] May 15, 2019 Money laundering in B.C.: Timeline of how we got here.

[185] November 27, 2018 Fentanyl kings in Canada allegedly linked to powerful Chinese gang, the Big Circle Boys; December 1, 2018 China won't stop flood of fentanyl into Canada, sources say.

[186] July 5 2018 An open letter to Attorney General David Eby and investigator Peter German on B.C.'s Dirty Money report; May 25 2019 On David Eby's trail of embedded bombshells about money laundering; Dec 6 2019 Vancouver community organizer Kevin Huang on how the media is failing when it talks about 'China'; See also: July 11 2016 History shows racism has always been a part of Vancouver real estate.

[187] July 13th, 2016 Revisiting real estate, race, and how the foreign-buyers narrative came to dominate Vancouver media.

A. GOVERNMENT RESPONSE IN BC

74. Media reporting has also touched on the government's response to money laundering.

75. As might be expected, the volume of freedom of Information ("FOI") requests to the Government of BC for documents relating to "money laundering" have reflected the media attention described above, with one request in 2013, five requests in 2016, three requests in 2017, six requests in 2018, 24 requests in 2019, and six requests in 2020.[188]

76. In February 18, 2018, BC's Attorney General advised the government would introduce new measures to combat money laundering by lenders connected to the fentanyl trade.[189]

77. In April 2019, the Government of British Columbia announced the *Land Owner Transparency Act,*[190] which creates a public registry of beneficial owners of property in BC. The Act requires corporations, trusts and partnerships to disclose beneficial owners. The Government stated the Act would "help crack down on illegal activities" and prevent homes from being used for money laundering.[191]

78. On April 4, 2019, the Provincial Government announced that it would establish a new "BC Financial Services Authority", as a Crown agency, to replace the Financial Institutions Commission (*"FICOM") in regulating credit unions, insurance and trust companies, pensions, and mortgage brokers.[192] On November 12, 2019, in a statement that referenced the Real Estate Regulatory Structure Review authored by Dan Perrin, the Provincial Government announced that the Financial Services Authority would act as a single regulator of the real estate industry.[193] The government advised that it was targeting fall 2020 for the introduction of new legislation that would effect the change to the real estate industry.[194]

---

[188] https://www2.gov.bc.ca/gov/search?q=%22money+laundering%22&id=4BAD1D13C68243D1960FECBBF7B8B091&tab=1

[189] February 18, 2018 Globe investigation into money laundering in B.C. real estate will lead to new rules, AG says.

[190] April 2, 2019 B.C. introduces law to prevent money laundering, tax evasion in real estate.

[191] British Columbia, "News Release: New legislation makes BC global leader in ending hidden ownership," *BC Gov News* (April 2, 2019), online: <https://archive.news.gov.bc.ca/releases/news_releases_2017-2021/2019FIN0037-000545.htm>.

[192] Ministry of Finance, "New Crown agency will better protect people's financial interests," *BC Gov News* (April 4, 2019), online: <https://news.gov.bc.ca/releases/2019FIN0038-000573>.

[193] British Columbia, "News Release: Single real estate regulator protects people, combats money laundering," *BC Gov News* (November 12, 2019), online: <https://www.bcfsa.ca/pdf/news/News20191112.pdf

[194] *Ibid*.

79. In early 2019, the City of Vancouver announced it would cap cash payments at $10K to prevent money laundering.[195]

5. TERMS OF REFERENCE REPORTS

A. The First German Report: Dirty Money

80. Following the above noted media reports, on September 28, 2017, the Attorney General of British Columbia, David Eby, appointed Peter German, Q.C., to conduct an independent review of money laundering in BC's casinos.[196]

81. On March 31, 2018, Dr. German published the results of that review in his report, "Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia (the "First German Report")."[197]

82. The First German Report provided Dr. German's conclusions on the BC casino industry's vulnerabilities to money laundering, along with a series of recommendations to remedy those vulnerabilities. With respect to real estate, Dr. German stated that making recommendations on the real estate sector was outside his mandate, but he nonetheless provided comments.[198] His comments appeared to be predominantly informed by media reporting, statements by the RCMP, the Attorney General of BC, and other unidentified sources.[199] He concluded that real estate is vulnerable to criminal actors, and an important sector for money laundering. He placed particular emphasis on mechanisms available to conceal ownership in real estate.[200] The First German Report provided recommendations to government. At recommendation 45, Dr. German suggested the Province of BC "undertake research into allegations of organized crime penetration of the real estate industry."[201]

---

[195] February 1, 2019 City of Vancouver caps cash payments at $10K to prevent money laundering.
[196] Attorney General, "Independent expert appointed to review B.C. anti-money-laundering policy" *BC Gov News* (28 September 2017), online: <https://news.gov.bc.ca/releases/2017AG0025-001642>.
[197] Peter German, "Dirty Money: An independent review of money laundering in Lower Mainland casinos conducted for the Attorney General of British Columbia," (March 31, 2018), online: <https://news.gov.bc.ca/files/German_Gaming_Final_Report.pdf>.
[198] *Ibid,* at 213.
[199] *Ibid,* at 213-214.
[200] *Ibid,* at 214.
[201] *Ibid,* at 215.

83. The Province of BC acceded to Dr. German's recommendation, retaining him to conduct a further review of real estate and other industries.

B. The Perrin Report

84. On April 18, 2018, the Minister of Finance for BC, the Hon. Carole James, announced the commencement of a review into the regulatory structure of real estate in BC, led by Dan Perrin.[202]

85. On September 27, 2018, Mr. Perrin released his report, "Real Estate Regulatory Structure Review" (the "Perrin Report").[203] Perrin found there to be a structure of overlapping regulatory authorities which was inefficient, duplicative, and oftentimes confusing for industry as well as the regulators themselves.

86. Dr. Perrin provided an overview of the history of regulatory structure of real estate in BC. In 2004, four of the Council's board members became government appointments (the remainder being elected by licensees). In 2016, following the publication of the report of the Independent Advisory Panel, then premier Christie Clarke announced that the self-regulation of the industry was at an end. This decision led to a bifurcated model with the Council handling licensing and discipline and the revived Office of the Superintendent of Real Estate ("the Superintendent") responsible for unlicensed real estate conduct and oversight of the *Real Estate Development and Marketing Act*, as well as oversight of the Real Estate Council of BC. To effect the end of self-regulation, 100% of the Council's board member positions became government-appointed positions.[204]

87. Mr. Perrin found that the 2016 changes led to significant tension between the Office of the Superintendent of Real Estate and the Real Estate Council of BC.[205] Lack of clarity on the overlapping roles of the Superintendent and Council engendered jurisdiction disputes, and the

---

[202] Ministry of Finance, "Review of real estate regulators to strengthen protections," *BC Gov News* (April 18 2018), online: <https://news.gov.bc.ca/releases/2018FIN0014-000654>
[203] Ministry of Finance, Ministry of Attorney General, "Province launches probe into dirty money in real estate," *BC Gov News* (September 28 2018), online: <https://archive.news.gov.bc.ca/releases/news_releases_2017-2021/2018FIN0072-001884.htm>.
[204] Dan Perrin, "Real Estate Regulatory Structure Review," (2018), online: <https://cullencommission.ca/files/Real_Estate_Regulatory_Structure_Review_Report_2018.pdf>, at 9-11.
[205] *Ibid,* at 19.

lack of industry expertise amongst the Council's new government-appointed board members noticeably slowed the processing of complaints.[206]

88. In light of these findings, Mr. Perrin recommended the Provincial government implement a single (not self-regulating) regulator. He recommended dividing responsibilities such that government be responsible for public policy development, in concert with the regulator, while the regulator be responsible for administrative policy to implement the government's public policy.[207]

C. The Maloney Report

89. On September 28, 2018, the Minister of Finance for BC, the Hon. Carole James, appointed Professor Maureen Maloney to chair an Expert Panel on Money Laundering in Real Estate (the "Expert Panel").[208]

90. On March 31, 2019, Professor Maloney and her co-authors Professor Tsur Somerville and Professor Brigitte Unger announced the release of the Expert Panel's report, "Combatting Money Laundering in BC Real Estate" (the "Maloney Report").[209] The Expert Panel's conclusions included :[210]

a. money laundering in BC real estate was contributing to housing prices and to BC's housing affordability crisis, with an estimated impact of a 5% increase on housing prices;

b. more provincial regulatory responses to money laundering are necessary;

c. data sets in BC should be linked in order to facilitate analysis of potential money laundering, and to better understanding of characteristics of money laundering;

---

[206] *Ibid,* at 21.
[207] *Ibid,* at 26.
[208] September 28, 2018 B.C. launches money laundering reviews into real estate, horse racing, luxury cars.
[209] May 8, 2019 Money laundering funded $5.3B in B.C. real estate purchases in 2018, report reveals.
[210] Maureen Maloney, Tsur Somerville, & Brigitte Unger, "Combatting money laundering in BC real estate," (March 31, 2019), online: <https://cullencommission.ca/files/Combatting_Money_Laundering_Report.pdf> ("Maloney et al."), at 1-4.

d. disclosure of beneficial ownership is the single most important measure to combat money laundering, and the *Land Owner Transparency Act*[211] appears to be compliant with best practices in this regard;

e. financial and real estate regulators currently do not have an anti-money laundering mandate, which is an untapped resource that could be used to more effectively combat money laundering;

f. the federal government should provide guidance and feedback to those responsible for issuing suspicious transaction reports, including regulators;

g. the federal government should collect and report statistics on anti-money laundering efforts and their effectiveness.

91. The report went on to make 29 recommendations to enhance the Province's ability to combat money laundering.

D. The Second German Report: "Dirty Money 2"

92. On March 31, 2019, the same day that the Maloney Report was released, Dr. German published his second report, "Dirty Money – Part 2: Turning the Tide – An Independent Review of Money Laundering in B.C. Real Estate, Luxury Vehicle Sales & Horse Racing" (the "Second German Report").[212]

93. Echoing the recommendations of the Expert Panel, Dr. German pointed to the problem of "opaque ownership structures [which] allow criminals to remain anonymous and provide a veil with which to conceal money laundering activity in real estate."[213] Dr. German concluded that investigation of foreign ownership of real estate is stymied by the lack of verification or validation of ownership data maintained in BC's land title system. The Expert Panel highlighted this issue as well, noting in particular that data on foreign ownership of real estate kept by Statistics Canada

[211] *Land Owner Transparency Act*, SBC 2019, c 23.
[212] Attorney General, "Review finds zero dedicated federal anti-money laundering police officers working in B.C.", *BC Gov News* (8 April 2019), online: <https://news.gov.bc.ca/releases/2019AG0031-000599>; Attorney General, "Second German report finds money laundering in B.C. luxury car market," *BC Gov News* (8 April 2019), online: <https://news.gov.bc.ca/releases/2019AG0042-000885>
[213] Second German Report, p. 13

varied significantly from data kept by the LTSA.[214] The Expert Panel stated that they had intended to conduct some tabulations of red flag indicators generated by FATF using LTSA data, but due to this problem in data, they were unable to "reliably use" the red flag indicator of foreign ownership.[215] Dr. German also pointed to problems with the structure of the provincial real estate data that does exist, highlighting a lack of machine-readability and an overreliance on freeform data entry rather than prepopulated lists of appropriate options.[216]

94. Dr. German reiterated the Expert Panel's call for a beneficial ownership registry, but went further than the Expert Panel: he suggested the registry record not just beneficial ownership, but also the sources of funds used to purchase real estate.[217] He also recommended that provincial real estate databases, such as the Land Title Survey Authority ("LTSA"), be tasked with conducting anti-money laundering screening.[218]

95. Additionally, Dr. German commented on money laundering vulnerabilities associated with private lending, noting that mortgages from unregulated lenders featured disproportionately in the analysis of other known indicators of money-laundering in real estate.[219]

E. The Commission of Inquiry into Money Laundering

96. On May 15, 2019, in the wake of these four reports, British Columbia Premier John Horgan announced the establishment of this Commission of Inquiry into Money Laundering in British Columbia ("the Commission"). In announcing the Commission, the Attorney General for BC, David Eby, stated:

> This inquiry will bring answers about who knew what when and who is profiting from money laundering in our province. The Honourable Justice Cullen will have the mandate, authority and resources to seek answers, perhaps most importantly

[214] Maloney et al., *supra* note 206, at 59.
[215] *Ibid.*
[216] Peter German, "Dirty money - part 2: Turning the tide - an independent review of money laundering in BC real estate, luxury vehicles & horse racing," (May 31, 2019), online; <https://cullencommission.ca/files/Dirty_Money_Report_Part_2.pdf>, at 14.
[217] *Ibid.*
[218] *Ibid.*
[219] *Ibid*, at 13.

among people and organizations who refuse to share what they know unless legally compelled to do so.[220]

PART 2: THE RESPONSE

6. REAL ESTATE COUNCIL OF BC

97. Beginning April 1, 2020, renewal of a real estate license under the *Real Estate Services Act*[221] will require licensees to complete the course, "Anti-Money Laundering in Real Estate."[222] The course was designed and offered by the Real Estate Council of BC, and aims:

> to give you the tools and knowledge you need to help prevent illicit funds from entering our real estate markets. By staying current and informed on anti-money laundering requirements and best practices, you can ensure that consumers are well-protected, and that the public can have confidence in BC's real estate industry.

98. The media also reported on the introduction of this course.[223]

7. RESPONSES FROM REALTORS

A. BC Real Estate Association

99. A full list of the BCREA's efforts with respect to anti-money laundering is here.

---

[220] Office of the Premier, "Government to hold public inquiry into money laundering" *BC Gov News* (15 May 2019), online: <https://news.gov.bc.ca/releases/2019PREM0052-000958>.
[221] *Real Estate Services Act*, SBC 2004, c 42.
[222] **Appendix 12**, Real Estate Council of BC, *Anti-Money Laundering in Real Estate* (April 1, 2020), online: <https://www.recbc.ca/professionals/licensing/continuing-education/anti-money-laundering-real-estate>.
[223] January 10, 2020 Mandatory anti-money laundering course rolls out for B.C. realtors.

100. On September 1, 2018, BCREA announced that it had launched a new action plan "to support REALTORS® and managing brokers in better understanding and meeting their FINTRAC reporting duties to help keep the proceeds of organized crime out of the housing market."[224] BCREA stated its plan to gather information about PCMLTFA compliance deficits, and to use that information to develop training for real estate agents, and to educate local media.

101. On November 1, 2018, BCREA published an article outlining the regulations that BC real estate agents are required to comply with, including FINTRAC reporting.[225]

102. On November 27, 2018, BCREA stated its concern regarding recent media reports about money laundering in BC.[226] BCREA stated that "In July, BCREA learned that BC brokerages and REALTORS® were having trouble understanding and meeting their reporting duties to [FINTRAC]." The report outlined the steps BCREA had taken, including a managing broker conference, updating its course on FINTRAC reporting, creating new communication, consulting with government, and encouraging real estate agents and the public to participate in the Expert Panel on Money Laundering in Real Estate investigation.

103. In December 2018, BCREA released an infographic entitled "The Role of REALTORS ® in Helping the Government Stop Money Laundering."[227] The infographic presents a series of "fact or fiction" scenarios on the interplay between real estate agents and money laundering. It advises that real estate agents are committed to stopping money laundering, including by reporting to FINTRAC, and have compliance programs to prevent money laundering. It explains that FINTRAC does not follow up with a real estate agent who has reported a transaction, nor will it stop transactions that have been reported. Additionally, the infographic states, "the only funds REALTORS® ever receive from buyers is the deposit and the majority of BC's real estate brokerages will only accept bank drafts to protect their brokerage from criminal exploitation."

---

[224] **Appendix 13**, April van Ert, *BCREA Launches FINTRAC Action Plan,* (1 September 2018), online: <https://www.bcrea.bc.ca/advocacy/bcrea-launches-fintrac-action-plan/>
[225] **Appendix 14**, Matt Mayers, *Real Estate Transparency to Build Public Confidence*, (1 November 2018), online: <https://www.bcrea.bc.ca/advocacy/real-estate-transparency-to-build-public-confidence/>
[226] **Appendix 15**, April van Ert, *BCREA Supports BC Government's Money Laundering Investigations*, (27 November 2018), online: <https://www.bcrea.bc.ca/news-releases/bcrea-supports-bc-governments-money-laundering-investigations/>
[227] **Appendix 16**, BCREA, *The Role of REALTORS® in Helping the Government Stop Money Laundering,* (December 2018), online: <https://www.bcrea.bc.ca/wp-content/uploads/2018-12moneylaunderinginfographic-1.pdf>

104. On January 16, 2019, BCREA released responses from FINTRAC to questions posed at a recent Conference for Managing Brokers.[228] Questions included why FINTRAC was focusing on real estate agents instead of banks, how to structure a compliance program in the face of deviation in expectations between FINRAC examiners, why FINTRAC was discouraging reliance on CREA compliance guidelines.

105. On February 13, 2019, BCREA announced that it had commissioned Deloitte to study residential and commercial real estate transactions to identify money laundering vulnerabilities, and would be providing this analysis to the Expert Panel on Money Laundering.[229] BCREA also stated it was working to dispel misconceptions about real estate agents and money laundering, while also helping real estate agents understand and meet their compliance duties.

106. On February 22, 2019, Deloitte submitted its analysis to the Expert Panel.[230] Its key findings were:

a. That there is a difference in the perceived available information compared to the actual information available to the real estate agent during a transaction with respect to identifying potential money laundering and/or terrorist financing. As a result, some real estate agents disagree with the legislative AML responsibilities of the real estate agent.

b. There continues to be a perception by real estate agents that because they generally do not handle cash, they are therefore not exposed to money laundering, however, the real estate agent's knowledge of the client purchasing or selling real estate is a crucial piece of information to the real estate transactions process, as it is information that is generally not available to other parties to the real estate process.

c. The brokerage's compliance officer relies heavily on real estate agents to fulfill the Know-Your-Client requirements, including the client risk rating and ongoing monitoring in order to meet the AML requirements. In other AML-regulated

[228] **Appendix 17**, Marianne Brimmell, *Getting to the Bottom of FINTRAC Compliance* (16 January 2019), online: <https://www.bcrea.bc.ca/advocacy/getting-to-the-bottom-of-fintrac-compliance/>
[229] **Appendix 18**, BCREA, *Understanding Money Laundering Vulnerabilities,* (13 February 2019), online: <https://www.bcrea.bc.ca/bcrea/understanding-money-laundering-vulnerabilities/>
[230] **Appendix 19**, Deloitte & Touche presentation to BCREA, *Assessing Money Laundering Vulnerabilities in the BC Real Estate Sector*, (22 February 2019)

industries, such as banking or securities, the client risk rating and ongoing monitoring are performed centrally and/or managed by the compliance officer to ensure a consistent approach across the organization.

d. With respect to the 'cost' of transacting with a potential money launderer or criminal, real estate agents that operated in a "community-based" brokerage were generally more concerned about damaging their personal reputation.

107. On March 4, 2019, BCREA made submissions to both the Expert Panel on Money Laundering and Dr. German's money laundering reviews.[231] These submissions paraphrased a selection of the findings and recommendations of the Deloitte Vulnerability Assessment and stated that BCREA would be undertaking education and training. BCREA also stated that it committed to working towards the following best practices:

a. Brokerages avoid accepting cash deposits aside from exceptional circumstances.

b. Educating brokerages so they can accurately and effectively report suspicious transactions, according to AML legislation.

c. Brokerages engage outside, independent professionals to conduct their two-year reviews.

d. Compliance officers participate in AML knowledge sessions, such as the Association of Certified Anti-Money Laundering Specialists.

108. BCREA disputed the following Deloitte recommendations (BCREA disputation follows the original Deloitte recommendation):

a. Where possible, the roles of managing broker and FINTRAC compliance officer should be clearly defined and separated, and the role of compliance officer expanded to include managing the brokerage's inherent risk for money laundering and terrorist financing rather than simply ensuring regulatory compliance. Part of the expansion of the compliance officer role should also include centralizing the

[231] **Appendix 20**, Darlene Hyde, "Letter to Expert Panel on Money Laundering, RE: British Columbia Real Estate Association submission to Expert Panel," *BCREA* (4 March 2019) online: <https://www.bcrea.bc.ca/wp-content/uploads/2019-03-04-submission-to-expert-panel-on-money-laundering.pdf>

ongoing monitoring and client risk rating responsibilities and enhancing processes for documentation and review.

Upon BCREA review, feedback from multiple real estate boards across the province challenged this finding as impractical as a "best practice". The added cost and complexity would not be workable for many brokerages, who already devote significant resources toward complying with an array of legislation at all levels of government.

b. Brokerages monitor past real estate transactions for known or alleged criminal activity and consider submitting suspicious transaction reports.

BCREA board feedback challenged this finding as impractical and as setting an expectation that cannot be met. If suspicion wasn't raised at the time of the original transaction, it is unlikely a review in the aftermath would yield any new findings.

109. BCREA also made four regulatory recommendations, including incorporating lawyers into the PCMLTFA, ensuring better consistency in FINTRAC examinations, better FINTRAC outreach to industry, and public reporting that represents the results of FINTRAC examinations, clarification of the AML role of real estate agents, including by way of Real Estate Council licensing, and more coordination between provincial and federal governments.

110. On April 15, 2019, BCREA, alongside the Appraisal Institute of Canada – BC Association, the BC Notaries, the Canadian Mortgage Brokers Association-BC, and the Real Estate Board of Greater Vancouver, released a set of joint anti-money laundering recommendations.[232] These recommendations were: 1) Accept only verified funds; 2) mandatory anti-money laundering education; 3) Smart regulation (including providing FINTRAC disclosure to BC Securities Commission and FICOM, now the BC Financial Services Agency, and coordinated action between the Federal and Provincial governments); 4) Ongoing engagement (between FINTRAC/other regulators and industry); and 5) timely and transparent reporting.

[232] **Appendix 21**, Darlene Hyde, Christina Dhesi, Jacqui Mendes, Samantha Gale, and Brad Scott, *BC Real Estate Sector Submits Anti-Money Laundering Recommendations To Government* (15 April 2019), online: https://www.bcrea.bc.ca/news-releases/bc-real-estate-sector-submits-anti-money-laundering-recommendations-to-government/;

111. On April 29, 2020, BCREA responded to the consultation on a corporate transparency register.[233] BCREA urged government use the existing corporate registry, without any additional fees, and urged government to be flexible, and avoid a "heavy-handed approach" to enforcement. BCREA also urged synchronization between the Land Owner Transparency Registry and a corporate beneficial ownership registry, as well as the partnership and any future trust register. BC requested government articulate clear minimum information thresholds, and take a "reactive approach" to verifying the accuracy of information: "By that we mean that the government only takes steps to verify information when alerted by another party that information might be incorrect."

112. In May, 2019, BCREA published an eBulletin entitled "Anti-Money Laundering: Opportunities for action."[234] The bulletin announced the commencement of a public inquiry into money laundering, referring to money laundering as a "media favourite" since the publication of reports by Peter German and the Expert Panel on Money Laundering in BC Real Estate. The bulletin detailed BCREA's efforts in relation to anti-money laundering, including: participating in the work of Dr. German and the Expert Panel; commissioning a vulnerability assessment of residential and commercial transactions, and collaborating with real estate actors on a statement of best AML practices and recommendations. The bulletin highlighted some of the recommendations made by the Expert Panel, and concluded with a statement of optimism regarding improvement of the system to keep proceeds of crime out of real estate, while warning that such changes may take a long time.

113. On December 5, 2019, the BCREA announced that it was developing an array of new resources with respect to anti-money laundering, such as infographics, podcasts, FAQ's, and training workshops.[235]

---

[233] **Appendix 22**, Darlene Hyde, Letter to Ministry of Finance RE: BC Consultation on a Public Beneficial Ownership Registry, dated April 29, 2020, online: < https://www.bcrea.bc.ca/wp-content/uploads/2020-04-29-Ministry-of-Finance-beneficial-corporate-ownership-registry.pdf>; see also **Appendix 23**, accompanying backgrounder (15 April 2019), online: <https://www.bcrea.bc.ca/wp-content/uploads/2019-04-15-backgrounder-to-the-real-estate-sector-anti-money-laundering-statement.pdf>

[234] **Appendix 24**, BCREA, "Anti-Money Laundering," *eBulletin* (May 2019), online: <https://web.bcrea.bc.ca/ebulletin/articles/2019-05_article1.html>

[235] **Appendix 25**, BCREA, *New Anti-Money Laundering Initiatives in Development,* (5 December 2019), online: <https://www.bcrea.bc.ca/advocacy/new-anti-money-laundering-initiatives-in-development/>

114. On August 13, 2020, BCREA launched a nine-week training program for managing brokers and compliance officers to improve their compliance programs and meet their anti-money laundering requirements.[236]

115. On August 13, 2020, BCREA wrote to BC Minister of Finance about the Land Owner Transparency Registry to request that where a person has applied to have their information withheld from public search, the registry display the fact that a property does have a beneficial owner.

116. On September 3, 2020, the BCREA released the article "Signs you should file a Suspicious Transaction Report."[237] The article identified markers such as using a nominee, purchasing property in the name of someone whose financial resources don't seem to align with the price of the property, investment property purchases by a non-resident, lack of concern with the property's price or condition, quick resale, payment of deposit by a third party, or financing from an unusual source.

117. On September 25, 2020, BCREA compiled its activity on money laundering into a user-friendly list.[238]

B. Local Real Estate Boards

i. The Function of Local Real Estate Boards

118. The BCREA represents all 11 real estate boards in British Columbia.[239] In winter 2019-2020, Commission Counsel spoke to each of these local real estate boards about their experience

---

[236] **Appendix 26**, Marianne Brimmell, *Get ready for mastering compliance: Anti-money Laundering Training for Brokers*, (13 August 2020), online: <https://bcreabeta.opacity.design/education/mastering-compliance-anti-money-laundering-training-for-brokers/>; see also **Appendix 27**, BCREA, *Mastering Compliance: Anti-Money Laundering Training for Brokers Program*, online: <https://www.bcrea.bc.ca/course-summary/Mastering-Compliance-Anti-Money-Laundering-Training-for-Brokers-Program/>

[237] **Appendix 28**, April van Ert, *Signs You Should File a Suspicious Transaction Report*, (3 September 2020), online: <https://bcreabeta.opacity.design/practice-tips/signs-you-should-file-a-suspicious-transaction-report/>

[238] **Appendix 29**, Marianne Brimmell, *Anti-Money Laundering Resources*, (25 September 2020), online: <https://www.bcrea.bc.ca/advocacy/anti-money-laundering-resources/>

[239] The local real estate boards ("REB's") are: BC Northern REB, Chilliwack and District REB, Fraser Valley REB, Kamloops & District Real Estate Association, Kootenay Association of REALTORS, Okanagan Mainline REB, Powell River Sunshine Coast REB, REB of Greater Vancouver, South

with anti-money laundering regulation. Much of the feedback received reflected experiences shared by all boards.

119. These 11 real estate boards are professional associations that operate under the provisions of the Societies Act of BC. The boards explained their role in the industry as providing primarily advocacy, education, and management of the local Multiple Listing Service® system. The boards require members to abide by the Canadian Real Estate Association's REALTOR® code. Some boards have their own unique code of conduct with rules and regulations that go beyond the REALTOR® code, CREA or BCREA expectations, or Real Estate Council of BC standards. Most boards accept complaints; most accept only member-to-member complaints, but some also accept complaints from the public.

ii. Complaints

120. All boards reported that they had never received a complaint with a money laundering dimension to it. All boards were aware of, and most were very concerned about, the media reporting on the connections between money laundering and real estate, and the public perception that real estate agents might be complicit. Boards provided the feedback below in response to these concerns.

iii. The Multiple Listing Service®

121. The Multiple Listing Service® ("MLS®") is the method by which most residential properties are listed for sale in BC. Each of the 11 local REBs manages their own MLS® system (though some boards share responsibilities). Across the province, posting a listing to MLS® requires the poster to have reviewed an active title search, and if the selling party is a corporation, a corporate search (and sometime copies of corporate bylaws) that demonstrates the real estate agent is liaising with an individual who has capacity to bind the corporation.

iv. FINTRAC Education

122. All boards expressed a desire for clearer, simpler, more user-friendly guidance from FINTRAC. Many expressed the view that most real estate agents and brokers, and indeed most members of the boards, were unfamiliar with how money laundering could be occurring in real

Okanagan REB, Vancouver Island REB, and Victoria REB. Not all real estate licensees in BC are members of a real estate board.

estate.[240] Some stated that their board prohibited the use of cash for deposits. Many boards repeated that true physical cash transactions were not possible in their jurisdictions, and expressed the view that if no cash was changing hands within the real estate transaction, the transaction must not be money laundering. Other boards noted that the amount of funds overseen by real estate agents (the deposit) is very small relative to the overall transaction, and therefore considered the scrutiny on real estate agents misplaced, because discerning the potential for money laundering would be extremely difficult or impossible for a real estate agent.

123. One board mentioned that most real estate agents believed that real estate agents were being targeted because the transfer of deposits were the main source of money laundering, and only very recently has FINTRAC provided targeted education to real estate agents to dispel this belief and spread information about the role of real estate agents in disrupting the wider web of money laundering. Most boards expressed a desire for better understanding of how money laundering might be entering the real estate sector in the absence of cash transactions.

124. Several boards had feedback on the existing FINTRAC guidance, considering it excessively long, complicated, and theoretical, and that its applicability to the on-the-ground experience of real estate agents and brokers was too opaque. All boards noted significant frustration from members who were struggling to understand their obligations and who did not find the FINTRAC guidance illuminating.

125. Several boards emphasized that most real estate agents and brokers are small businesspeople, not compliance experts. There was a concern that real estate agents lack the background or resources to digest and apply the FINTRAC guidance in its current state. Certain board members with prior experience in the financial industry described the discrepancy between financial institution compliance officers, who are trained and employed as specialists in compliance matters, including anti-money laundering, and real estate agents/brokers who are trained and employed as salespeople, with a specialty in property sales. Those board members suggested this discrepancy was responsible for the friction between FINTRAC and the real estate industry. All boards stressed a need for more accessible content.

126. Multiple boards commented that they had noticed an improvement in FINTRAC's availability, guidance, and presence at conferences in 2019. Some boards mentioned specific presentations they found very useful and enlightening – these were instances in which FINTRAC

[240] Boards pointed to several resources which they shared with their members, see **Appendix 30**.

representatives or compliance experts attended in person to describe the myriad ways in which money laundering may infiltrate the real estate market. The boards that had attended these events stated that after the event, members expressed a much better understanding of the purpose behind the FINTRAC reporting and real estate agents' role in monitoring transactions. Several boards were also enthusiastic about the prospect of clarity from the Real Estate Council's (forthcoming, at that time) anti-money laundering course.

v. FINTRAC Reporting

127. With respect to reporting to FINTRAC, any boards expressed a desire for standardized forms, or a more user-friendly system to submit FINTRAC reports, such as an app, and expressed frustration with FINTRAC's refusal to endorse draft forms proposed by the Canadian Real Estate Association.

128. There was much confusion over what would constitute a "suspicious" transaction amongst boards. Those with jurisdiction in the Lower Mainland commented that an oft-cited example, a student with no obvious source of income purchasing a million dollar property, would often not be out of the ordinary, and the student might explain that funds were from parents, or the transaction was subject to financing. One noted that BCREA stats (reportedly from FINTRAC) concluded 70% of BC real estate agents were "not compliant" with reporting obligations, and the board member suggested that this high number was unlikely to reflect "bad apples"; more likely this figure reflects a lack of uptake by real estate agents, which, they said, reflects poorly on FINTRAC as much as real estate agents.

129. Others identified concern regarding reporting a longstanding client without being certain wrongdoing was occurring, and potentially causing harm to that client.

130. Several boards stated that despite years of reporting, they were not aware of any real estate STR that had led to the discovery of money laundering, or led to a money laundering conviction, and thus they had difficulty seeing the utility in reporting. However, contrary to this view, other boards expressed a recognition of the importance of reporting to FINTRAC, as a transaction may not appear "suspicious" until "pieces of the puzzle" from various sectors were reviewed in tandem. Some board representatives expressed a desire for clear demarcation of the features that real estate agents should consider "suspicious," to avoid variation in interpretation by different real estate agents.

131. Several expressed desire for better responsiveness on the part of FINTRAC. One board commented that there had been a significant improvement in 2019, in which queries were responded to in 1-2 days, instead of a typical multiple day lag time in preceding years. Still, that board commented that with the speed of real estate transactions expected by clients, a response time in hours would be more useful.

vi. FINTRAC Audits

132. Another oft-repeated perspective was that FINTRAC's expectations for compliance, as expressed during an audit, are vague, and always in flux, such that "the goalposts are always moving." Many expressed concern at the lack of standardization across FINTRAC examiners, with the same behaviour leading to reprobation from FINTRAC at an audit of one brokerage but not another. Several commented that there was a discrepancy between the FINTRAC educational guidance and the feedback received from auditors.

133. Almost all boards commented that FINTRAC audits seemed excessively focused on "bureaucratic trivia," i.e. compliance with minutiae of FINTRAC reporting standards, such as the requirement to refrain from using abbreviations for province names or identification types. Many expressed the view that the FINTRAC audit process failed to educate brokerages on how to improve their anti-money laundering system or reporting process beyond these minutiae. Several lamented the poor messaging during the audit process and expressed a desire for FINTRAC to provide more education as part of the audit.

vii. Special Concerns

134. Rural real estate boards expressed concern about the lack of resources available to their specific circumstances. Some of these boards stated a desire for better education as to how money laundering might be occurring outside the concerns typically associated with money laundering in the media, such as housing affordability and scarcity, speculation, and very expensive homes.

135. An additional concern raised by many boards was the discrepancy between FINTRAC's expectations of the industry, and the regulatory history and overall culture of the industry. Several pointed to how FINTRAC requirements were perceived as invasive or contrary to privacy. Some suggested that the ambiguity currently present in FINTRAC guidance would necessarily lead to an uneven application in practice and pointed to instances in which clients have moved to real estate agents that ask fewer questions that encroach on client privacy (though other boards

suggested this concern is overhyped, and may simply be speculation). Several boards reported being aware of instances in which clients expressed concern about the intrusiveness of FINTRAC forms.

8. RESPONSE FROM MORTGAGE BROKERS

136. On February 20, 2018, the Canadian Mortgage Brokers Association – BC (CMBA-BC) published a news release responding to statements by Attorney-General David Eby that he intended to close loopholes in mortgage lending, in connection with a Globe & Mail story on money laundering in the real estate sector in BC.[241] CMBA-BC stated there were "no loopholes to close," but suggested rather that the government should increase enforcement against unlicensed lending activity. CMBA-BC suggested existing legislation was sufficient to enable government to require more robust financial reporting for licensees and pointed to regulation of mortgage investment corporations and syndicators by the Securities Commission.

137. On March 21, 2019, CMBA-BC made submissions to the Expert Panel on Money Laundering.[242] CMBA-BC recommended introduction of mandatory AML education, creation of a new licensee role for compliance oversight, and better articulation of the definition of "mortgage broker" in the *Mortgage Broker Act* in light of *AZTA Management v. Croft Agencies Ltd.*, 2014 BCSC 1462. CMBA-BC also pointed to a need for clarity for bank employees who broker third party mortgages, for whom the legislation appears to create requirements, but which requirements are neither followed nor enforced.

138. The Mortgage Brokers Institute of British Columbia (MBIBC) currently offers an Anti Money Laundering course which seeks to educate mortgage brokers on what money laundering is, how to recognize it, and how to avoid participating in transactions that may be related to money laundering.[243]

---

[241] **Appendix 31**, Samantha Gale, "Mortgage Brokers Association recommends stronger enforcement of existing regulations to control use of mortgages for money laundering" *CMBA-BC* (February 20, 2018), <online: http://www.mbabc.ca/wp-content/uploads/2013/02/CMBA-Money-Laundering-News-Release.pdf>.

[242] **Appendix 32**, Samantha Gale, "Letter to Expert Panel on Money Laundering re Submissions from the Canadian Mortgage Brokers Association-BC," (March 21, 2019), online: <https://www.cmbabc.ca/wp-content/uploads/2019/03/Anti-Money-Laundering-Submission-from-CMBA-BC-2019-03-21.pdf>.

[243] **Appendix 33**, Mortgage Brokers Institute of BC, *Available Courses*, online: <https://www.mbibc.ca/available-courses/>

139. The MBIBC has also sought BC FSA approval for its periodical "Regulatory Update" course, the content of which, for 2020 onwards, includes recent instances of mortgage broker misconduct that may touch on money laundering.[244]

140. The CMBA-BC has previously held several events with AML education, including:

a. February 14, 2019: "Dialed-In with CMBA-BC: FINTRAC reporting" a roundtable discussion to discuss money laundering risks and solutions;[245]

b. April 4, 2019: "Taking Action Against Money Laundering" as part of the CMBA-BC's Expert Speaker Series, a presentation on the role of policy makers in mitigating money laundering, including recommendations for best practices made by industry groups;[246] and

c. May 30, 2019: "An Update on BC Anti Money Laundering Policies," a presentation overview of the Dr. German and Expert Panel reports on money laundering, as part of the CMBA-BC Expert Speaker Series.[247]

141. In response to the Ministry of Finance's consultation on the *Mortgage Brokers Act*, in March-April 2020 CMBA-BC submitted eight briefing notes on various aspects of the Act. One of these briefing notes[248] cites a lack of independence and impartiality of the adjudication process, and recommends that an investigation into mortgage broker conduct be submitted to a panel of lawyers, licensees, and other industry experts to resolve. CMBA-BC suggests use of an independent panel would instil confidence by both industry and public, and stated:

142. Efforts to fight money laundering will be challenged when industry members do not have faith in the fairness and impartiality of a regulator – they may adopt an "us vs them" approach filled with distrust and extreme caution.[249]

---

[244] *Ibid.*
[245] **Appendix 34**, CMBA-BC, *Dialed-In with CMBA-BC: FINTRAC reporting*, (February 14, 2019), online: <https://www.cmbabc.ca/event/dialed-in-with-cmba-bc-fintrac-reporting/>.
[246] **Appendix 35**, CMBA-BC, *Taking Action Against Money Laundering*, (April 4, 2019), online: <https://www.cmbabc.ca/event/expert-speaker-series-april-4-2019/>.
[247] **Appendix 36**, CMBA-BC, *An Update on BC Anti Money Laundering Policies* (May 30, 2019), online: <https://www.cmbabc.ca/event/expert-speaker-series-vancouver-may-30-2019/>.
[248] **Appendix 37**. Samantha Gale, "Briefing Note: Mortgage Brokers Act Consultation: Independence in the Adjudication Process," *CMBA-BC*, (April 20, 2020).
[249] *Ibid,* at 3.

APPENDIX 30

AML Resources identified by Local Real Estate Boards

Boards flagged the following resources available to real estate agents for education on the topic of money laundering in real estate:

1. Canadian Real Estate Association sources. Members have access to resources through CREA Education Hub on REALTORLink. There is a page dedicated to FINTRAC within the portal and it includes:
    a. FINTRAC FAQ document, titled “FINTRAC Information for REALTOR® Members”;
    b. Template FINTRAC documents:
        1. FINTRAC - Receipt of Funds Record;
        2. FINTRAC - Office Policy Template;
        3. FINTRAC - Template Consent Letter;
        4. FINTRAC - Risk Assessment Form;
        5. FINTRAC - Individual Identification Information Record;
        6. FINTRAC - Identification Mandatory/Agent Agreement;
        7. FINTRAC - Corporation/Entity Identification Information Record;
    c. names of companies that offer anti-money laundering services to real estate professionals;
2. CREA-created courses, including:
    a. Introduction to Canada’s FINTRAC Regime;
    b. CREA Lite M3: Legal.
3. BCREA’s resources, including:

a. FINTRAC: Compliance for REALTORS®, Brokers and Broker Managers;

b. FINTRAC presentation at BCREA Advocacy Exchange: Conference for Managing Brokers, held September 19th, 2018;

4. FINTRAC:

a. FINTRAC's webpage;

b. FINTRAC's online webinar (http://video.isilive.ca/fintrac/2016-03-21.html);

5. Newsletters repeating information from 3rd party sources.

Appendix 1

FATF – *Money Laundering & Terrorist Financing Through the Real Estate Sector* – June 29, 2007

Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING THROUGH THE REAL ESTATE SECTOR

29 June 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Various reports produced by the FATF over the last few years have made reference to the fact that the real-estate sector may be one of the many vehicles used by criminal organisations to launder their illicitly obtained money.[1] The general objective of this report is to develop more information on this issue and present a clearer picture of the way that real estate activity can be used for money laundering or terrorist financing.

2. The study aims to accomplish two primary goals: First, it explores the means by which illicit money is channelled through the real-estate sector to be integrated into the legal economy. Second, it identifies some of the control points that could assist in combating this phenomenon. One of the most effective ways to understand how the sector is abused is to examine concrete case studies; therefore, the report is based primarily on information provided by participating FATF and non-FATF members.

3. Several characteristics of the real estate sector make it attractive for potential misuse by money launderers or terrorist financiers. The report outlines the reasons for this. From the case examples provided during the research for this project, several basic techniques were identified, such as the use of complex loans or credit finance, the use of non-financial professionals, the use of corporate vehicles and so on. The report briefly describes these techniques, followed by one or more most striking case examples. To reach out to the private sector, part of the research has been to develop a basic list of risk indicators from the case examples. These indicators may assist financial institutions and others involved in certain types of real estate activities in customer due diligence and in performing a risk analyses on new and existing clients.

4. The project identified three areas that seem especially vulnerable for misuse in money laundering schemes involving real estate and thus suitable for further consideration. In almost all case examples provided, wire transfers to channel the money have been involved at some stage. Also emerging markets seem to be more vulnerable to misuse of the real estate sector. Due to the worldwide market growth of real estate-backed securities and the development of property investment funds, the range of options for real estate investments has also grown. This effect has not gone without notice in emerging markets. Money laundering transactions can be easily camouflaged in genuine commercial transactions among the huge number of real estate transactions taking place. Complicating matter is the fact that often these less developed economies do not have an average market price for real estate, but rather prices varying across sectors and districts. To complete real estate transactions in some stage of the process involvement of legal expert is inevitable. The case examples have shown this category, when not covered by AML/CFT obligations, often becomes the weakest link in the process.

[1] This report is the product of research carried out by a project team operating under the umbrella of the FATF typologies initiative. The FATF project team was led by Spain and the Netherlands with the participation of Australia, Belgium, Canada, Japan, Lebanon, Luxembourg, Mexico, Myanmar, Norway, Pakistan, Portugal, South Africa, South Korea, Sweden, Ukraine, the United Kingdom, the United States, Interpol, the European Central Bank, and the OECD.

INTRODUCTION: NATURE OF THE REAL-ESTATE SECTOR

5. The real estate sector merits closer consideration given the large scope of monetary transactions, its significant social impact, and because of the number of cases in which money laundering, and in limited circumstances terrorist financing and tax fraud schemes, have been detected.[2] Abuse in this sector also has the undesirable effect of political, institutional and economic destabilisation. Moreover, due to the international nature of the real-estate market, it is often extremely difficult to identify real estate transactions associated with money laundering or terrorist financing.

6. Given that the purchase or sale of a property is one of the largest financial transactions a family or individual may undertake, changes in property prices have a substantial impact on the considerations taken into account by potential buyers and sellers of properties. Fluctuations in property prices have an impact on decisions about where to live and work in addition to affecting an owner's net worth. Moreover, to the extent that property values influence rents, the effect is manifested in the distribution of wealth between landlords and tenants. Finally, property prices significantly influence the building industry. Taken together, these factors all suggest that fluctuations in property prices may influence economic activity and price stability by affecting aggregate supply and demand, the distribution of income, and the debt decisions undertaken by households.[3]

7. Nevertheless, it is difficult to monitor and explain variations in property prices due to a lack of reliable and uniform information. Property markets are geographically segmented and numerous factors shape the local price of real-estate. Understanding the factors that underlie pricing in the property market is therefore essential.

8. Historically there exists a commercial and residential real-estate market, and the property in both types of market may be bought and sold, managed and/or developed. More recently, new investment vehicles have emerged, including *property investment funds* (PIF) and *real estate investment trusts* (REIT). Such instruments allow average citizens to invest in markets – historically only available to the very wealthy – in order to create a diversified portfolio.

9. Investment in the real-estate sector offers advantages both for law-abiding citizens and for those who would misuse the sector for criminal purposes. Real property has historically appreciated in value, and many countries offer incentives to buyers, including government subsidies and tax reduction. Most importantly for misuse by criminals, however, is the facility the sector may provide for obscuring the true source of the funds and the identity of the (ultimate) beneficial owner of the real asset, which are two key elements of the money laundering process.

10. The real-estate sector is therefore of extraordinary importance to the economy in general and the financial system in particular. The widespread use of mechanisms allowing households to access the property market, the elimination of personal limitations on property ownership, the economic development and growth of tourism in many regions have all led to exponential growth in the number

---

[2] It is important to note as is mention by the OECD (Sub-group on Tax Crimes and Money Laundering) in its real estate report that in many countries, their tax authorities investigate these cases in partnership with other law enforcement agencies. In some instances, parallel investigations for tax fraud and money laundering may be pursued. The OECD examined tax fraud and money laundering involving the real estate sector, along with identity theft and identity fraud. It also developed a training manual to assist tax auditors in detecting and reporting cases of suspected money laundering and/or terrorist financing. The confidential report contains: the scope and nature of the issue, how cases are successfully detected and investigated, a list of red flag indicators (catalogue), the benefits of multi-agency co-operation (including effective exchange of information), compliance results and risk prevention strategies and an inventory of relevant case studies.

[3] European Central Bank (2006).

of financial transactions linked to real-estate. The extraordinary range of possibilities for misusing these processes also allows suspected criminals to integrate and enjoy illegally obtained funds.

11. Through the implementation of international standards in recent years, countries have put various measures into place within their formal financial sector – which includes, among others, banks and credit unions – in order to prevent money laundering and terrorist financing. Because of the tendency for illegal activity to move to other financial / economic areas that may have less formal oversight or where there is relatively less potential for detection, countries must consider extending AML/CFT measures to other parts of their economies, if they want to respond successfully to this threat. For the real-estate sector, this would necessarily include such key players as real-estate agents, legal advisors and notaries.

BASIC TECHNIQUES

12. In order to misuse the real-estate sector, a number of methods, techniques, mechanisms, and instruments[4] are available. Many of these methods are in and of themselves illegal acts; however, certain of them might be considered perfectly legal if they were not associated with a money laundering or terrorist financing scheme (or if this association could not be detected. Through examination of case examples from past money laundering and terrorist financing cases, this study has identified a series of the more common or basic methods and then grouped them according to type or "typology".

- Use of complex loans or credit finance.
- Use of non-financial professionals.
- Use of corporate vehicles.
- Manipulation of the appraisal or valuation of a property.
- Use of monetary instruments.
- Use of mortgage schemes.
- Use of investment schemes and financial institutions.
- Use of properties to conceal money generated by illegal activities.

Typology 1: Complex Loans and Credit Finance

13. Intercompany loans have become a frequent instrument used as a means for raising funds. The ease with which such loans can be arranged makes them popular with the general public. These loans are also used in the real estate sector. Where an instrument is frequently used, misuse of the instrument becomes a possibility as well. Depending on the way in which the loan is structured, two different schemes have been detected.

Loan-Back Schemes

14. Intelligence and law enforcement reports indicate "loan-back" transactions are used by suspected criminals to buy properties – either directly or indirectly – through the purchase of shares in property investment funds. Essentially, suspected criminals lend themselves money, creating the appearance that the funds are legitimate and thus are derived from a real business activity. The purpose of the loan is to give the source of the money an appearance of legitimacy and to hide the true identity of the parties in the transaction or the real nature of the financial transactions associated with it.[5]

---

[4] This report uses the terminology commonly used by the FATF in its various projects. See Annex A to this report and FATF (2005) for more on this terminology.

[5] The lack of information caused by the internationalisation of these structures and their specific morphology make it difficult to understand the true relationship between the various corporate vehicles involved in the loan structure and to be sure of the real origin of the funds, and thus determine whether they are linked to criminal activities or not. In several cases, offshore company loans were used. See FATF (2006) for more on the use of legal persons for money laundering.

Case study 1.1: Proceeds of drug trafficking laundered into real estate

(Predicate offence: money laundering forged loan agreement)

An individual set up three companies. For one of the companies he held bearer shares. To hide his involvement in the companies he used a front-man and a trust and company service provider[6] as legal representatives. For each of the companies, the legal representatives opened bank accounts with three different banks in different jurisdictions. The individual used the three companies to set up a loan-back scheme in order to transfer, layer and integrate his criminal money. He then co-mingled the criminal funds with the funds that originated from the legal activities of one of his companies.

Next the front man then bought real estate. To finance that transaction he arranged for a loan between the two companies.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **The source of the funds used to finance the real estate transaction was from abroad, in particular from offshore jurisdictions and jurisdictions with strict bank secrecy.**
- **The lender of the money, an offshore company, had no direct relation with the borrower of the money**
- **A financial institution was not involved in the loan structure.**
- **There was no loan agreement between the lender and borrower.**
- **The loan agreement was legally invalid.**
- **The information in the loan agreement was inconsistent or incorrect.**
- **The conditions in the loan agreement were unusual (for example, no collateral was required).**
- **No payment of interest or repayment of the principal.**
- **Transaction monitoring by financial institutions showed payable-through accounts, by which incoming payments from abroad were immediately transferred abroad without a logical reason.**

Source: Netherlands.

Back-to-Back Loan Schemes

15. As with *loan-back* schemes, *back-to-back loans* are also known to be used in real-estate related money laundering schemes. In this case, a financial institution lends money based on the existence of collateral posted by the borrower in the usual way. However, the collateral presented to the financial institution originates from criminal or terrorist activities. Although financial institutions are obligated to disclose the existence of these funds on a risk dossier, there are occasions where this analysis may contain shortcomings. Instances where the collateral posted is not specified in the loan agreement or unreliable information as to the nature, location and value of the collateral make it very difficult to recognise a back-to-back loan.

Case study 1.2: Back-to-back loan used to launder funds

(Predicate offence: forged loan agreement, in particular the failure to mention the security underlying the loan and money laundering)

An individual set up two companies in different jurisdictions. He used a front man and a trust and company service provider as legal representatives to hide his involvement. One of the companies, led by the front-man, owned real estate and generated income through rental activity. He set up a back-to-back loan structure to use his criminal money for his real estate investments. He then arranged a bank guarantee between two banks in case of a default of the loan. The bank was willing to provide the bank guarantee with the pledged deposit of one of his companies as collateral. The money placed as a deposit was generated by the individual's criminal activity.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **No reference in the loan agreement to the underlying collateral.**

[6] See Annex A for definitions of this term and others used in this report.

- **The collateral provided was not sufficient**
- **The collateral provider and other parties involved in the loan structure were not known.**
- **The borrower of the money was not willing to provide information on the identity and background of the collateral provider and/or the other parties involved in the loan structure.**
- **The complex nature of the loan scheme could not be justified**
- **There was an unexpected loan default.**

Source: Netherlands.

Typology 2: The Role of Non-Financial Professionals

16. Research has shown that when governments take action against certain methods of money laundering, criminal activities tend to migrate to other methods. In part, this reflects the fact that more aggressive policy actions and enforcement measures increase the risk of detection and therefore raise the economic cost of using these methods.

17. FATF experts have observed in recent years that money launderers are increasingly forced to develop elaborate schemes to work around AML/CFT controls. This has often meant seeking out the experience of professionals such as lawyers, tax advisors, accountants, financial advisors, notaries and registrars in order to create the structures needed to move illicit funds unnoticed. These professionals act as *gatekeepers* by providing access to the international financial system, and knowingly or not, can also facilitate concealment of the true origin of funds.[7]

Obtaining Access to Financial Institutions Through Gatekeepers

18. A number of cases reveal that criminals and terrorists have used non-financial professionals or gatekeepers to access financial institutions. This is especially important during the process of determining eligibility for a mortgage, opening bank accounts, and contracting other financial products, to give the deal greater credibility. It has also been documented that bank accounts are opened in the name of non-financial professionals in order to carry out various financial transactions on their behalf. Examples include depositing cash, issuing and cashing cheques, sending and receiving international fund transfers, etc., directly through traditional saving accounts or indirectly through correspondent accounts.[8]

Case study 2.1: Misuse of a real estate agent to gain introduction to a financial institution, possible link to terrorist financing

(Predicate offence: suspected terrorist financing)

A trustee for a trust established in an offshore centre approached a real estate agent to buy a property in Belgium.

The real-estate agent made inquiries with the bank to ask whether a loan could be granted. The bank refused the application, as the use of a trust and a non-financial professional appeared to be deliberately done to disguise the identity of the beneficial owner. The bank submitted a suspicious transaction report.

Following the analysis of the financial intelligence unit, one of the members of the board of the trust was found to be related to a bank with suspected links to a terrorist organisation.

Indicators and methods identified in the scheme:

- **Instrument: real estate, loan.**
- **Mechanisms: bank, trust, real-estate agent.**

[7] FATF (2001), p. 12.

[8] Although it is not the scope of the report, the FATF experts have observed the misuse of the correspondent accounts as a way to hide the origin or destination of money flows and the real participants in the transaction. On several occasions, the misuse of these accounts has been linked to the type of operations reflected in it, especially when cheques or cover payments were used.

- **Techniques: offshore customer, non-account holder customer, physical person intermediary, high risk jurisdiction, loan, purchase of real estate.**
- **Opportunity taken: using a trust and appealing to a non-financial profession was clearly done to disguise the identity of the beneficial owner.**

Source: Belgium, 2003.

Assistance in the Purchase or Sale of Property

19. Non-financial professionals such as notaries, registrars, real-estate agents, etc., are sometimes used by suspected criminals on account of their central role in carrying out real-estate transactions. Their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

20. Until relatively recently, however, these professionals have not been obligated under international standards to report suspicious activity to their national financial intelligence units (FIUs). In some countries where non-designated financial professionals fall under the scope of anti-money laundering legislation, these systems are still in the initial stages of implementation[9], so that the level of co-operation and the effectiveness of their suspicious transaction reporting have not yet been extensively tested. Operational problems have also arisen. In some cases, these have resulted from difficulties in centralising information gathered from various domestic authorities, and in others it stems from differences in legal systems between jurisdictions (common law and civil law, for example).

21. Several cases have come to light revealing that the role of non-financial professionals in detecting illegal activity can also be significant in this area. There have been examples of notaries and registrars detecting irregularities in the signing of the property transfer documents (for example, using different names or insisting on paying a substantial part of the cost of the transaction in cash). Other examples include buying land designated as residential through a legal person and then reclassifying it a short time later for commercial development. Professionals working with the real-estate sector are therefore in a position to be key players in the detection of schemes that use the sector to conceal the true source, ownership, location or control of funds generated illegally, as well as the companies involved in such transactions.

Case study 2.2: Use of a notary when buying a real estate

(Predicate offence: suspected money laundering by organised crime)

An East European was acting under a cover name as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients".

The funds were then used to issue a cheque to a notary for the purchase of a property. The attention of the notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross border transaction and wire transfers to launder money that, according to police sources, came from activities related to organised crime.

It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Indicators and methods identified in the scheme:

- **Instruments: check, wire transfers, real estate.**

[9] In some countries the sector contains a large group of supervised natural and legal persons. That may be the cause for concerns regarding the capacity to provide adequate supervision.

- **Mechanisms: notary, bank.**
- **Techniques: business account, front company customer, purchase of real estate, cross border transaction, incoming wire transfer, reverse/flip real estate, unknown source.**
- **Opportunity taken: use of a notary when buying a real estate. Since the company's bank account was not used for any other transaction, it can be deduced that this company was a front company set up for the mere purpose of carrying out the property transaction.**

Source: Belgium, 2003.

Trust Accounts

22. A *trust account*[10] is a separate bank account, which a third party holds on behalf of the two parties involved in a transaction. Funds are held by the trustee until appropriate instructions are received or until certain obligations have been fulfilled. A trust account can be used during the sale of a house, for example. If there are any conditions related to the sale, such as an inspection, the buyer and seller may agree to use a trust account. In this case, the buyer would deposit the amount due in a trust account managed by, or in the custody of, a third party. This guarantees the seller that the buyer is able to make the payment. Once all the conditions for the sale have been met, the trustee transfers the money to the seller and the title to the property is passed to the buyer.

Case study 2.3: Use of a solicitor to perform financial transactions

(Predicate offence: distribution of narcotics)

An investigation of an individual revealed that a solicitor acting on his behalf was heavily involved in money laundering through property and other transactions.

The solicitor organised conveyancing for the purchase of residential property and carried out structured transactions in an attempt to avoid detection. The solicitor established trust accounts for the individual under investigation and ensured that structured payments were used to purchase properties and pay off mortgages.

Some properties were ostensibly purchased for relatives of the individual even though the solicitor had no dealings with them. The solicitor also advised the individual on shares he should buy and received structured payments into his trust account for payment.

Indicators and methods identified in the scheme:

- **Instruments: cash deposits, real estate.**
- **Mechanisms: solicitor, trust accounts.**
- **Techniques: structured cash transactions, establishment of trust accounts to purchase properties and pay off mortgages, purchase of property in the names of the main target.**
- **Opportunity taken: the solicitor set up trust accounts on behalf of the target and organised for transactions to purchase the property, pay off mortgages, and shares were purchased to avoid detection. In some cases properties were purchased in the names of relatives of the target.**

Source: Australia.

Management or Administration of Companies

23. There have been documented cases of non-financial professionals approached by money launderers and terrorists not just to create legal structures, but also to manage or administer these companies. In this context, these professionals may have been generally aware that they are taking an active role in a money laundering operation. Their access to the companies' financial data and their direct role in performing financial transactions on behalf of their clients make it almost impossible to accept that they were not aware of their involvement.

[10] Also known as an *escrow* account.

Case study 2.4: Abuse of a notary's client account

(Predicate offence: suspected trafficking in narcotics)

A company purchased property by using a notary's client account. Apart from a considerable number of cheques that were regularly cashed or issued, which were at first sight linked to the notary's professional activities, there were also various transfers from the company to his account.

By using the company and the notary's client account, money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions.

Police sources revealed that the sole shareholder of this company was a known drug trafficker.

Indicators and methods identified in the scheme:

- **Instruments: cheque, cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: intermediary account, purchase of real estate, incoming wire transfer.**
- **Opportunity taken: by using the company and the notary's client account money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions**

Source: Belgium, 2002.

Typology 3: Corporate Vehicles

24. Corporate vehicles – that is, legal persons of all types and various legal arrangements (trusts, for example)[11] – have often been found to be misused in order to hide the ownership, purpose, activities and financing related to criminal activity. Indeed that practice is so common that it almost appears to be ubiquitous in money laundering cases. The misuse of these entities seem to be most acute in tax havens, free-trade areas and jurisdictions with a strong reputation for banking secrecy; however, it may occur wherever the opacity of corporate vehicles can be exploited.

25. Apart from obscuring the identities of the beneficial owners of an asset or the origin and destination of funds, these corporate vehicles are also sometimes used in criminal schemes as a source of legal income. In addition to shell companies, there are other specialised companies that carry out perfectly legitimate business relating to real estate, which have sometimes been misused for money laundering purposes. This aspect is illustrated by the use, for example, of property management or construction companies. The use of corporate vehicles is further facilitated if the company is entirely controlled or owned by criminals.

Offshore Companies[12]

26. Legal persons formed and incorporated in one jurisdictions, but actually used by persons in another jurisdiction without control or administration of a natural or legal resident person and not subject to supervision, can be easily misused in money laundering transactions. The possibilities for identifying the beneficial owner or the origin and destination of the money are at times limited. In these scenarios actors with wrongful intentions have the distinct advantage of extra protection in the form of bank secrecy.

[11] See Annex A for definitions of some of these terms.

[12] It applies to the situation where a company is incorporated in one jurisdiction for persons who are resident in another jurisdiction. See FATF (2006) for the terminology relating to offshore companies.

Case study 3.1: Use of an offshore company to buy real estate.

(Predicate offence: suspected violations related to the state of bankruptcy)

A bank reported a person whose account had remained inactive for a long period but which suddenly was inundated with various cash deposits and international transfers. These funds were then used to write a cheque to the order of a notary for the purchase of a real estate.

It appeared that the party involved had connections with a company in insolvency and acted in this way to be able to buy the property with a view to evading his creditors.

The final buyer of the real estate was not the natural person involved but an offshore company. The party involved had first bought the property in his own name and subsequently had passed it on to the aforementioned company.

Indicators and methods identified in the scheme:

- **Instrument: cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: personal account, purchase of real estate, incoming wire transfer, dormant account, offshore transactions.**
- **Opportunity taken: use of an offshore company to buy real estate. It appeared that the party involved had connections with a company in insolvency and acted in this way to be able to buy the property with a view to getting away from his creditors.**

Source: Belgium, 2002.

Legal Arrangements

27. The use of some legal arrangements such as trusts can play an important role in money laundering. Under certain conditions these legal arrangements can conceal the identity of the true beneficiary in addition to the source and/or destination of the money.

28. The nature and/or structure of certain trusts can result in a lack of transparency and so allow them to be misused:[13]

- Certain trusts may exist without the need for a written document constituting them.
- Although there may be a deed defining the trust, in some cases it does not need to identify the depositary and/or a specific beneficiary.
- There may be no obligation to register decisions regarding the management of a trust, and it may not be possible to disclose them in writing to anyone.
- In some types of trust, such as discretionary trusts, the beneficiary may be named or changed at any time, which makes it possible to safeguard the identity of the beneficiary at all times up until the moment the ownership of the assets is transferred.
- Trusts set up to protect assets may protect the depositary against decisions to freeze, seize or attach those assets.
- Trusts may be set up to manage a company's shares, and they may make it more difficult to determine the identities of the true beneficiaries of the assets managed by the trusts.
- Certain legislation may expressly prohibit the freezing, seizure or attachment of assets held in trust.
- Certain clauses commonly referred to as escape clauses, allow the law to which the trust is subject to be changed automatically if certain events arise. Such clauses make it possible to protect the assets deposited in the trust from legal action.

[13] See FATF (2006) for a short explanation of trusts.

29. These conditions may create a significant obstacle for the authorities charged with applying anti-money laundering and counter terrorist financing laws – especially in relation to international co-operation – thus significantly slowing the process of collecting information and evidence regarding the very existence of the trust and identifying its ultimate beneficiary. Under these circumstances it may be very difficult, if not impossible, for a bank or other financial institution to comply with the "know-your-customer" policies applicable in the country or territory in which it is located.[14]

Case study 3.2: Use of trusts to buy real estate

(Predicate offence: suspected serious tax fraud)

Two trusts were established in an offshore centre by a law firm. The trustee had been requested to accept two payment orders in favour of a bank in order to buy real estate. The communication between these trusts and their trustee always took place through the law firm. It appeared that the trust had been used to conceal the identity of the beneficial owners.

Information obtained by the FIU revealed that the beneficiaries of the trusts were individuals A and B, who were managers of two companies, established in Belgium that were the subject of a judicial investigation regarding serious tax fraud. Part of the funds in these trusts could have originated from criminal activity of the companies.

Indicators and methods identified in the scheme:

- **Instruments: wire transfers, real estate.**
- **Mechanisms: lawyer, trust, bank.**
- **Techniques: trust account, purchase of real estate, legal entity transactor, offshore, and incoming wire transfer.**
- **Opportunity taken: use of trusts to buy real estate. The trusts were used to conceal the identity of the true owners.**

Source: Belgium, 2005.

Shell Companies

30. A shell company is a company that is formed but which has no significant assets or operations, or it is a legal person that has no activity or operations in the jurisdiction where it is registered. Shell companies may be set up in many jurisdictions, including in certain offshore financial centres and tax havens. In addition, their ownership structures may occur in a variety of forms. Shares may be held by a natural person or legal entity, and they may be in nominative or bearer form. Some shell companies may be set up for a single purpose or hold just one asset. Others may be set up for a variety of purposes or manage multiple assets, which facilitates the co-mingling of legal and illicit assets.

31. The potential for anonymity is a critical factor in the use of shell companies. They may be used to hide the identity of the natural persons who are the true owners or who control the company.[15] In particular, permissive practices regarding the form of the shares, whether corporate, nominative or bearer, together with the lack of co-operation on the collection of information, represent a significant challenge when seeking to determine the ultimate beneficial owner.

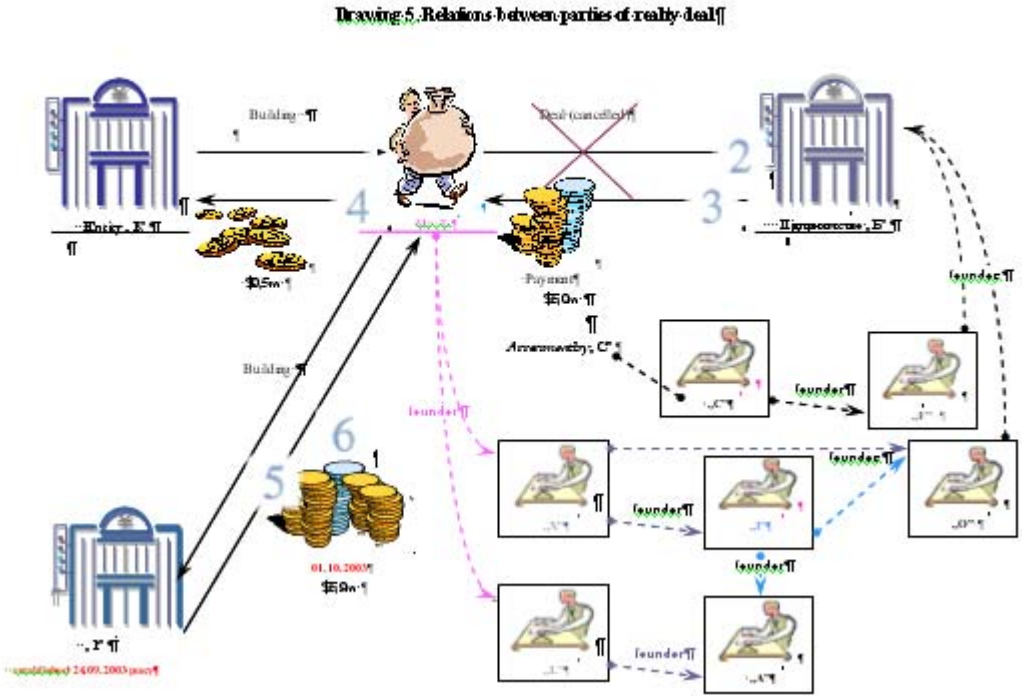
[14] However, it was pointed out in FATF (2006) that, in jurisdictions where trust administrators are licensed and regulated to ensure that they comply with FATF standards on knowing the beneficial owner, these difficulties might be able to be avoided.

[15] Commonly referred to as the *beneficial owner*.

Case study 3.3: Use of a shell company to buy real estate

This scheme involved the purchase of real estate, which was then sold for the higher price to the figureheads. In this case the financial intermediaries informed the financial intelligence unit (FIU) only about the transfer amount. To detect and investigate such cases it was therefore necessary to obtain information from relevant "gatekeepers", especially from registrars of real estate.

The case, investigated by Ukrainian FIU, started from the STR submitted by the auditor of the property buyer. Information was then received from the state registrar of real estate proprietors.



Entity P bought the building in the Ukrainian capital.
Entity K - first owner;
Mr. T - first buyer;
Entity B - next buyer. But the deal was cancelled in 3 months;
Entity P - new buyer.

Suspicion about the transaction was aroused because:

The selling price of building was 10 times higher then purchase price 3 days later.
The purchase price for Mr. T was determined based on the assessment of the state registrar of real estate.
The selling price was based on the assessment of private expert from entity C.
Mr. T did not have his own money. He would have had to work for 200 years to acquire this amount (USD 500 000) through his legal income. Nevertheless, on the day of payment, Mr. T received money from B as an advance for the same building.

In three months the deal with B was cancelled and the building was sold to P for USD 5.9 million. There are close relations between T, B and C, shown at the diagram. There was thus strong probability that the transfers of money to Mr. T were done for the purpose of laundering of USD 5.4 million.

Source: MONEYVAL (Ukraine).

Property Management Companies

32. When using the real-estate sector, the purchase or construction of properties is a commonly used means by which criminals carry out financial transactions. However, a property that is bought or constructed using illegally obtained funds may subsequently be rented out to provide an apparently

legal source of income in order to camouflage movements of funds between various jurisdictions (for example, the tenant and the landlord are located in different jurisdictions).

33. In cases where a company is owned or controlled by a criminal group, a possible way to use the property for money laundering is to mix cash of illegal origin with legitimate rental income. It then appears to be the result of the company's legitimate profits. In other cases, criminals seem to use the company's property management services to create a veil of legitimacy over other transactions they conduct. Those cases showed the active involvement of property management companies in criminal activity. The level of their participation can vary widely both in what kind of property is involved and how the property management company is being misused. The company may be an integral part of the organised criminal group or it may provide a part of the criminal business activity, fundamentally money laundering.[16]

Case study 3.4: Use of property management companies

(Predicate offence: suspected fraud)

The FIU received a suspicious transaction report from notary A on one of his clients, person B, a foreigner without an address in Belgium, who in his office had set up a company for letting real estate. The sole manager and shareholder of this company was a family member of B, who also resided abroad.

Shortly after its creation the company bought a property in Belgium. The formal property transfer was carried out at notary A's office. The property was paid for through the account of notary A by means of several transfers, not from company X, but from another foreign company about which individual B did not provide any details. The establishment of a company managed by a family member with the aim of offering real estate for let and paid by a foreign company disguised the link between the origin and the destination of the money.

Police intelligence revealed that the individual was known for financial fraud. The investment in the property was apparently financed by the proceeds of these funds.

Indicators and methods identified in the scheme:

- **Instruments: cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: business account, purchase of real estate, transactor inconsistencies, non-resident customer, unknown source.**
- **Opportunity taken: the establishment of a company managed by a family member with the aim of letting real estate paid by a foreign company disguised the link between the origin and the destination of the money**

Source: Belgium, 2005.

Non-trading real estate investment companies[17]

34. Several characteristics of these companies make them especially vulnerable to abuse by suspected criminals. First, it is often very difficult to identify the real owner or controller. Second, the company can be created very easily with no minimum initial capital and without an authentic deed. Additionally, these entities are only recorded at the trade register. Finally, the shares of such companies can be sold without certification so that the true owner is not easily identified.

16 See Serious Organised Crime Agency (2006).

17 Also known by its French acronym, *SCI* or *société civile immobilière*.

Case Study 3.5: Misuse of *non trading real estate investment companies*

(Predicate offence: suspected organised criminal activities)

Two French non-trading real estate investment companies managed by two residents of a western European country successively bought two high value properties for a significant amount (more than EUR 20 million) with a single payment (not a loan).

The analysis of the FIU revealed that beneficial owner of the two properties was a resident of an Eastern European country. Further analysis showed that offshore Company A had moved the funds used to purchase the properties through SWIFT wire transfers. This offshore company was well known for holding shares of Company B registered in the very same country as the beneficial owner of the properties. Company B itself was known for its links to organised crime. Analysis also showed that the two managers of the real estate investment companies were senior staff of Company B.

Indicators and methods identified in the scheme:

- **Instrument: real estate, single payment.**
- **Mechanisms: bank, *société civile immobilière* (SCI).**
- **Techniques: purchase of real estate, French SCI and foreign/offshore companies as intermediary, high value, physical intermediaries linked to the beneficial owner.**
- **Opportunity taken: the FIU analysis revealed that the 2 managers of the French SCI were linked to the beneficial owner through a company owned by him and in which the two managers had senior responsibilities**

Source: France, 2006.

Typology 4: Manipulation of the Appraisal or Valuation of a Property

35. Manipulation of the real value of properties in relation to real estate involves the overvaluing or undervaluing of a property followed by a succession of sales and purchases. A property's value may be difficult to estimate, especially in the case of properties that might be considered atypical, such as hotel complexes, golf courses, convention centres, shopping centres and holiday homes. This difficulty further facilitates the manipulation when such property is involved.

Over-valuation or Under-valuation

36. This technique consists of buying or selling a property at a price above or below its market value. This process should raise suspicions, as should the successive sale or purchase of properties with unusual profit margins and purchases by apparently related participants.

37. An often-used structure is, for example, the setting up of shell companies to buy real estate. Shortly after acquiring the properties, the companies are voluntarily wound up, and the criminals then repurchase the property at a price considerably above the original purchase price. This enables them to insert a sum of money into the financial system equal to the original purchase price plus the capital gain, thereby allowing them to conceal the origin of their funds.

Successive Sales and Purchases

38. In the case of successive sales and purchases, the property is sold in a series of subsequent transactions, each time at a higher price. Law enforcement cases have shown that these operations also often include, for example, the reclassification of agricultural land as building land. The sale is therefore fictitious, and the parties involved belong to the same criminal organisation or are non-financial professionals in the real-estate sector who implicitly know the true purpose of the transactions or unusual activity.

39. In addition to placing obstacles to discovering the true identity of the owners of the property and the real origin of the funds used in the transaction, these constructs usually also have a significant tax impact, as they generally avoid the liability for capital gains tax.

Case study 4.1: Use of a lawyer when buying a real estate.

(Predicate offence: suspected organised crime activity)

A lawyer created several companies the same day (with ownership through bearer shares, thus hiding the identity of the true owners). One of these companies acquired a property that was an area of undeveloped land. A few weeks later, the area was re-classified by the town hall where it is located so that it could be urbanised.

The lawyer came to the Property Registry and in successive operations, transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions.

With each succeeding transfer of the property, the price of the land was increased. The participants in the individual transfers were shell companies controlled by the lawyer. Finally the mortgage was cancelled with a cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it can be concluded that this company was a front company set up merely for the purpose of carrying out the property transactions.

After investigation it was learned that the purchaser and the seller were the same person: the leader of a criminal organisation. The money used in the transaction was of illegal origin (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Indicators and methods identified in the scheme:

- **Instruments: cheques and cover payments.**
- **Mechanisms: correspondent bank accounts.**
- **Techniques: business account, front company customer, purchase of real estate, cross border transaction, incoming wire transfer, reverse/flip real estate, unknown source.**
- **Opportunity taken: use of a lawyer when buying real property and performing bank transactions through correspondent bank accounts. Since the correspondent bank account was not used for any other transaction, it can be deduced that the lawyer set up the correspondent account for the purpose of carrying out the property transactions.**

Source: Spain, 2006.

Typology 5: Monetary Instruments

40. The use of monetary instruments in real estate transactions has traditionally dealt primarily with the use of cash. Although methods of payment continue to evolve, cash continues to be one of the main ways of obtaining and handling funds at the early stages of the process in many of the cases that ultimately involve funds of illegal origin.

41. Other monetary instruments used by criminals in their real-estate activities are cheques and wire transfers through conduit or correspondent bank accounts.

Cash

42. The purchase of high-value properties in cash is one way in which large sums of money can be integrated into the legal financial system. Some jurisdictions have observed that there has been a marked increase in demand for high denomination banknotes in their territory, which seems to be inconsistent with the progressive change in public preferences towards other means of payment. Specific geographic and financial concentrations of demand and cross-border movements have also been detected (specific locations, banks, ports, etc.). Although this demand also arises for reasons not strictly considered to be money laundering or terrorist financing activities, such as tax avoidance, evasion or fraud, it does seem to be clear that the real estate sector may be a key contributing factor in the increase in this demand for some jurisdictions, as the black economy tends to grow during a property boom.

43. As well as being used to buy real estate, cash is also used in currency exchange and to structure deposits. It is common to structure cash transactions involving funds from criminal or terrorist sources and then to use these funds to buy, build or renovate a property. When the improved property is finally

sold, the transaction has the advantage that it is difficult, or even impossible, to relate it to a specific individual or a criminal activity.

44. Cash is also used in rental or financial leasing transactions.[18] These processes may be used by money launderers or terrorists to obtain the use of a property without having to fear losing it through its being seized or frozen if their criminal activity is discovered by the authorities. Moreover, it can also be used directly by criminals to settle contracts close to the start of the operation, receiving a reimbursement from the leasing company in the form of a cheque, for example, thus giving the transaction an air of legitimacy. It should be noted that this analysis found that a large share of the market remains in the hands of legal entities which are independent from the banks and financial institutions, thus creating a different channel for funds and making investigation and analysis difficult given the fragmentation of the information.

Case study 5.1: Use of cash to buy real estate

(Predicate offence: drug trafficking)

A criminal organisation operating in the Americas and Europe, laundered resources generated from drug trafficking through the misuse of bureaux de change and exploitation of apparently legitimate real-estate businesses in different countries. The criminal organisation led by Mr. B, sent cocaine from South America to Europe, disguising it in rubber cylinders that were transported by air. The money generated from the trafficking was collected in Europe and forwarded in the same way back across the Atlantic.

In Latin-American Country 1, Mr B acquired an existing bureau de change; he changed its name and became its main shareholder and general director. With the purchase of an already constituted financial institution, the criminal organisation avoided the strict controls implemented by the regulatory authorities as regards to the constitution and operation of financial entities.

In European country 2, the criminal organisation acquired commercialisation companies, created real estate corporations managed by citizens of Latin-American Country 1 and opened bank accounts in various financial institutions, declaring as commercial activity trading in jewels, financial intermediation and real estate activities, among others.

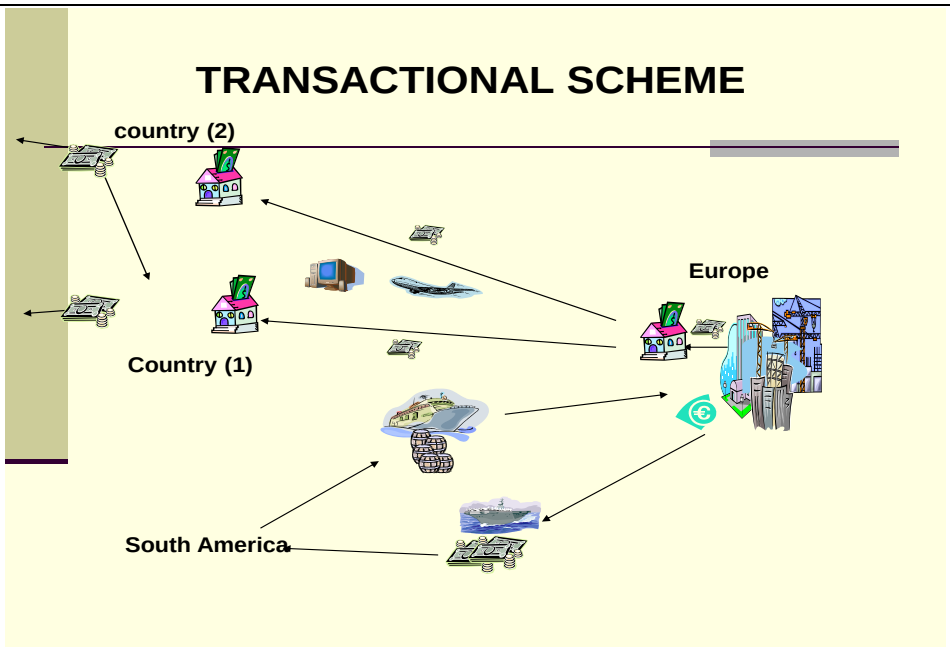
Those companies performed unusual transactions, such as cash deposits in amounts above EUR 500,000 and immediate transfer orders for the same amounts to foreign accounts belonging to Mr. B's bureau de change in Latin-American Country 1 and American Country 2; allegedly for investments in the real-estate sector; money was deposited in low denomination currency and some counterfeit notes were identified as well.

Intelligence information revealed that the account of the bureau de change located in American Country 2, received during a year and a half period, deposits for more than USD 160 million.

Indicators and methods identified in the scheme:

- **Maritime exportation of drugs from America to Europe and cash imports trough the same route.**
- **Incorporation of jewellery and real-estate companies in Europe, managed by citizens of Latin-American Country 1 to launder the money generated from drugs trafficking.**
- **Acquisition of an existing bureau de change in Latin-American Country 1, opening several bank accounts located in Latin-American Country 1, American Country 2 and Latin-American Country 3.**
- **Cash deposits in amounts above EUR 500 000 on behalf of the real state corporations located in Europe and immediate transfer orders for the same amounts to foreign accounts belonging to Mr. B's bureau de changeg in Latin-American Country 1 and American Country 2; allegedly for investments in real state sector.**
- **Intelligence information revealed that the account of the exchange house located in American Country 2, received during a year and a half period, more than USD 160 million.**
- **No continuity in the resources in the accounts.**

[18] Leasing is considered to mean contracts with the sole purpose of granting the use of real property purchased for this purpose in accordance with the specifications of the future user, in exchange for consideration in the form of the periodic payment of instalments to recoup the cost of the asset, excluding the value of the purchase option and financial charges. Leased goods must be used by the user solely for his business purposes. A financial leasing contract must include a purchase option in favour of the user at the end of the lease.



Source: Mexico.

Cheques and Wire Transfers

45. A number of cases revealed that criminals frequently use what might be termed *payable-through accounts* to channel large sums of money, generally through a series of transactions. In many cases sums are initially paid into these accounts in cash, cheques or via international wire transfers. The money never stays in the account for long, the rate of turnover of the funds is high, and the funds are then used to purchase real estate. There would appear to be no commercial or economic justification for using these accounts. The same could apply to correspondent accounts when used as transit account. Suspicion about a legitimate use can be appropriate, when the account has high turnover, it appears to deal exclusively with wire transfer payments (MT 103 plus MT 202 messages) or cheques and the account appears to have no commercial or economic justification for such use.

46. Analysis of the accounts in the cases studied often showed that they were opened for the sole purpose of conducting transactions and operations of this type. The basic purpose of the operation was, as always, to conceal the true origin of the funds and their ownership.

Case study 5.2: Use of a transit account to buy real estate and launder the funds from human being trafficking

(Predicate offence: suspected trafficking in human beings)

A bank's suspicions were raised after a bank cheque was issued to the order of a notary upon request of an Asian national for purchasing real estate. Analysis of the account transactions showed that the account received several transfers from Asians residing abroad and was known through an investigation regarding a network of Asian immigrants.

The analysis showed that the account had been used as a transit account by other Asian nationals for the purchase of real estate.

Indicators and methods identified in the scheme:

- **Instruments: wire transfers, cheques, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: personal account, purchase of real estate, transit account, incoming wire transfer.**
- **Opportunity taken: use of a transit account by non resident nationals for purchasing real estate.**

Source: Belgium, 2005

Typology 6: Mortgage Schemes

47. Mortgage loans comprise one of the main assets on the balance sheets of banks and other financial institutions. An inherent risk in this activity arises from the fraudulent or criminal use of these products. Through this misuse of the mortgage lending system, criminals or terrorists mislead the financial institution into granting them a new mortgage or increasing the amount already lent. This use constitutes, in the majority of the cases analysed, a part of the financial construction established to carry out criminal activities.

48. It was observed in many instances that financial institutions consider these mortgage products to be low risk. A risk-based approach to monitoring subjects related to money laundering and terrorist financing, similar to those based on customer due diligence or "know your customer" principles, could mitigate some of the risk of this activity.

Illegal Funds in Mortgage Loans and Interest Payments

49. Illicit actors obtain mortgage loans to buy properties. In many cases, illegal funds obtained subsequently are used to pay the interest or repay the principal on the loan, either as a lump sum or in instalments. The tax implications of using these products should also not be overlooked (for example, eligibility for tax rebates, etc.).

50. Front men are also sometimes used to buy properties or to apply for mortgages. The analysed cases seem to indicate that this misuse of mortgages goes hand in hand with a simulated business activity and the related income so as to deceive the bank or other financial institution when applying for the mortgage. On occasion the property is apparently purchased as a home, when in reality it is being used for criminal or terrorist activities (for example, selling or storing drugs, hiding illegal immigrants, people trafficking, providing a safe house for members of the organisation, etc.).

Case study 6.1: Use of illegal funds in mortgage loans and interest payments

(Predicate offence: forgery, deception, fraud, money laundering)

An individual used a front-man to purchase real estate. The value of the real estate was manipulated by using a licensed assessor (realestate agent) to set up a false higher but plausible assessment of the market value of the property after renovation. The bank was willing to grant a mortgage on the basis of this false assessment. After the disbursement of the loan the real estate was paid for. The remaining money was then transferred by the owner to bank accounts in foreign jurisdictions with strict bank secrecy. The renovation took never place. The company finally went into default and the loan could not be reimbursed.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **Applying for a loan under false pretences.**
- **Using forged and falsified documents.**
- **The client persisted in representing his financial situation in a way that was unrealistic or that could not be supported by documents.**
- **The loan amount did not relate to the value of the real estate.**
- **Successive buying and selling transactions of the real estate were involved.**
- **The client had several mortgage loans concerning several residences**

Source: Netherlands.

Under-valuation of Real Estate

51. Illicit actors often omit a part of the price from the purchase contract. In other words, the amount listed on the contract of sale is less than the real purchase price paid. The price shown on the contract is paid for with a mortgage loan; whereas the part not appearing on the contract is paid in cash

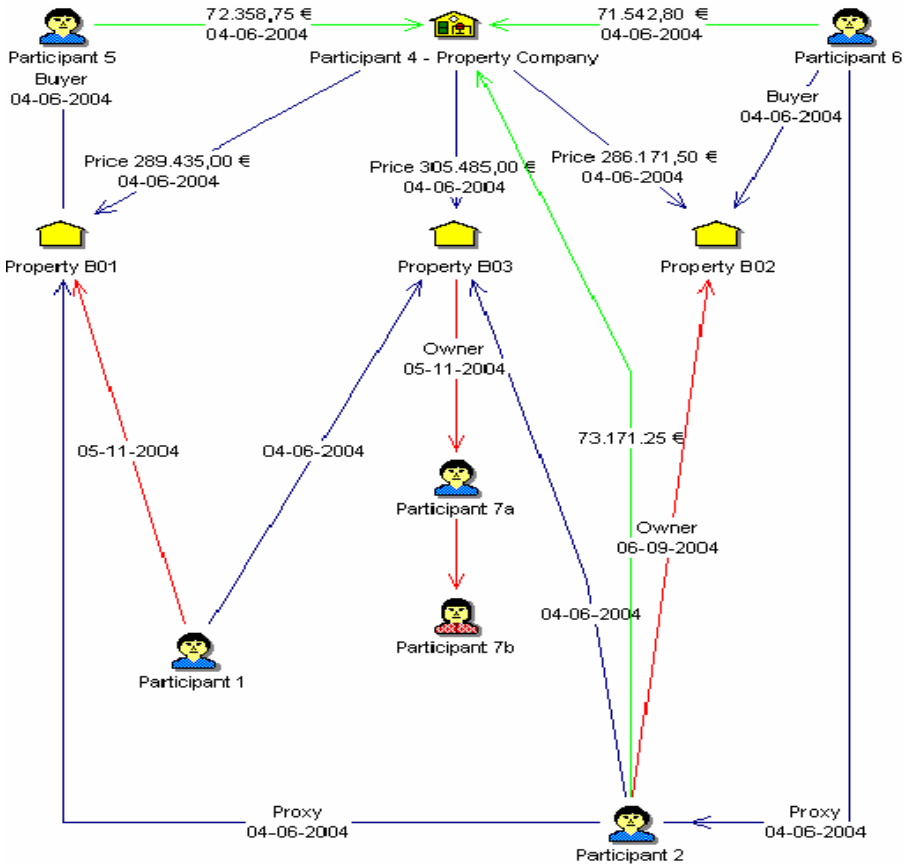
produced by the criminal organisation or terrorist group's criminal activities and is paid to the seller under the table.

52. When the property is sold at fair market price the illicit actor converts illegal income into seemingly legitimate profits. The proceeds might remain available in the bank account of the criminal organisation or terrorist group in the jurisdiction in which the property is located and thus constitute a critical starting point for an investigation.

53. If the criminal organisation or terrorist group is unable to find a seller willing to accept money under the table or is unable to influence the valuation of the property by the independent appraiser, it may still pay for part of the price set in the contract in cash from illegal activities, with a sum of money left over from not using the whole of the mortgage granted to it. In all these scenarios, it should be obvious to the bank or other financial institution that part of the purchase price is being paid via an alternative route, and it should verify whether this is consistent with the known profile of the customer in relation to the customer's pattern of income and expenses.

Case 6.2: Undervaluation of real estate in a terrorist financing scheme

(Predicate offence: money laundering, terrorist financing, manipulation of the appraisal of a property)



The authorities in Country A became aware, during the investigation of the finances of a terrorist organisation in Country B, that the police in Country B had searched the offices of real-estate agents allegedly used by the terrorist group to conceal funds by buying property.

It was found that the owners of the real-estate agents had conducted various real-estate transactions in Country A, either directly or as proxies, using the services of a law firm which had placed its own structure of bank accounts at the disposal of the parties under investigation. Both the law firm and the bank at which it held its accounts were located in Country A.

There was information in Country A regarding the involvement of participants 1 and 2 in the purchase of three properties. On a single day in 2005, Participants 1 and 2 made three deposits of EUR 3 210 each as down-payments to reserve properties in a residential complex in a coastal region of Country A for subsequent purchase. These properties were being built by the property company (Participant 4). Three un-notarised contracts of sale were signed by the property company and Participant 2, acting on his own behalf and as the verbal proxy of the purchasers (Participants 5, 6, 7). On the same day, Participant 1 transferred EUR 210 000 into the current account held by the law firm in Country A (Participant 3).

Three bank drafts were requested, for the sums of EUR 69 000, EUR 68 000, and EUR 73 000, with the funds being drawn from the law firm's current account. These were used to make the first payment against the contract of sale, which named the purchasers and set the final price.

Subsequently, after signing the property transfer documents before a notary in Country A, various assignments were made in the un-notarised contracts of sale that made changes to the final ownership of the properties:

○ Participant 1 ultimately bought property B01, and parking space 01.
○ Participant 2 ultimately bought property B02, and parking space 02.
○ Participants 6 and 7 ultimately bought property B03, and parking space 03.

The law firm (Participant 3) undertook all the legal formalities and attended the signing of the transfer documents and acted as a translator for the purchasers.

To reconstruct the route taken by the funds used to buy the properties and to be reasonably sure of the origin of this money a number of obstacles had to be overcome. The first obstacle was the use of the bank drafts received by the property company in Country A (Participant 4) in each case. Bank drafts were used for the initial payments against the un-notarised contracts and the final payments before signing the deeds[19].

These bank drafts were issued by the main office located near the properties and the relevant funds deducted from current account held by the law firm (Participant 3). Funds transfers were paid into this current account. On some occasions these referred to a person's name and in others a generic sender.

In the case of the property eventually purchased by Participant 1, at the time of signing the property transfers two certificates issued by a financial institution were submitted, certifying that the funds with which the property was being bought belonged to a non-resident in Country A.

The law firm (Participant 3) stated that at the time of agreeing to act as an advisor to Participant 1 that it knew Participant 1 to be a real-estate agent in Country B and that it was working for third parties who were interested in making investments in Country A, and that for this reason it was unaware of the origin of the funds being paid into its account for the transactions in which it was acting as an intermediary on behalf of Participant 1.

Examining each of the legal and financial transactions described above on their own there does not appear, at first glance, to be any suspicious activity. However, a look at the overall operation provides an argument for the conclusion that the people investigated and the law firm (Participant 3) were facilitating real-estate investments in Country A while hiding the origin of the funds and their true owner.

The purchase of the three properties was designed as a single transaction from the outset:

○ The deposits were paid on the same date, as were the contracts of purchase with the property company (Participant 4) in Country A, and they were all signed by Participant 2.

○ The funds used to make the first payments arrived in a single transfer, against which three bank drafts were requested. These drafts had sequential serial numbers.

○ The three transactions have the same legal structure: payment of the deposit, un-notarised contract of sale, assignment of rights to a second purchaser by means of an un-notarised contract, and deed of sale in the name of a person other than the one who had initially signed the contract with the property company (Participant 4) in Country A.

○ Various legal entities and natural persons acting on behalf of third parties intervened between the property and the final purchaser:

○ The law firm (Participant 3), which had as its client a real estate agent in Country B, carried out legal transactions on behalf of third parties.

[19] In the case of the property bought by Participant 2, it was impossible to obtain evidence of the means of payment used to make the final payment before signing the property transfer documents.

○ From the point of view of the property company, a law firm (Participant 3) and a property company in Country B were buying property on behalf of individuals who paid with bank drafts.

Indicators and methods identified in the scheme:

- **The property which Participants 1 and 2 (who were the managers of the property companies in Country B) were going to buy for themselves was finally assigned to third parties.**
- **The properties that certain third parties were initially going to buy were finally bought by Participants 1 and 2 for themselves.**
- **One of the managers of the property company in Country B, Participant 1, bought an option to buy a property for four times its value even though the property was virtually identical to another which he already had the right to purchase and which he had transferred to a third party at cost. This would imply a profit of >250% if this price was actually paid, although in the contract there is no reference to the form or date of payment.**
- **Participant 1 first bought his property and then one month later applied for a mortgage on it. This may either be for tax reasons or a sign that the funds with which he acquired the property were not his.**
- **In addition to the parties investigated (Participants 1 and 2), there is a thread running throughout the operation as analysed, namely the law firm (Participant 3):**
- **The law firm (Participant 3) placed its current account with a bank in Country A at the disposal of Participants 1 and 2 so that they could send funds, while knowing that as professionals in the property business that they could open non-resident accounts in Country A either in the name of the company for which they worked or in their own names.**
- **The participants also obtained bank drafts for the various payments arising out of the contracts they signed. The combination of the use of bank drafts and the current account of a law firm considerably complicated the task of tracking the funds with which the property was bought, as, starting with the property transfer documentation it is necessary to contact the seller to obtain the bank draft number, and then obtain information about the origin of the funds used to purchase the draft from the bank, to finally arrive at the law firm.**
- **Given the active participation of the law firm in all the legal transactions relating to the properties (from the signing of the first, un-notarised contracts of sale, through to the signing of the property transfer documents, in which the law firm was present to act as a translator for the final buyers) the contract transferring the right of purchase that Participant 1 obtained from the purchaser (Participant 5) for four times its value can only be interpreted as a transaction intended to provide the buyer (Participant 5), or others, with an apparently legitimate origin for at least EUR 200 000.**

Source: Spain 2006.

Over-valuation of Real Estate

54. Cases have also occurred in which illicit actors overvalued properties in order to obtain the largest possible mortgage. This over-valuation was achieved by manipulating the appraisal or by setting up a succession of purchases. Properties that have a more subjective valuation offer more scope for overvaluation, as is the case of hotel complexes, leisure centres, golf courses, restaurants, unique buildings, etc.

55. When applying for a mortgage, illicit actors often submit false documentation regarding the real value of the property underlying the operation. Additionally, they often use front men or corporate vehicles as a party to the mortgage agreement. The list of participants (for example directors, representatives, etc.) also changes frequently. On occasion, it has been noticed that some time after the mortgage was granted by the financial institution, the borrower defaulted on payment. When the bank tried to recover the debt from the front-man, it found that the latter did not know who was really behind the operation or where they might be located, leading to the debtor's being classified as insolvent. The same thing happens if the defaulter is a corporate vehicle.

Case 6.3: Overvaluation of real estate and used of third parties launder funds

(Predicate offence: money laundering, forged loan agreement)

The parents of Mr X (Mr and Mrs Y) purchased a residential property and secured a mortgage with a Canadian bank. In his mortgage application, Mr Y provided false information related to his annual income and his ownership of another property. The property he had listed as an asset belonged to another family member.

Mr and Mrs Y purchased a second residence and acquired another mortgage at the same Canadian bank. A large portion of the down payment came from an unknown source (believed to be Mr X). The monthly mortgage payments were made by Mr X through his father's bank account. This was the primary residence of Mr X. Investigative evidence shows that Mr X made all mortgage payments through a joint bank account held by Mr and Mrs Y and Mr X.

Mr X then purchased a residential property and acquired a mortgage from the same Canadian bank. Mr X listed his income (far higher than the amounts he had reported to Revenue Canada) from Company A and Company B. Mr X made the down payment and monthly payments. Over two years, Mr X paid approximately CAD 130 000 towards the mortgage. During this time his annual legitimate income was calculated to be less than CAD 20 000.

Mr X also used his brother Mr Z as a front man (nominee) on title to purchase an additional property. Investigators discovered that Mr Z had stated an annual income of CAD 72 000 on his mortgage application listing his employer as Mr X although Mr Z had never worked for his brother, and his total income for two years was less than CAD 13 000.

Mr X made the down payment on this property, and his tenants, who were members of Mr X's drug trafficking enterprise, paid all the monthly mortgage payments. A total of CAD 110 000 was paid towards this property until Mr X and his associates were arrested.

Mr X and his father purchased a fifth property. The origin of the down payment, made by Mr Y, was unknown but is believed to be the proceeds of Mr X's drug enterprise. Monthly payments were made by Mr X.

The use of real estate was one of many methods Mr X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr X and his associates revealed that he felt it was a fool-proof method to launder drug proceeds.

Mr X was convicted in 2006 of drug trafficking, possession of the proceeds of crime and laundering the proceeds of crime in relation to this case.

Indicators and methods identified in the scheme:

- **The use of real estate was one of many methods Mr X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr X and his associates revealed that he felt it was a fool-proof method to launder drug money.**
- **The only problem he faced was securing a mortgage alone, so he had to use a nominee to secure the mortgage or to co-sign on the mortgage. A problem surfaced in this investigation when various properties were sold prior to a restraint order being served. This resulted in a portion of the funds being secured in a lawyer's trust account, which could not be restrained. It was the investigator's belief that up to CAD 500,000 was being held in this trust account.**

Source: Canada 2006.

Typology 7: Investment Schemes and Financial Institutions

56. Direct or indirect investment in the real estate sector by banks and other financial institutions is significant.[20] However, the volume of investment by insurance companies and pension fund managers is also significant, as these institutions place a large part of their long-term liabilities in the property sector at both national and international levels. Bank and other financial institution investment policies demonstrate that investment in property is gaining ground relative to other direct investments.

[20] In the majority of countries, On the balance sheets of banks and financial institutions in most countries, the asset item referred to as credit investments mainly consists of mortgage lending transactions. This means that at times the evolution of the financial system is highly correlated with that of the real-estate sector.

57. Indirect investments are those considered to be limited or in which there is no direct control over the assets of the fund or investment vehicle. Moreover, real estate investment funds may or may not be publicly listed. If funds are unlisted it means that some or the entire fund or investment vehicle is capitalised by the financial institution. The number of co-investors generally ranges from two to ten.

58. The legal structures used for real estate investment funds vary:

- Investment trusts in the real estate sector, either listed or unlisted.[21]
- Companies operating in the real estate sector, either listed or unlisted.[22]
- Associations and unlisted limited companies.

59. A number of cases have revealed that criminal organisations can influence property investment funds in various ways, depending on their degree of involvement:

- Partners in limited companies.
- Co-investors in property investment funds.
- Managers with direct or indirect control over the investment decisions made by property investment funds.

60. Institutions frequently outsource the management of their real estate assets to advisors or intermediaries, who, if they are managers of assets held in trust, may also outsource this task. Thus, several counterparties may be involved in the investment process, beginning with the investment policy set by the financial institution and ending with the investment ultimately made. The criminal organisation or terrorist group may operate or be situated at any point along this chain.

61. Through investment schemes in the real estate sector, the bank or other financial institution may, whether wittingly or not, facilitate or involve itself or become a vehicle for third parties to launder money.

Case study 7.1: Investments in hotel complexes through a front-man

(Predicate offence: organised criminal activities)

On the French west seacoast, an individual presented a project to a district planning authority which involved several real-estate project management companies to develop a golf course with a hundred villas and apartments on property owned by the authority.

The total cost of the operation was very high and was to be funded mostly with funds originating from abroad. The analysis of the FIU revealed that the individual as well as close members of his family had already been involved in previous cases transmitted to the judicial authorities, in which the family had been implicated in the laundering of funds originating from Eastern Europe.

Indicators and methods identified in the scheme:

- **Instrument: real estate.**
- **Mechanisms: bank, district-planning authority, real-estate project management companies.**
- **Techniques: purchase of real estate, involvement of a natural person as an intermediary, high value.**
- **Opportunity taken: the FIU investigations revealed that this individual and members of his family had acted as a front-man for persons from Eastern Europe suspected of being linked with organised crime.**

Source: France, 2006.

[21] Known as *real estate investment trusts* (REITs) in the US and *property investment funds* (PIFs) in the UK.

[22] Known as *real estate operating companies* (REOC) in the US.

Typology 8: Concealing Money Generated by Illegal Activities

62. The use of real estate to launder money seems to afford criminal organisations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and even obtaining tax advantages (such as rebates, subsidies, etc.).

63. Some areas within the real-estate sector are more attractive than others for money laundering purposes, since the financial flows associated with them are considerable. This makes the task of hiding the funds of illegal origin in the total volume of transactions easier. The real estate sector offers numerous possibilities for money laundering: hotel businesses, construction firms, development of public or tourist infrastructure (especially luxury resorts), catering businesses. It is worth highlighting that over the course of the study, trends in these activities were noticed that depend on different regional characteristics: for example, more cases occur in coastal areas, in areas with a pleasant climate, and where non-resident foreign nationals are concentrated, etc. It is also worth noting that countries which have regions of this kind are more aware of the problem and have increasingly begun to establish appropriate measures and controls in the real-estate sector.

Investment in Hotel Complexes, Restaurants and Similar Developments

64. Real estate is commonly acquired in what is known as the integration or final phase of money laundering. Buying property offers criminals an opportunity to make an investment while giving it the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash.

Case study 8.1: Purchase of real-estate in order to establish a restaurant

(Predicate offence: trafficking in illegal labour force)

An Asian national had purchased real estate in order to start a restaurant that he had financed by a mortgage at Bank A. This mortgage was repaid by transfers from an account opened with Bank B in name of his spouse. Within one year his spouse's account was credited by cash deposits and debited by cash withdrawals, as well as transfers to Bank A.

On the debit side of the account there were also various transfers to China in favour of a natural person. The repayment of the mortgage by transfers from an account opened with another bank in name of his spouse.

The main individual involved was known to be part of network that illegally smuggled foreign workers to Belgium.

Indicators and methods identified in the scheme:

- **Instruments: loan, wire transfer, cash, real estate.**
- **Mechanisms: bank.**
- **Techniques: personal account, purchase of real estate, physical person intermediary, cash deposit, withdrawal, outgoing wire transfer.**
- **Opportunity taken: repayment of the mortgage by transfers from an account opened with another bank in name of his spouse.**

Source: Belgium, 2004.

RED FLAG INDICATORS

65. Building on the cases and other information analysed, the participants in this study also identified a number of common characteristics that, when detected individually or in combination, might indicate potential misuse of the real estate sector for ML/TF purposes. These "red flag" indicators when available can assist financial institutions and others in the conduct of customer due diligence for new and existing clients. They also may help in performing necessary risk-analysis in the more general sense for the sector. Thus, valid indicators may help in identifying suspicious activity that should be reported to competent national authorities according to AML/CFT legislation.

66. The indicators developed by this study of the real estate sector are set out in Annex B. They are not intended to represent an exhaustive list of all the possible types of transactions that might be linked to money laundering or terrorist financing. Nor does it imply that the transactions listed are necessarily linked to such activities. It needs to be borne in mind that money laundering always aims to disguise itself as a "normal" transaction. The criminal nature of the activity derives from the origin of the funds and the aim of the participants.

67. Because the international standard in this field primarily focuses on prevention, it is essential to emphasise two types of measures: *i)* Detection of suspicious transactions before they are completed, so as to avoid the funds being fed into the system; and *ii)* analysis of these transactions in cases where it is impossible to detect suspicious activity in order to detect such activity in the future.

ISSUES FOR CONSIDERATION

68. Regarding the real estate sector, there are other issues for consideration apart from the ones previously mentioned that can play a key role in the process of detecting misuse within the sector as a way to channel illicit money. Additionally, all the concerns expressed in the report have policy implications which need to be considered by countries either at a national or international level.

69. This study of typologies should help to identify the weaknesses or loopholes in the prevention systems currently in place, and may lead to the setting up or development of measures to protect the sector from criminal activities linked to money laundering, and thus avoiding its becoming an attractive destination for money obtained from criminal sources.

70. It is therefore important to highlight that the preventive framework to which this report aims to contribute must be constructed in accordance with the preventive measures laid down in these practices or systems. In the same way, it must be pointed out that any relaxation of the controls on these practices or systems could represent an enormous boost to the success of investments in the real estate sector by criminals.

71. In this context, the FATF should play a central role – together with World Bank and International Monetary Fund – in helping develop appropriate measures in emerging markets, as a way to stop illegal money flows.

72. Finally, as the key parties to real estate transactions, DNFBPs need to be encouraged by organisations and legislators in the fight against ML/TF. Real estate agents in particular are involved in the vast majority of real estate transactions and therefore can play a key role in detecting money laundering and terrorist financing schemes. Although this research has demonstrated the growing use of emerging markets and new methods of payments to launder money or finance terrorism through the real estate sector, simpler schemes such as large cash transactions are still commonly used. Because they are in direct contact with buyers and sellers, real estate agents generally know their clients better than the other parties in the transactions. Therefore, they are well placed to detect suspicious activity or identify red flag indicators.

73. The FATF Recommendations recognise the importance of customer due diligence, record-keeping and reporting requirements for the real estate sector. To ensure effective compliance with these requirements, it is important that authorities inform the sector of its obligations and share sector-specific indicators with the industry.

74. Also, it was observed during the research for the project that wire transfers still constitute the best way to allocate money between countries. Although controls have been established within the financial sector and for certain actors within it, settlement systems are still not included in the ML/TF legislation in most countries.

75. Finally, as they are key figures within the real estate sector and its transactions, designated non-financial businesses and professions (DNFBPs) need to be encouraged by organisations and legislators to implement effective AML/CFT measures.

Emerging markets

76. The worldwide market growth of real estate-backed securities and the development of property investment funds has meant that the range of options for real estate investments has also grown. Emerging markets in particular can offer attractive returns at low prices with considerable room for growth. This has not gone unnoticed by many suspected criminals.

77. As a result of a the property boom in emerging markets, it has come to light that many money launderers believe that it is easier to camouflage genuine commercial transactions - funded by their illicitly obtained funds - among the huge number of transactions taking place. Complicating matters is the fact that often these less developed economies do not have an average market price for real estate but rather prices varying across sectors and districts. Examining each and every transaction is impossible, and obtain a clear valuation of its real price is therefore also impossible. At times this situation is made worse by the fact that the banking sector is insufficiently developed, in terms of its financial products and conditions, resulting in financial and company structures that make the tasks of supervision or investigation yet more difficult.

78. Emerging markets often contain several characteristics that are highly favourable for money laundering, including:

- A high level of state intervention as a result of private sector financial structures and banking systems still at the embryonic stage.
- Absence, or limited development, of AML/CFT legislation and absence of indicators of the seriousness and social impacts of these phenomena.
- Lack of foreign capital in sectors other than raw materials.
- Banking and competent authorities (*i.e.* police, tax authorities, courts, etc.) lack training and the means necessary to detect and combat money laundering and terrorist financing.

Wire transfers

79. This method is common to practically all the schemes analysed and is probably one of the most accessible and widely used methods by criminals. The growing introduction of new technologies in financial markets and their increasing globalisation have meant that borders are disappearing and there are fewer obstacles to both legal and illegal activities. It also needs to be borne in mind that as a result of their growing use, the regulatory standards applicable to the financial markets regarding these wire transfers are scant as regards preventing money laundering and terrorist financing, and focus almost exclusively on the standardisation of the data fields used in order to automate and speed up transactions.

80. It needs to be borne in mind that wire transfers can be performed by highly regulated financial institutions and also through by less regulated institutions, such as alternative remittance systems. We need to also include those institutions providing message services and settlement services (*e.g.* FEDWIRE, CHIPS, SWIFT, etc). Therefore differentiating between the providers of the activity on a risk based manner seems appropriate. Additionally, we need to take into consideration the system and instrument used in each institutions to perform their transactions in relation to the regulation level. It means that we need not only consider the institutional regulation, but also if the money flows go through saving accounts, correspondent accounts, cheques, etc that can be considered as wire transfers.

81. The minimal information customers are required to provide in some jurisdictions to prove their identity facilitates the abuse of the system by criminal organisations and terrorist groups by making it possible for them to be almost undetectable while moving large sums of money between countries in seconds. The speed of execution, whether in person or not, the minimal documentation required and the high level of anonymity mean that they are commonly used by money launders abusing these regulatory loopholes. The fact that in only a few countries wire transfer offices are being supervised and subject to anti money laundering and counter terrorist financing requirements, makes the offices even more vulnerable for misuse.

82. Wire transfer systems move billions every day in domestic and international transfers, and although some countries have introduced limited standards for their surveillance, they are extremely difficult to control. It may be concluded from the information compiled that there are no effective

international controls on wire transfers, particularly as regards international transfers. It would be worthwhile to look into the current standards for the category. It could be said that the reliable identification of the parties (payer, payee, etc.) in wire transfer is indispensable to any effective effort to combating money launderings.

Notaries, registrars and similar figures

83. As illustrated throughout this report, notaries and registrars seem to be the weakest link in the chain of real estate transactions, and they may be able to play a role in the detection of high risk transactions relating to the real estate sector. The importance of AML/CFT requirements for third parties has already been recognised by the FATF under Recommendation 9. Due to their central position in the legal system in relation to these real estate transactions, they could potentially also perform a role in centralising and filtering information. However according to the legal professions it is not clear what the boundaries are in complying with the requirements. The FATF is currently undertaking a dialogue with the legal professions and further work in guidance on the recommendation will be elaborated. Some FATF members have charged prevention bodies within the professional associations to which notaries and registrars belong with providing information to the authorities (both judicial and administrative) with powers in relation to money laundering and terrorist financing under the authority of national laws.

84. In countries where the legal professions are considered public servants, a possible solution would be that a system put in operation by notaries and registrars would encompass, in particular, the identification and analysis of patterns of transactions where there is a risk of their concealing money laundering or terrorist financing activities. These models should include mechanisms for notifying financial intelligence units, for example, of those cases in which the level of risk increases or does not decrease after analysis. On this basis, the co-operation of notaries and registrars in the fight against ML and TF would be more clearly supported. It should obviously be pointed out that only a small proportion of these transactions constitute or form part of real money laundering or terrorist financing activities, a conclusion which can only be reached by the competent authorities.

85. Some FATF members consider an overall database at the level of the professional association[23], which would include the majority of the details of all transactions authorised by a notary or registrar and thus serve as the central gathering point for information from these public servants. However, in establishing system like this, countries would also need to consider cost effectiveness and privacy protection issues. A series of risk templates could be applied to this database to extract the relevant information required automatically for subsequent analysis. Approaching openly these gatekeepers and raising awareness on their vulnerabilities and risks as regards to money laundering and or terrorism financing is crucial for the competent authorities in order to reinforce the preventive network against those offences.

[23] From the research, it was clear that, because of the complex nature of real estate transactions, authorities experience difficulties in getting a complete picture of the role played by a person in the financial system. The nationwide database of financial products through which the authorities would be able to locate accounts and other products and then approach the relevant financial institution or other actors in the sector to seek more information through appropriate investigative or judicial means could help in this regard to provide a more complete picture.

ANNEX A - TERMINOLOGY[24]

Beneficial owner: This term refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. As used in this study, the term *beneficial owner* applies as well to the true owner of real property.

Instrument – An ML/TF *instrument* is an object of value (or one which represents value) that in some way or other is used to carry out ML/TF activity. Examples of ML/TF *instruments* include cash funds, cheques, travellers' cheques, precious metals or stones, securities, real property, etc.

Legal arrangements – This term refers to express trusts or other similar structures, such as (for AML/CFT purposes) the *fiducie*, *Treuhand* and *fideicomiso*.

Legal persons – A legal person is a corporate body, foundation, Anstalt, partnership or association, or any similar entities that can establish a permanent customer relationship with a financial institution or otherwise own real property.

Mechanism – An ML/TF *mechanism* is a system or element that carries out part of the ML/TF process. Examples of ML/TF *mechanisms* include financial institutions, money remitters, legal entities and legal arrangements, etc.

Method – In the ML/TF context, a *method* is a discrete procedure or process used to carry out ML/TF activity. It may combine various techniques, mechanisms and instruments, and it may or may not represent a typology in and of itself.

Scheme – An ML/TF *scheme* is a specific operation or case of money laundering or terrorist financing that combines various methods (techniques, mechanisms and instruments) into a single structure.

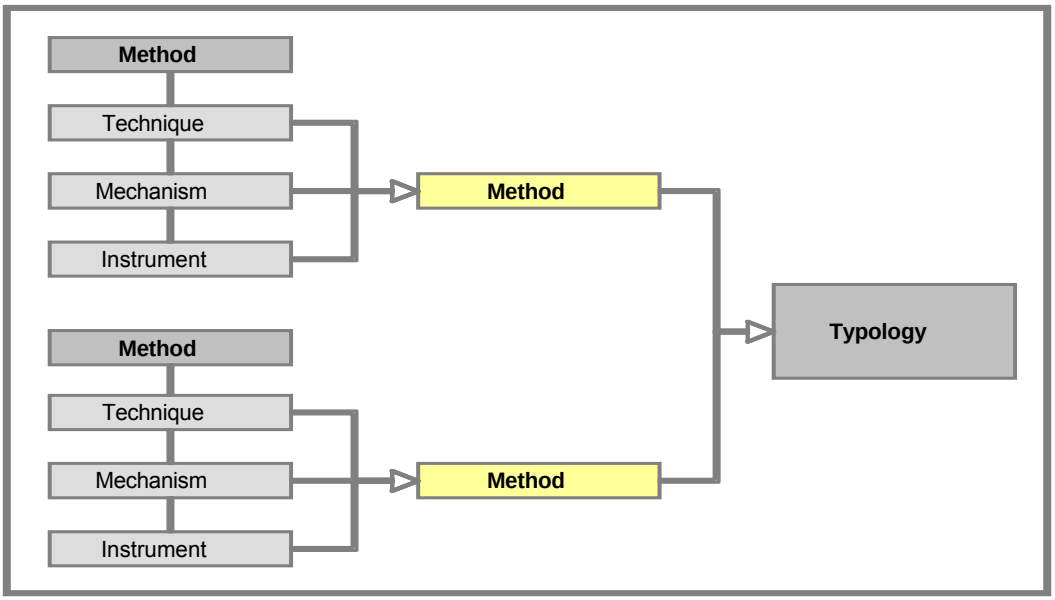
Technique – An ML/TF *technique* is a particular action or practice for carrying out ML/TF activity. Examples of ML/TF *techniques* include structuring financial transactions, comingling of legal and illegal funds, over- and under- valuing merchandise, transmission of funds by wire transfer, etc.

Trust and Company Service Provider (TCSP): This term refers to all persons or businesses that specialise in acting as a formation agent of legal persons for third parties. For a fuller definition of this type of activity, see the "Glossary" to the *FATF 40 Recommendations*.

Typology – An ML/TF *typology* is a pattern or series of similar types of money laundering or terrorist financing schemes or methods.

This report uses the terminology commonly used by the FATF in its typologies analysis. The following figure illustrates the relationship between the various elements of typologies analysis.

[24] Sources used for these terms include FATF (2003), FATF (2004) and FATF (2005).


Method
Technique
Mechanism
Instrument
Method
Method
Technique
Mechanism
Instrument
Method
Typology

ANNEX B - RED FLAG INDICATORS

Building on the cases and other information analysed, the participants in this study also identified a number of common characteristics that, when detected individually or in combination, might indicate potential misuse of the real estate sector for ML/TF purposes. These "red flag" indicators when available can assist financial institutions and others in the conduct of customer due diligence for new and existing clients. They also may help in performing necessary risk-analysis in the more general sense for the sector. Thus, valid indicators may help in identifying suspicious activity that should be reported to competent national authorities according to AML/CFT legislation.

These indicators are not intended to represent an exhaustive list of all the possible types of transactions that might be linked to money laundering or terrorist financing. Nor should it in any way be implied that the transactions listed here are *necessarily* linked to such activities. It should be remembered that activities related to money laundering or terrorist financing are always carried out with the aim of appearing to be "normal". The criminal nature of the activity derives from the origin of the funds and the aim of the participants.

Natural persons

- Transactions involving persons residing in tax havens or risk territories[25], when the characteristics of the transactions match any of those included in the list of indicators.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- Transactions involving persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities involving illegal enrichment, or there are suspicions of involvement in such activities and that these activities may be considered to underlie money laundering
- Transactions involving persons who are in some way associated with the foregoing (for example, through family or business ties, common origins, where they share an address or have the same representatives or attorneys, etc.).
- Transactions involving an individual whose address is unknown or is merely a correspondence address (for example, a PO Box, shared office or shared business address, etc.), or where the details are believed or likely to be false.
- Several transactions involving the same party or those undertaken by groups of persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Individuals who unexpectedly repay problematic loans or mortgages or who repeatedly pay off large loans or mortgages early, particularly if they do so in cash.

[25] The definition of a risk territory could be either one that is determined by the financial institution or another entity applying the indicator directly or else one that has been defined by the national authorities of the country in which the institution or entity is located.

Legal persons

- Transactions involving legal persons or legal arrangements domiciled in tax havens or risk territories, when the characteristics of the transaction match any of those included in the list of indicators.
- Transactions involving recently created legal persons, when the amount is large compared to their assets.
- Transactions involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions involving foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.
- Transactions involving legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Transactions involving legal persons whose addresses are unknown or are merely correspondence addresses (for example, a PO Box number, shared office or shared business address, etc.), or where the details are believed false or likely to be false.
- Various transactions involving the same party. Similarly, transactions carried out by groups of legal persons that may be related (for example, through family ties between owners or representatives, business links, sharing the same nationality as the legal person or its owners or representatives, sharing an address, in the case of legal persons or their owners or representatives, having a common owner, representative or attorney, entities with similar names, etc.).
- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.
- Formation of legal persons to hold properties with the sole purpose of placing a front man or straw man between the property and the true owner.
- Contribution of real estate to the share capital of a company which has no registered address or permanent establishment which is open to the public in the country.
- Transactions in which unusual or unnecessarily complex legal structures are used without any economic logic.

Natural and legal persons

- Transactions in which there are signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.
- Transactions which are begun in one individual's name and finally completed in another's without a logical explanation for the name change. (For example, the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed over to the owner, reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.).
- Transactions in which the parties:
  - Do not show particular interest in the characteristics of the property (*e.g.* quality of construction, location, date on which it will be handed over, etc.) which is the object of the transaction.
  - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
  - Show a strong interest in completing the transaction quickly, without there being good cause.

- Show considerable interest in transactions relating to buildings in particular areas, without caring about the price they have to pay.

- Transactions in which the parties are foreign or non-resident for tax purposes and:
  - Their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying, even temporarily, etc.).
  - They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).
- Transactions in which any of the payments are made by a third party, other than the parties involved. Cases where the payment is made by a credit institution registered in the country at the time of signing the property transfer, due to the granting of a mortgage loan, may be excluded.

Intermediaries

- Transactions performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, etc.).
- Transactions carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Transactions taking place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.

Means of payment

- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions where there are doubts as to the validity of the documents submitted with loan applications.
- Transactions in which a loan granted, or an attempt was made to obtain a loan, using cash collateral or where this collateral is deposited abroad.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments, or where payment is made by endorsing a third-party's cheque.
- Transactions with funds from countries considered to be tax havens or risk territories, according to anti-money laundering legislation, regardless of whether the customer is resident in the country or territory concerned or not.
- Transactions in which the buyer takes on debt which is considered significant in relation to the value of the property. Transactions involving the subrogation of mortgages granted through institutions registered in the country may be excluded.

Nature of the Transaction

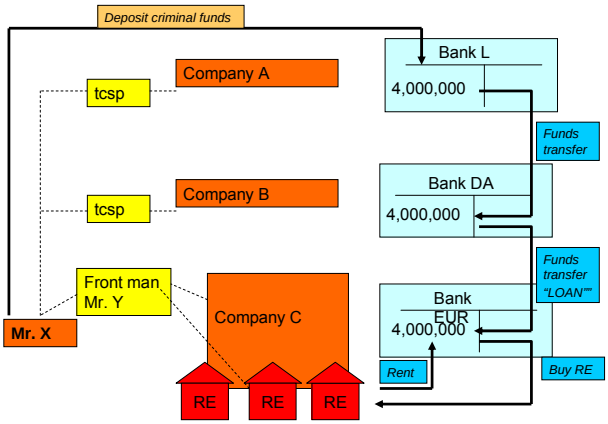
- Transactions in the form of a private contract, where there is no intention to notarise the contract, or where this intention is expressed, it does not finally take place.
- Transactions which are not completed in seeming disregard of a contract clause penalising the buyer with loss of the deposit if the sale does not go ahead.
- Transactions relating to the same property or rights that follow in rapid succession (for example, purchase and immediate sale of property) and which entail a significant increase or decrease in the price compared with the purchase price.

- Transactions entered into at a value significantly different (much higher or much lower) from the real value of the property or differing markedly from market values.
- Transactions relating to property development in high-risk urban areas, in the judgement of the company (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Recording of the declaration of a completed new building by a non-resident legal person having no permanent domicile indicating that the construction work was completed at its own expense without any subcontracting or supply of materials.
- Transactions relating to property development in high-risk urban areas based on other variables determined by the institution (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).

ANNEX C – COMPLETE CASE STUDIES FOR TYPOLOGIES 1 AND 6

Case Study 1.1: Proceeds of drug trafficking laundered into real estate

Mr. X deposited money earned from drug activities into Company A's account at offshore Bank L. Mr. X set up Company A in order to disguise his identity and to place his criminal funds the bank under false pretences. Mr. X also held **bearer shares** issued by Company A., Mr X. established Company B in another offshore jurisdiction under the same circumstances.



Mr X was shareholder of Company A and B but was not registered as such in the public registers. Mr. X made use of a local trust in each location and gave them power-of-attorney to act as his legal representative (through a trust and company service provider: **TCSP**). The local trusts opened accounts at Bank L and at Bank DA on behalf of Company A and Company B respectively. The trusts explained to the banks that the companies that they represented were part of an international structure and that they wanted to benefit from favourable tax arrangements by means of **inter company loans**. This was the reason given for frequent debits and credits of the accounts for incoming and outgoing foreign funds transfers.

Mr X set up Company C in the European country where he is living. Mr. X is the owner of Company C; however, he uses a **front-man**, Mr Y, who is the owner and manager according to the public register at the Chamber of Commerce and the shareholder register. Company C conducted legal counselling activities. This way Mr. X was able to monitor and control the activities in Company C without becoming known to the authorities. Mr Y opened accounts on behalf of Company C with Bank EUR.

Mr X used Companies A, B and C to set up a **loan-back scheme** in order to transfer, layer and integrate his criminal money. The criminal funds, initially placed in the account of Company A in a bank in an offshore jurisdiction, were ultimately invested into real estate in Europe. The real estate was used to expand his legal counselling activities in Company C. The set up of the international loan-back structure, involving Company A, B and C, complicated the audit trail, legitimated the international funds transfers between the various bank accounts of the companies that Mr X controlled. Also Mr X **co-mingled** the criminal funds, disguised as a loan, with the funds originating from the legal activities of Company C, which made the criminal funds difficult to detect and to trace, thus involving a company with legitimate activities in the money laundering scheme, *i.e.* the integration phase (and avoiding attracting the attention of the authorities).

Mr. X arranged for Mr. Y to buy real estate. To finance the transaction, Mr. X arranged for a loan agreement to be drawn up between Companies B and C. The parties in the contract were the trust of Company B and Mr. Y of Company C. To execute the cash disbursement under the loan, Mr. X ordered the trust of Company A to transfer funds from the account in Bank L to the account of Company B in Bank DA. Next he ordered the trust of Company B to transfer funds from the account in Bank DA to the account of Company C in Bank EUR. The description given to Bank DA en Bank EUR referred to the loan agreement between Company B and C. Both banks did not know about the relationship between Companies B and C. The funds deposited in the account of Company C in Bank EUR were then transferred to the seller of the real estate. Periodically Company C made payments of the principal and interest to Company B from the earnings of the counselling activities. Company B transferred the money to Company A which was used by Mr. X to finance his criminal activities. The interest costs were deducted from the taxable result and declared in the tax return.

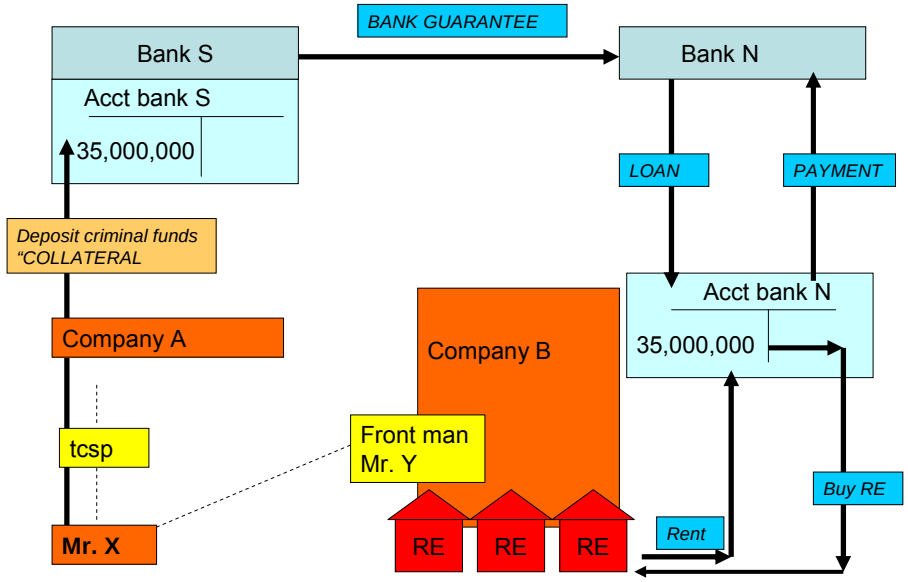
Indicators and methods identified in the scheme:

- **The source of the funds used to finance the real estate transaction was from abroad, in particular from off shore jurisdictions and jurisdictions that have strict bank secrecy.**
- **The lender of the money, an offshore company, had no direct relation with the borrower of the money**
- **A financial institution was not involved in the loan structure.**
- **There was no loan agreement between the lender and borrower.**
- **The loan agreement was legally invalid.**
- **The information in the loan agreement was inconsistent or incorrect.**
- **The conditions in the loan agreement were unusual, for example, there was no collateral required.**
- **No payment of interest or repayment of the principal.**
- **Transaction monitoring by the financial institutions showed payable-through accounts, by which incoming payments from abroad were transferred abroad immediately without a logical reason.**

Source: Netherlands.

Case Study 1.2: Back-to-back Loan Used to Launder Funds

(Predicate offence: forged loan agreement, in particular the failure to mention the security underlying the loan and money laundering)



Mr. X was a criminal who deposited funds via one of his corporate vehicles (Company A) into an account at Bank S. Company A was in an offshore jurisdiction that had strict bank secrecy. Mr X. was the owner of Company A, did not want to disclose his identity and thus used a **TCSP** to manage Company A. Mr. X used Company C to mask his real identity. Mr X also set up and controls Company B of which he is the owner. According to the public registers, the official owner and manager of Company B was Mr. Y who acts as a **front-man**. Company B owned several buildings that were rented out to natural persons and companies. This way Mr. X generated legal rental income via Company B.

Mr. X was short of money from legitimate sources to expand his legal activities. Based on the financial situation of Company B, Bank N was not willing to grant a loan without additional security. He set up a **back-to-back loan** structure to use his criminal money to invest in real estate.

Bank N was willing to lend money to Company B under the condition that Company B provided sufficient collateral and was willing to pay a high-risk premium on top of the market interest rate. Mr. X. arranged for Bank S to provide a **bank guarantee** to Bank N which could be drawn by Bank N on Bank S in case of a default on the loan. Bank N´s credit risk regarding Company B was then fully covered. The loan fit into the financial situation and activities of Company B.

Bank S was willing to provide the bank guarantee to Bank N in name of Company A, with the **pledged deposit** as collateral. The money deposited in Bank S originated from the criminal activities of Mr. X. If Bank N were to withdraw the guarantee on Bank S, Bank S would have used the deposit pledged by Company A to settle the payment with Bank N. For Bank N the original collateral provider Company A, *i.e.* Mr X, was not visible. Bank N only saw Bank S´s guarantee. Bank N lent the money to Company B. Through the payment by Bank N as part of the reimbursement of the back-to-back loan, Mr. X was able to provide a valid reason for the money used to finance the real estate. The collateral originated from criminal activities. The laundered money was invested in real estate that provided for legal rental income.

The earnings of Company B were continuously skimmed off by Mr. X to finance his illegal activities. Company B initially made loan and interest payments to Bank N. After a period of time, Company B stopped the payment of the principal and interest. Based on the loan agreement and the banking terms, Bank N withdrew the bank guarantee on Bank S. Bank S used the pledged deposit to settle the payment to Bank N.

Indicators and methods identified in the scheme:

- **No reference in the loan agreement to the underlying collateral.**
- **The collateral provided was not sufficient**
- **The collateral provider and other parties involved in the loan structure were not known.**
- **The borrower of the money was not willing to provide information on the identity and background of the collateral provider nor on the other parties involved in the loan structure.**
- **The complex nature of the loan scheme could not be justified**
- **There was an unexpected loan default.**

Source: Netherlands.

Case study 6.1: Use of Illegal Funds in Mortgage Loans and Interest Payments

(Predicate offence: forgery, deception, fraud, money laundering)

Mr. X was the owner of Company A and the individual controlling its activities. Mr. X hired Mr. Y as **front man** of Company A. Company A had some low-profile activities in managing and exploiting properties. During the life of Company A, Mr. Y set up a relationship with Bank EUR that provided for accounts and payment services. The property managed by Company A was used for activities by other companies owned by Mr. X (for storage, for example).

Mr. X. planned to buy office buildings for EUR 8 000 000 via Company A. The office buildings had to be renovated to be marketable. Mr. X. knew a licensed assessor (real estate agent), Mr. Z. Mr. X. and Mr. Z found a way to set up a **false but plausible assessments of the market value** of the office buildings after renovation (EUR 13 000 000). Mr. X ordered Mr. Y to negotiate a **mortgage** with Bank EUR to finance the purchase and renovation of the property. Based on the assessment, Bank EUR was willing to grant a mortgage of EUR 13 000 000. Mr. Y entered into the loan agreement on behalf of Company A as the buying party. After the disbursement of the loan, the real estate was paid for. Mr X. then paid Mr. Y EUR 500 000 and had the remaining EUR 4.5 million, together with the proceeds of other criminal activities, transferred into several bank accounts in countries with strict **bank secrecy**. The mortgage of Bank EUR was presented to the foreign banks as the legitimate source of the funds that were being transferred to the accounts. In this way, the money was layered and integrated. The renovation of the office buildings never took place. Meanwhile the activities of Company A rapidly decreased. Company A finally went into default. Bank EUR called the loan, but Mr. Y was not in a position to reimburse it along with the interest payment. Mr Y stated that he was not aware of the persons behind Company A, their whereabouts and the background of the accounts to which the money was transferred.

Indicators and methods identified in the scheme:

- **Applying for a loan under false pretences.**
- **Using forged and falsified documents.**
- **The client persisted in a picture of the financial situation that was unrealistic or that could not be supported by documents.**
- **The loan amount did not relate to the value of the real estate.**
- **Successive buying and selling of the real property involved.**
- **The client had several mortgage loans relating to several residences**

Source: Netherlands.

BIBLIOGRAPHY

European Central Bank (2006), "Assisting House Price Developments in the Euro Area", ECB Monthly Bulletin, ECB, Frankfurt, February 2006. *www.ecb.int/pub/mb/html/index.en.html*.

FATF (2001), *Typologies Report 2000-2001*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2003), *FATF Recommendations*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2004), *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2005), "Money Laundering and Terrorist Financing Trends and Indicators", *Typologies Report 2004-2005*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2006), *Misuse of Corporate Vehicles: Typologies Report*, FATF, Paris. *www.fatf-gafi.org*.

Serious Organised Crime Agency (2006), *The Vulnerability of UK Letting Agents to Money Laundering*, SOCA, London.

Appendix 2

FATF Report – *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* – June 2013

FATF

FATF REPORT

Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals

June 2013

Appendix 2

FINANCIAL ACTION TASK FORCE

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

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

ACRONYMS

AML/CFT	Anti-money laundering/counter financing of terrorism
APG	Asia/Pacific Group on Money Laundering
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
DNFBPs	Designated non-financial businesses and professions
ECHR	European Convention on Human Rights
FIU	Financial intelligence units
GIABA	Intergovernmental Action Group against Money Laundering in West Africa
GIFCS	Group of International Finance Centre Supervisors
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money laundering
OECD	Organisation for Economic Co-operation and Development
PEP	Politically exposed person
SRBs	Self-regulatory bodies
STR	Suspicious transaction report
TF	Terrorist financing

EXECUTIVE SUMMARY

In June 2012, the Financial Action Task Force (FATF) Plenary met in Rome and agreed to conduct typology research into the money laundering and terrorist financing (ML/TF) vulnerabilities of the legal profession.

Since the inclusion of legal professionals in the scope of professionals in the FATF Recommendations in 2003, there has been extensive debate as to whether there is evidence that legal professionals have been involved in ML/TF and whether the application of the Recommendations is consistent with fundamental human rights and the ethical obligations of legal professionals.

The purpose of this typology is to determine the degree to which legal professionals globally are vulnerable for ML/TF risks in light of the specific legal services they provide, and to describe red flag indicators of ML/TF which may be useful to legal professionals, self-regulatory bodies (SRBs), competent authorities and law enforcement agencies.

This typology report does not offer guidance or policy recommendations, nor can it serve as a "one-size-fits-all" educational tool for individual legal professionals practicing in different settings, across countries with varying supervisory regimes and secrecy, privilege and confidentiality rules.

The report concludes that criminals seek out the involvement of legal professionals in their ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism.

The report identifies a number of ML/TF methods that commonly employ or, in some countries, require the services of a legal professional. Inherently these activities pose ML/TF risk and when clients seek to misuse the legal professional's services in these areas, even law abiding legal professionals may be vulnerable. The methods are:

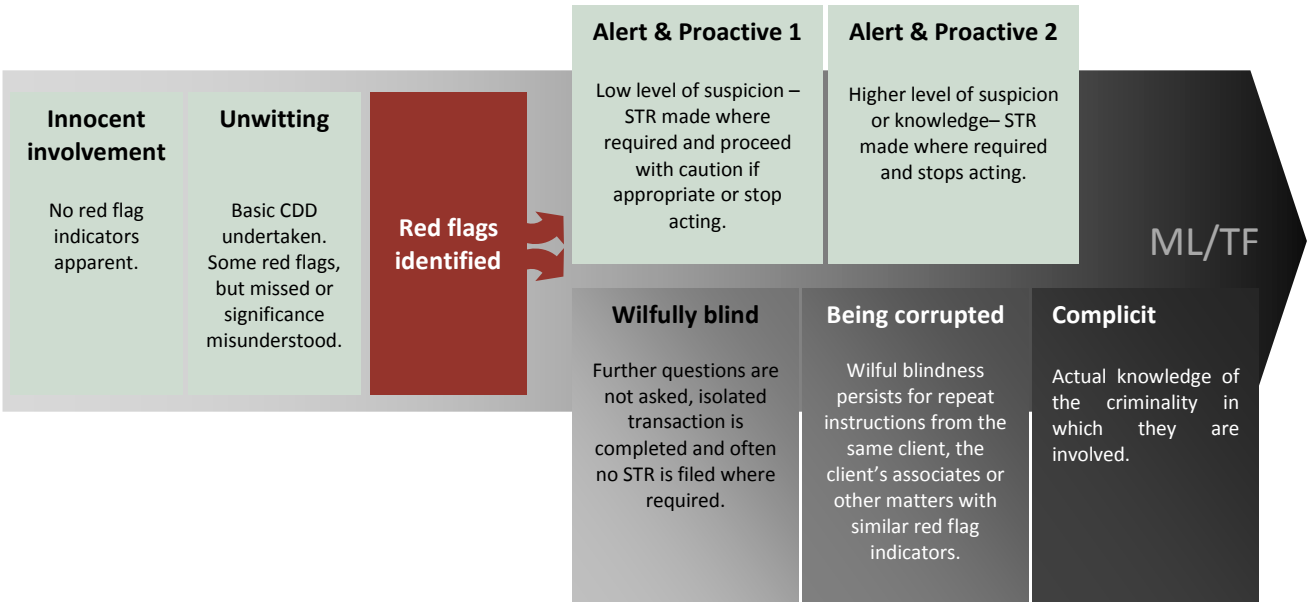
- misuse of client accounts;
- purchase of real property;
- creation of trusts and companies;
- management of trusts and companies;
- managing client affairs and making introductions;
- undertaking certain litigation; and
- setting up and managing charities.

In this report, over 100 case studies referring to these and other ML/TF methods were taken into account. While the majority of case studies in this report relate to ML activity, similar methodologies are capable of being used for TF activity.

While some cases show instances where the legal professional has made a suspicious transaction report (STR), a significant number involve a prosecution or disciplinary action, so a higher standard

of intent had to be proven, meaning those cases were more likely to involve a legal professional who was or became complicit. From reviewing the case studies and literature as a whole, the involvement of legal professionals in the money laundering of their clients is not as stark as complicit or unwitting, but can best be described as a continuum.

Involvement of Legal Professionals in money laundering and terrorist financing (ML/TF)



Red flag indicators relating to the client, the source of funds, the type of legal professional and the nature of the retainer, were developed with reference to these cases and educational material provided by SRBs and competent authorities. Whatever the involvement of the legal professional, the red flag indicators are often consistent and may be useful for legal professionals, SRBs, competent authorities and law enforcement agencies. Red flag indicators should be considered in context and prompt legal professionals to undertake risk-based client due diligence. If the legal professional remains unsatisfied with the client's explanation of the red flags, the next step taken will depend on the unique and complex ethical codes, law governing his or her professional conduct and any national AML/CFT obligations.

Combating ML/TF relies on legal professionals:

- being alert to red flags indicating that the client is seeking to involve them in criminal activity
- choosing to abide by the law, their ethical obligations and applicable professional rules; and
- discerning legitimate client wishes from transactions and structures intended to conceal or promote criminal activity or thwart law enforcement.

While some SRBs and professional bodies are quite active in educating their members on the ML/TF vulnerabilities they face and the red flag indicators which could alert them to a suspicious

transaction, this level of understanding or access to information on vulnerabilities was not consistent across all countries which replied to the questionnaire. A lack of awareness and attendant lack of education increases the vulnerability of legal professionals to clients seeking to misuse otherwise legitimate legal services to further ML/TF activities.

Case studies show that not all legal professionals are undertaking client due diligence (CDD) when required. Even where due diligence is obtained, if the legal professional lacks understanding of the ML/TF vulnerabilities and red flag indicators, they are less able to use that information to prevent the misuse of their services. Greater education on vulnerabilities and awareness of red flag indictors at a national level may assist to reduce the incidence of criminals successfully misusing the services of legal professionals for ML/TF purposes.

Finally, the report challenges the perception sometimes held by criminals, and at times supported by claims from legal professionals themselves, that legal professional privilege or professional secrecy would lawfully enable a legal professional to continue to act for a client who was engaging in criminal activity and/or prevent law enforcement from accessing information to enable the client to be prosecuted. However, it is apparent that there is significant diversity between countries in the scope of legal professional privilege or professional secrecy. Practically, this diversity and differing interpretations by legal professionals and law enforcement has at times provided a disincentive for law enforcement to take action against legal professionals suspected of being complicit in or wilfully blind to ML/TF activity.

CHAPTER 1

INTRODUCTION

BACKGROUND

As financial institutions have put anti-money laundering (AML) measures into place, the risk of detection has become greater for those seeking to use the global banking system to launder criminal proceeds. Increasingly, law enforcement see money launderers seeking the advice or services of specialised professionals to help them with their illicit financial operations.[1]

In 2004, Stephen Schneider[2] published a detailed analysis of legal sector involvement in money laundering cases investigated by the Royal Canadian Mounted Police. This is the only academic study to date which has had access to law enforcement cases and contains a section focussed solely on the legal sector, both in terms of vulnerabilities and laundering methods. His research identified a range of services provided by legal professionals which were attractive to criminals wanting to launder the proceeds of their crime. Some of the services identified include: the purchasing of real estate, the establishment of companies and trusts (whether domestically, in foreign countries or off-shore financial centres), and passing funds through the legal professional's client account.

Financial Action Task Force (FATF) typologies have confirmed that criminals in many countries are making use of mechanisms which involve services frequently provided by legal professionals, for the purpose of laundering money.[3]

A particular challenge for researching money laundering / terrorist financing methods that may involve legal professionals is that many of the services sought by criminals for the purposes of money laundering are services used every day by clients with legitimate means.[4]

There is evidence that some criminals seek to co-opt and knowingly involve legal professionals in their money laundering schemes. Often however the involvement of the legal professional is sought because the services they offer are essential to the specific transaction being undertaken and because legal professionals add respectability to the transaction.[5]

Schneider's study noted that in some cases the legal professional was innocently involved in the act of money laundering. In those cases, there were no overt signs that would alert a legal professional

1 FATF (2004)

2 Schneider, S. (2004)

3 FATF (2006) and FATF (2007)

4 Schneider, S. (2004)

5 Schneider, S. (2004)

that he/she was being used to launder the proceeds of crime. However, Schneider identified other cases where legal professionals continued with a retainer in the face of clear warning signs. He questioned whether it might be the case that legal professionals lacked awareness of the warning signs that they were dealing with a suspicious transaction or were simply wilfully blind to the suspicious circumstances. [6]

Subsequent FATF typologies research mentions the involvement of legal professionals in money laundering/terrorist financing (ML/TF). This research has generally tended to focus more on how the transactions were structured, rather than on the role of the legal professional or his/her awareness of the client's criminal intentions.

Organisations representing legal professionals and some academics have sometimes criticised claims that legal professionals are unwittingly involved in money laundering.[7] They have questioned whether it is even possible to identify key warning signs which might justify imposing anti-money laundering/counter financing of terrorism (AML/CFT) requirements on legal professionals and even whether this might be an effective addition to the fight against money laundering and terrorist financing.[8]

Further, certain sources suggest that legal professionals are required to adhere to strict ethical or professional rules and this fact should therefore be a sufficient deterrent to money laundering or terrorist financing occurring in or through the legal sector. Following this same line of thinking, these sources of existing criminal law may sufficiently deter legal professionals from wilfully engaging in money laundering[9].

Since Schneider's 2004 study, a number of countries have implemented the FATF Recommendations for legal professionals.[10] This extension of AML/CFT requirements to the legal professions has created the need for legal professionals, their supervisory bodies and financial intelligence units (FIUs) to better understand how legal services may be misused by criminals for money laundering and terrorist financing.

This typology study was undertaken to synthesise current knowledge, to systematically assess the vulnerabilities of the legal profession to involvement in money laundering and terrorist financing, and to explore whether red flag indicators can be identified so as to enable legal professionals to distinguish potentially illegal transactions from legitimate ones.

---

6 Schneider, S. (2004), pp. 72

7 Middleton, D.J. and Levi, M. (2004), pp 4

8 Middleton, D.J. and Levi, M. (2004), pp 4

9 For example the CCBE Comments on the Commission Staff Working Document "The application to the legal profession of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering" www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_130207_CCBE_comme1_1194003555.pdf

10 FATF Recommendations 22(d), 23(a) and Interpretative Note to Recommendations 23 and 28 (b).

OBJECTIVES

The key objectives of this report:

1. Identify the different functions and activities within the legal profession on a world-wide basis, the different types of AML/CFT supervision for the legal profession and the key issues raised by stakeholders on why applying an AML/CFT regime to the legal profession has been challenging.

2. Identify examples where legal professionals have been complicit in money laundering, with a view to identifying red flag indicators and why their services were of assistance to criminals.

3. Identify specific types of transactions in which legal professionals may have been unknowingly involved in money laundering, with a view to identifying red flag indicators and why their services are of assistance to criminals.

4. Obtain information on the level of reporting from the legal profession and the types of matters reported, with a view to identifying red flag indicators.

5. Consider how the supervisory structure and legal professional privilege, professional secrecy, and confidentiality influences reporting approaches across the legal profession, along with the role ethical obligations did play or should have played in the case studies obtained.

6. Identify good practice in terms of awareness raising and education of the legal profession, positive interaction between law enforcement and professional bodies, and the role of effective sanctioning by either professional bodies for ethical breaches and law enforcement for criminal conduct.

There is extensive literature and litigation on the question of the appropriateness of the inclusion of legal professionals in the AML/CFT regime in the light of their ethical obligations and a client's fundamental rights.[11] There has also been extensive debate as to whether legal professionals are complying with legal obligations to undertake CDD and make suspicious transaction reports (STRs) when this requirement applies to the profession.[12]

Analysing these issues from a policy perspective is not within the scope of a typology study. This report discusses some of the ethical obligations of legal professionals and considers the remit of legal professional privilege/professional secrecy; however, it does so to describe the context in which legal professionals operate. The report also examines the context in which legal professionals covered by the FATF Recommendations undertake their activities and how those Recommendations have been applied in a range of countries. This in turn, will assist in assessing the ML/TF vulnerabilities facing the legal profession. Likewise, the report looks at suspicious transaction reporting by legal professionals with the aim of identifying areas of potential vulnerability, which legal professionals are themselves recognising.

11 Gallant, M. (2010); Levi, M. (2004); Chervier, E. (2004)

12 European Commission(2006); Deloitte (2011)

METHODOLOGY USED IN THIS STUDY

Led by the Netherlands and the United Kingdom, the project team was made up of experts from: the Asia Pacific Group on Money Laundering (APG), Australia, Austria, Canada, China, Denmark, France, the Group of International Finance Centre Supervisors (GIFCS), Italy, the MONEYVAL Committee of the Council of Europe, Switzerland, the United States and the World Bank. In addition, to government and law enforcement representatives, the project team included members from the private sector having supervisory responsibilities for AML/CFT compliance.

In preparing this report, the project team has used literature and initiatives from the sources listed below (a detailed list of these sources is included in Annex 1). The research relies on literature and studies from 2003 onwards to ensure a focus on more current case examples and determine whether vulnerabilities persisted following the inclusion of legal professionals in the FATF Recommendations.

- Typologies studies previously undertaken by FATF.
- Other studies produced by international organisations such as the World Bank and the Organisation for Economic Co-operation and Development (OECD).
- Research initiatives carried out by academics and consultants either within individual countries or on a regional basis.
- Research initiatives carried out by government authorities.
- Research initiatives undertaken by AML/CFT supervisors, non-government organisations and the private sector.

To supplement information from these sources, the project team also developed two questionnaires: one for FATF members and associate members and one for self-regulatory bodies (SRBs) and professional bodies (a list of countries who responded to the questionnaire is available in Annex 2).

The project team received 76 responses to the questionnaire were received from October 2012 to January 2013 from 38 countries. Responses were from both civil and common law countries and included members of FATF, the Caribbean Financial Action Task Force (CFATF), GIFCS, the Middle East and North Africa Financial Action Task Force (MENAFATF) and Moneyval. SRBs and professional bodies also provided responses.

A workshop on money laundering and terrorist financing in the legal sector was held during the joint FATF/GIABA (Intergovernmental Action Group against Money Laundering in West Africa) experts' meeting on typologies held in Dakar, Senegal, in November 2012. Presentations were made by participating representatives from government departments, FIUs and law enforcement agencies (Netherlands, Canada, Nigeria, the United Kingdom) as well as from AML/CFT supervisors (Spain, Gibraltar and the Netherlands) and from the International Bar Association.

The workshop considered:

- Ethical challenges for the legal profession;

- Good practice in supervision;
- The usefulness of STRs filed by legal professionals; and
- Money laundering case studies demonstrating different types of involvement by legal professionals, in order to identify vulnerabilities and red flag indicators.

Informal workshops were also held in February 2013 with the American Bar Association and the Council of European Bars to consider a number of the case studies identified from the literature review and the FATF questionnaire responses. The purpose of these workshops was to consider case studies from the perspective of the private sector to understand the professional, ethical and legal obligations of the range of legal professions in different countries, as well as identify warning signs of money laundering for either the legal professionals themselves or the SRBs representing them.

The literature review, workshops and questionnaire responses painted a consistent picture of the vulnerabilities of legal professionals, as well as a consistent view of the red flag indicators, which may be of use for legal professionals, supervisors and law enforcement.

These sources also provided an extensive collection of cases demonstrating different types of involvement of legal professionals in money laundering and a few cases involving possible terrorist financing. While the majority of case studies in this report relate to ML activity, similar methodologies are capable of being used for TF activity.

In May 2013, a consultation on the draft report took place in London with representatives from the legal sector, who had previously contributed to the typology project. This consultation aimed to ensure that nuances specific to different legal systems and countries where sufficiently recognised and that the responses provided to the questionnaire by SRBs and professional bodies where accurately reflected in the report.

CHAPTER 2

SCOPE OF THE LEGAL SECTOR

The FATF Recommendations, including in the most recent revision of 2012, apply to legal professionals only when they undertake specified financial transactional activities in the course of business. The Recommendations do not apply where a person provides legal services 'in-house' as an employee of an organisation.[13]

This section examines the context in which legal professionals covered by the FATF Recommendations undertake their activities and how those Recommendations have been applied in a range of countries[14].

TYPES OF LEGAL PROFESSIONALS AND THEIR ROLES

Legal professionals are not a homogenous group, from one country to another or even within an individual country.

There are approximately 2.5 million legal professionals practicing in the countries covered by the questionnaire responses.. The size of the sector within each country ranged from 66 legal professionals to over 1.2 million. Titles given to different legal professionals varied between countries, with the same title not always having the same meaning or area of responsibility from one country to another. While some generalisations can be made depending on whether the country has a common law or civil law tradition, even these will not always hold true in all countries. See Annex 4 for a discussion of the types of activities undertaken by legal professional identified through the questionnaire responses.

The range of activities carried out by legal professions is diverse and varies from one country to another. It is therefore important that competent authorities understand the specific roles undertaken by different legal professionals within their respective country when assessing the vulnerabilities and risks that concern their legal sector.

13 Annex 3 contains the relevant definitions for the range of legal professions considered in this report.

14 Jurisdictions that responded to the questionnaire.

APPLICATION OF AML/CFT OBLIGATIONS

In 2003, FATF issued updated Recommendations, which for the first time specifically included legal professionals.

The FATF Recommendations have explicitly required legal professionals to undertake CDD[15] and to submit STRs since the revision of the Recommendations in 2003. From that time, competent authorities have also been required to ensure that legal professionals are supervised for AML/CFT purposes.

As evidenced by mutual evaluation reports[16], full implementation of these specific Recommendations has not been universal. As a consequence, a major part of the legal profession is not covered.

In order to assess the current vulnerabilities, the project team felt it was important to understand in what situations legal professionals were covered by the AML/CFT obligations within their countries and how these obligations applied to them. The application of the CDD and reporting obligations are discussed below, while the approach to the supervisory obligations is covered in Chapter 3.

From the questionnaire responses, while countries have continued to transpose the requirements almost every year since 2001, the majority of countries did so between 2002 and 2004 and between 2007 and 2008.

CLIENT DUE DILIGENCE

Box 1: **Recommendation 22**

The customer due diligence and record-keeping requirements set out in Recommendations 1, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

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

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

15 CDD includes identifying and verifying the identity of the client, beneficial owners where relevant, understanding the nature and purpose of the business relationship (including the source of funds). Records of the CDD material must be maintained.

16 The third round of mutual evaluations was based on the 40+9 Recommendations. The FATF Recommendations were revised in 2012, for the fourth round of mutual evaluations, due to begin after the publication of this report.

The majority of countries that apply CDD obligations to legal professionals have done so through national law. A few countries also have SRB-issued guidance to reinforce the legal requirements or provide specific details of the requirements.

In three of the four responses to the questionnaire, where legal professionals are not currently subject to CDD provisions as set out in the FATF Recommendations[17], a number of professional bodies have applied some CDD requirements to their members.

To ensure compliance with international obligations imposed by the United Nations and the FATF regarding targeted financial sanctions, many countries require legal professionals to have regard to whether a client is on a sanctions list. In the United States this list also includes known terrorists, narcotics traffickers and organised crime figures. While this is a separate requirement, apart from the AML/CFT CDD obligations, it does require legal professionals to have some understanding of the identity of their client.

REPORTING OBLIGATIONS

Box 2: **Recommendation 23**

The requirements set out in Recommendation 18 to 21 apply to all DNFBPs, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transaction when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

Interpretive Note to Recommendation 23

1. Lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: a) in the course of ascertaining the legal position of their client, or b) in performing their task of defending or representing the client in, or concerning judicial, administrative, arbitration or mediation proceedings.
3. Countries may allow lawyers, notaries, other independent legal professionals and

17 Australia, Canada (although notaries in British Columbia are covered in law), and the United States. In Turkey the law applying the obligations has been suspended awaiting the outcome of legal action, but no specific due diligence requirements have been applied by the relevant professional body. In Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations provide that lawyers must undertake client identification and due diligence, record-keeping and internal compliance measures when undertaking designated financial transactions. These provisions are in force but are inoperative as a result of a court ruling and related injunctions.

accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.

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

The reporting obligations in the countries which responded to the questionnaire can be characterised as follows:

- Where the obligation to file an STR is applied to legal professionals the obligation is always contained in law rather than guidance.
- In the majority of countries, the STR is submitted directly to the FIU. In seven[18] of the countries, the STR is filed with the SRB. These are civil law countries in Europe.
- In the two of the four countries where AML/CFT obligations for filing an STR have not been extended to legal professionals[19], there is a requirement to comply with threshold reporting, which applies to cash payments above a certain amount. In such cases, the legal professional reports with the knowledge of the client.
- A few[20] countries combine the requirement to make an STR with threshold reporting.

UNIQUE FEATURES OF THE SECTOR

ETHICAL OBLIGATIONS

Ethical obligations apply to legal professionals and the work they undertake.

During the joint FATF/GIABA experts' meeting in November 2012 the International Bar Association (IBA) presented its *International Principles on Conduct for the Legal Profession*[21] and outlined some of the competing ethical requirements that legal professionals (other than notaries) must consider when complying with AML/CFT requirements.

The IBA principles were adopted in 2011 and are not binding for member bar associations and law societies. Each professional association and legal sector regulator or supervisor has its own ethical or professional rules or code of conduct[22]. Many – but not all -- are able to enforce compliance with those rules and have the power to remove legal professionals from practice.

18 Belgium, Czech Republic, Denmark, France, Germany, Luxembourg, and Portugal.

19 Australia and the United States.

20 Curacao requires all cash transactions over 20 000 to be reported, while in Montenegro all contracts for sale of real property must be filed in addition to STRs being made.

21 International Bar Association (2011)

22 Note – in countries which have a federal system, this can differ from state to state as well.

While differences may apply in individual countries, the relevant principles from the IBA are outlined below to give an indication of the types of professional obligations which apply to legal professionals other than notaries.

Box 3: **The IBA principles on conduct for the legal profession**

1. **Independence**

   A legal professional shall maintain independence and be afforded the protection such independence offers in giving clients unbiased advice and representation. A legal professional shall exercise independent, unbiased professional judgment in advising a client, including as to the likelihood of success of the client's case.

2. **Honesty, integrity and fairness**

   A legal professional shall at all times maintain the highest standards of honesty, integrity and fairness towards the lawyer's clients, the court, colleagues and all those with whom the lawyer comes into contact.

3. **Conflicts of interest**

   A lawyer shall not assume a position in which a client's interest conflict with those of the lawyer, another lawyer in the same firm, or another client, unless otherwise permitted by law, applicable rule of professional conduct, or, if permitted, by client's authorisation.

4. **Confidentiality/professional secrecy**

   A legal professional shall at all times maintain and be afforded protection of confidentiality regarding the affairs of present or former clients, unless otherwise allowed or required by law and/or applicable rules of professional conduct.

   Commentary on the principle: However a legal professional cannot invoke confidentiality/professional secrecy in circumstances where the legal professional acts as an accomplice to a crime.

5. **Clients' interests**

   A legal professional shall treat client interests as paramount, subject always to there being no conflict with the legal professional's duties to the court and the interests of justice, to observe the law, and to maintain ethical standards.

   Commentary on the principle: Legal professionals must not engage in, or assist their client with, conduct that is intended to mislead or adversely affect the interests of justice, or wilfully breach the law.

The role of a notary varies significantly depending on whether the professional is a civil-law notary or public law notary, and accordingly the professional and public obligations of a notary vary from country to country. However, the relevant principles from the International Union of Notaries code of ethics[23] provides an indication of the general principles:

[23] International Union of Notaries (2004)

Box 4: **International Union of Notaries Code of Ethics**

Notaries must carry out their professional duties competently and with adequate preparation, performing their essential functions of advising, interpreting and applying the law, acquiring specific knowledge of notarial matters and conforming to professional standards.

Notaries must always verify the identities of parties and the capacity in which they are acting. They must also give expression to their wishes.

Notaries must comply with their professional duty of confidentiality both in the course of their professional services and thereafter. They are also obliged to ensure that this requirement is similarly satisfied by their employees and agents.

Notaries are not bound by their professional duty of confidentiality purely as a result of their obligation to act in concert with any public authorities with which they become involved because of a specific regulation or an order of a judicial or administrative body, including in particular the authority responsible for monitoring the propriety of commercial transactions.

Notaries must conduct themselves in the course of their professional duties with impartiality and independence, avoiding all personal influence over their activities and any form of discrimination against clients.

When acting in their official capacity notaries must balance the respective interests of the parties concerned and seek a solution with the sole objective of safeguarding both parties.

Notaries must act suitably and constructively in the discharge of their duties; they must inform and advise the parties as to the possible consequences of their instructions, having regard to all aspects of normal legal procedure for which they are responsible; they must select the judicial form most appropriate to their intentions and ensure its legality and relevance; they must provide the parties with any clarification requested or necessary to ensure conformity with decisions taken and awareness of the legal force of the deed.

Many SRBs consider that these codes of conduct and professional rules prevent legal professionals from being knowingly involved in money laundering or terrorist financing. Furthermore, if a member had doubts about a transaction or client, that the member would either stop acting or refuse to act, as he or she could not, according to the code of ethics, engage in criminal activity with the client.

The case studies show that many areas of the legal professional's work are open to exploitation by criminals and may attract misuse for money laundering or terrorist financing, as criminals identify weaknesses in processes, legislation and understanding of red flag indicators.

Under professional obligations, the duties to the court (and in the case of the notaries - to the public), take precedence over duties to the client, with the result that the legal professional must not engage in criminal conduct and must not act in a way which facilitates their client engaging in criminal conduct.

Participants at the Dakar meeting acknowledged that the FATF Recommendations specifically recognise the challenges posed by legal professional privilege and professional secrecy. The

Recommendations seek to ease that conflict for legal professionals by specifying that there is no requirement to submit an STR when privilege or secrecy applies.

Further, where legal professionals fail to act with integrity by becoming involved in money laundering or terrorist financing, then professional disciplinary action can be considered. Depending on the specific involvement of the legal professional, this can be in addition to, or instead of, taking criminal action against the professional.

However, there are a number of other ethical or professional challenges highlighted in responses to questionnaires and in meetings, particularly with regard to the manner in which the AML/CFT regime applied to legal professionals other than notaries:

- Where there was a requirement in national law to obtain due diligence information and provide it to law enforcement or other competent authorities, especially without the requirement for a court order, many legal professionals considered this to impinge upon their ability to act with appropriate independence.
- Where following the filing of an STR, legal professionals were required to continue with a transaction or expected to do so to avoid tipping off, but were unable to discuss the STR with the client, then some legal professionals felt they were being required by law to continue to act in the face of a conflict of interest. Many expressed the view that if an STR was warranted, it was a sign that the trust at the heart of the client/legal professional relationship had been broken and it was no longer appropriate to act on behalf of the client.

As this is a typology project, it is not appropriate for this report to comment on the merits of these views or to recommend a policy response. However, further consideration of these challenges by others at a future date may assist in more effectively addressing the vulnerabilities identified later in this report.

CLIENT FUNDS

Most legal professionals are permitted to hold client funds.

From the questionnaire responses, the professional body holds the client funds in a few civil law countries[24]. The professional body requires an explanation of who the funds are held for and why, and will monitor the accounts for any unusual transactions which would suggest money laundering.

In almost all other countries however, legal professionals are required to hold client funds in a separate account[25] with a recognised financial institution, and use it only in accordance with their client's instructions and in relation to the provision of legal services.

---

24 Belgium, France, the Netherlands , In Austria the legal professional holds the money but must notify the Bar of any payment over EUR 40 000, while all deposits with a notary in Italy must be recorded in a public register.

25 These accounts have various names, including client accounts and trust accounts.

In many countries there is a requirement to provide an annual report to the professional body that could also inspect the accounts. In a few[26] countries, rules prohibit the acceptance of cash over set limits, although these limits varied significantly. Within some countries, cash is an acceptable form of payment for legal professionals' services, but its receipt is subject to threshold reporting requirements.

These obligations are often outlined in law or professional rules and could be enforced by disciplinary sanctions.

Box 5: **Example of professional body holding client funds: CARPA (France)**

The system in France known as CARPA is outlined below[1]:

This system was introduced by an Act of 25 July 1985 and requires that all income be credited to a special account. There is one CARPA for each Bar, one account for each legal professional member of the Bar and one sub-account for each case.

Any withdrawal of money must be authorised by the CARPA. Any receipt of fees cannot be done without a written authorisation by the client. Any movement of capital from one sub-account to another is forbidden unless authorised by the President of the CARPA.

The sums of money only pass in transit through the CARPA and the CARPA immediately controls the suspicious lack of movement on a sub-account. No sub-account is allowed to be overdrawn.

The CARPA is controlled by an internal committee but also by the bankers and an independent accountant: they check the nature of the case handled by the legal professional, the origin of the money and the identity of the beneficiary of a payment.

1. Chervrier, E. (2004) pp. 194-196.

The use of client accounts has been identified previously[27] as a potential vulnerability, as it may enable criminals to either place money within the financial system and / or use the money as part of their layering activity, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional.

CONFIDENTIALITY, PRIVILEGE AND PROFESSIONAL SECRECY

The right of a client to obtain legal representation and advice, to be candid with his legal adviser and not fear later disclosure of those discussions to his prejudice, is recognised as an aspect of the fundamental right of access to justice laid down in the Universal Declaration of Human Rights.

26 Canada, Italy, the Netherlands and Spain.

27 Schneider (2004); FATF (2004).

As outlined above, the FATF Recommendations recognise this right by excluding information covered by legal professional privilege or professional secrecy from the obligation to file an STR and provides that it is a matter for each country as to what those terms cover.[28]

The terms **confidentiality**, **legal professional privilege** and **professional secrecy** are often used interchangeably to describe the protection provided for this right, but legally each term has a different application, meaning and consequence, depending on the country under consideration.

The area of legal professional privilege and professional secrecy is complex, with subtle differences in application from country to country. The summary below is taken from questionnaire responses and provides a high-level overview.

The concept of **confidentiality** seems to apply to all types of legal professionals and to all information obtained in the course of the legal professional's interaction with clients and potential clients. In most countries, it appears that confidentiality can be waived by the client or overridden by express provisions in law.

Legal **professional privilege** and **professional secrecy** appear to offer a higher level of protection to information than does confidentiality. The remit of legal professional privilege and professional secrecy is often contained in constitutional law or is recognised by common law, and is tied to fundamental rights laid down in treaty or other international obligations.

Often, the protection offered to information subject to legal professional privilege and professional secrecy is also contained in criminal law, either in a statute or a rule of evidence. In many countries, the protection will be given to information received or given either for the purpose of current or contemplated litigation, or for the seeking of advice where the legal professional is exercising their skill and judgement as a legal professional. However, some of the questionnaire responses suggested that the protection applies to all information obtained by or provided to the legal professional

In many countries:

- The client can waive his or her right to legal professional privilege or professional secrecy, but in some countries, the legal professional is obliged to ignore the client's waiver if the professional decides that a waiver is not in the client's best interests.
- Legal professional privilege or professional secrecy will be lost if the legal professional is being used for the purpose of committing a crime or a fraud. However the extent of information needed to invoke the crime/fraud exemption varies from country to country, but is usually higher than the basis on which an STR is required to be filed.
- Legal professional privilege or professional secrecy can be removed by express words contained in a statute but only for limited purposes.

The consequences of a breach of legal professional privilege and professional secrecy also vary from one country to another.

---

28 FATF (2012).

In some countries, such a breach will constitute a criminal offence and the legal professional could be subject to imprisonment. In other countries a breach is sanctioned by disciplinary action and/or the client can sue the legal professional. Therefore, any uncertainty over the extent to which legal professional privilege or professional secrecy is exempt from the STR obligations within a country may expose the legal professional to significant personal liability.

In most countries, if evidence is obtained in breach of legal professional privilege or professional secrecy, that evidence cannot be used in court, and in some cases any other evidence obtained as a result of the inappropriately obtained evidence is also inadmissible. This may cause the prosecution to collapse.

A number of respondents indicated that legal professional privilege and/or professional secrecy did not apply to notaries in their country.

A number of countries also reported there were significant restrictions on their ability to obtain search warrants for a legal professional's office or other orders for the production of papers from a legal professional.

Essentially the remit of confidentiality, legal professional privilege and professional secrecy depends on the legal framework in place in the country under consideration and the specific type of legal professional involved.

There have been four completed legal challenges[29] to the application of AML/CFT obligations to legal professionals in Europe. Each of these cases related to the national implementation of the FATF Recommendations in the specific country and considered the rights of access to justice and to privacy enshrined in the European Convention on Human Rights (ECHR).

In each of those cases, the infringement of the broader rights under consideration by the application of the AML/CFT regime to legal professionals was considered proportionate and appropriate, on the basis that legal professional privilege/ professional secrecy was sufficiently protected. For two of the countries[30], this protection required that STRs be submitted via the SRB rather than directly to the FIU.

Box 6: **Summary of decision in the Michaud case**

In its final decision, given on 6 March 2013, in the case of Michaud v France (request no 12323/11), the European Court of Human Rights unanimously held that there was no violation of Article 8 (right to respect for private life) of the ECHR.

The case concerned the application of the AML/CFT requirements on legal professionals, with respect to the requirement to file STRs. The applicant claimed this obligation contradicted Article 8 of the Convention which protects the confidentiality of the exchanges between a legal professional and his client.

29 Bowman v Fels (2005) EWCA Civ 226; ECJ C-305/05, *Ordre des barreaux francophones et germanophone et al. v. Conseil des Ministres*, 2007; ECHR *André et autres v. France*, 2008 and Michaud v. France ECtHR (Application no. 12323/11).

30 Belgium and France.

The Court underlined the importance of the confidentiality of the exchanges between legal professionals and their clients, as well as the professional secrecy of legal professionals. However the Court considered that the obligation to report suspicious transactions was necessary to achieve the justifiable purpose of the defence of order and the prevention of criminal offences, since it is aimed at fighting against money laundering and associated offences. The Court decided that the implementation of the obligation to report suspicious transactions in France was not a disproportionate infringement on the professional secrecy of legal professionals for two reasons.

Firstly, because they were not required to make a report when they are defending a citizen; and secondly, because French law allows legal professionals to make the report to the president of their bar rather than directly to the authorities.

The questionnaire responses indicate that further litigation on similar issues is currently underway in Monaco and Turkey. In Canada, the Court of Appeal for British Columbia[31] has recently upheld an earlier decision that the application of CDD obligations to legal professionals was constitutionally invalid. The requirement to retain the CDD material was found to constitute an unacceptable infringement of the indepence of legal professionals because of the court's concern that law enforcement might obtain an use this material to investigate clients. The Canadian government is seeking to appeal the decision.

31 Federation of Law Societies of Canada v Canada (Attorney General) 2013 BCCA 147.

CHAPTER 3

VULNERABILITIES

VULNERABILITIES IDENTIFIED IN LITERATURE

The literature reviewed for this typology suggested that criminals would seek out the involvement of legal professionals in their money laundering schemes, sometimes because a legal professional is required to complete certain transactions, but also, to access specialised legal and notarial skills and services which could assist in laundering the proceeds of crime and in the financing of terrorism.

Key ML/TF methods that commonly employ or, in some countries, require the services of a legal professional were identified in the literature as follows:

- use of client accounts
- purchase of real property
- creation of trusts and companies
- management of trusts and companies
- setting up and managing charities

While not all legal professionals are actively involved in providing these legitimate legal services which may be abused by criminals, the use of legal professionals to provide a veneer of respectability to the client's activity, and access to the legal professional's client account, is attractive to criminals.

There is also a perception among criminals that legal professional privilege/professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional.

In terms of TF, while few case studies specifically mention the involvement of legal professionals, they do mention the use of companies, charities and the sale of property. As such it is clear that similar methods and techniques could be used to facilitate either ML or TF, although the sums in relation to the later may be smaller, and therefore the vulnerability of legal professionals to involvement in TF cannot be dismissed.[32]

[32] FATF (2008)

VULNERABILITIES IDENTIFIED THROUGH STRS AND ASSET RECOVERY

STRs and confiscated assets are two data sets that can provide information for competent authorities to assess the extent of AML/CFT risk and vulnerability within their country. The observations below are taken from responses to the FATF questionnaire.

CONFISCATION OF ASSETS

The types of assets acquired by criminals with the proceeds of their crime are evidence of the laundering methods utilised and highlight areas of potential vulnerability. Real estate accounted for up to 30% of criminal assets confiscated in the last two years, demonstrating this as a clear area of vulnerability.

REPORTS ABOUT LEGAL PROFESSIONALS

Analysis of the STRs information provided in the FATF questionnaire responses reveals that financial institutions and other designated non-financial businesses and professions (DNFBPs) were reporting suspicious transactions involving legal professionals, whether they were complicitly or unknowingly involved in their client's criminality. These STRs mentioning potential involvement of legal professionals in money laundering amounted to between .035% and 3% of all STRs reported[33].

REPORTING BY LEGAL PROFESSIONALS

The table below shows the number of reports as identified via the FATF questionnaire[34].

The wide range of activities undertaken by different types of legal professionals in different countries complicates comparisons. In certain countries, notaries and/or solicitors undertake the majority of transactional activities and advocates, barristers or legal professionals have a predominantly advocacy-based role. In these situations, there are naturally more reports originated by the former group than the latter.

The level of reporting by the legal sector is unlikely to be at the same level as that of the financial institutions. There is a significant difference in the volume of transactions undertaken by legal professionals in comparison to financial institutions. Also, the level of involvement in each transaction, which affects the basis on which a suspicion may arise and be assessed, is significantly different.

A more relevant comparison may be to other DFNBPs, especially those providing professional services. From the figures below, the reports by legal professionals averaged 10% of those of DFNBPs, ranging from less than 1% to 20%. Understanding the proportion of the legal sector to the rest of the DFNBPS in a country makes such a comparison more informative.

---

33 These figures were calculated by comparing the number of STRs identified by the FIU in the questionnaire response as having a legal professional as a subject, with the total number of STRs in that jurisdiction for the relevant year.

34 Not all of the thirty-eight jurisdictions which responded to the questionnaire provided STR figures.

However, given the number of legal professionals in each of the countries responding to the FATF questionnaire and the range of transactions they are involved in, reporting levels of zero or even single figures year after year, raises the question as to the underlying reasons relevant to that country. Chapter 6 of this report considers a number of possible contributing factors to the current reporting levels.

Table 1: **Sampling of Suspicious Transaction Reports Filed in 2010 from those countries responding to the questionnaire**

	Legal professionals			DNFBPs	Total
Country	Advocate/ Barrister/ Lawyer	Notary/Other	Solicitor		
Austria	23			-	2 211
Belgium	0	163		1 179	18 673
Curacao	0	0		69	757
Denmark	4			26	2 315
Finland	7			4 040	21 454
France		881		1 303	19 208
Hong Kong/China	99			157	19 690
Ireland			19	82	13 416
Italy	12	66		223	37 047
Jordan	0			0	208
Liechtenstein [1]	5			113	324
Montenegro	0			-	68
Netherlands [2]	27	356		-	198 877
Norway	7			82	6 660
Portugal	5			-	1 459
St Vincent and Grenadines	0			1	502
Spain	39	345		580	2 991
Sweden	1			321	12 218
Switzerland	13			322	1 146
Trinidad and Tobago	0			25	111
United Kingdom	11	141	4 913	13 729	228 834

Table Notes:

1. Legal professionals in Liechtenstein only report when acting as a financial intermediary, rather than when performing activities set forth in the list contained in FATF Recommendation 22(d).

2. The Netherlands requires reports of unusual transactions rather than suspicious transactions.

Table 2: **Sampling of Suspicious Transaction Reports Filed in 2011 from those countries responding to the questionnaire**

Country	Legal Professionals			DNFBPs	Total
	Advocate/ Barrister/ Lawyer	Notary/Other	Solicitor		
Austria	10			-	2 075
Belgium	1	319		1 382	20 001
Curacao	3	7		887	10 421
Denmark	5			14	3 020
Finland	16			6 247	28 364
France		1 357		1 691	22 856
Hong Kong/China	116			161	20 287
Ireland			32	129	11 168
Italy	12	195		492	48 836
Jordan	0			0	248
Liechtenstein [1]	5			142	289
Montenegro	1			-	50
Netherlands [2]	11	359		-	167 237
Norway	11			68	4 018
Portugal	7			-	1 838
St Vincent and Grenadines	0			1	255
Spain	31	382		537	2850
Sweden	0			321	11 461
Switzerland	31			527	1 615
Trinidad and Tobago	2			90	303
United Kingdom	4	166	4 406	11 800	247 160

Table Notes:

1. Legal professionals in Liechtenstein only report when acting as a financial intermediary, rather than when performing activities set forth in the list contained in FATF Recommendation 22(d).

2. The Netherlands requires reports of unusual transactions rather than suspicious transactions.

Most countries who responded to the survey indicated that they did not separate record STRs relating to TF from those relating to ML. A handful of jurisdictions reported receiving TF specific STRs from DNFBPs and one jurisdiction reported receiving STRs in double figures for 2010 and 2011 from legal professionals which related specifically to TF.

In light of the approach to recording statistics and the similarities of the methodologies for ML and TF, while the STRs do not provide a clear picture of the vulnerabilities of the legal profession to TF, again they certainly do not provide a case for dismissing that vulnerability.

REPORTING ON CLIENTS

Respondents to the FATF questionnaire advised that almost all the STRs submitted by the legal profession are on their own clients. The FATF Recommendations state that STRs should relate to all funds, irrespective of whether they are held by the client or third parties. Only the United Kingdom and Norway identified STRs being made by legal professionals in this broader context.

VULNERABILITIES IDENTIFIED BY LEGAL PROFESSIONALS

Respondents to the FATF questionnaire identified that, among the STRs submitted by legal professionals, the top four areas reported are:

- Purchase and sale of real property,
- Formation, merger, acquisition of companies,
- Formation of trusts and
- Providing company or trust services.

A number of countries' legal professionals also identify probate (administering estates of deceased individuals), tax advice and working for charities as areas giving rise to circumstances requiring them to file an STR.

The top five predicate offences featuring in STRs from legal professionals among the respondent countries were:

- corruption and bribery
- fraud
- tax crimes
- trafficking in narcotic drugs and psychotropic substances
- unclear offences, but unexplained levels of cash or private funding

STRs from legal professionals in a few countries also identified a range of other offences such as terrorism, trafficking in human beings and migrant smuggling, insider trading, and forgery. .

USEFULNESS OF STRS BY LEGAL PROFESSIONALS

It is difficult to assess the direct usefulness of individual STRs, as the collection of feedback in many countries is sporadic. However, from the level of case studies and questionnaire responses, it appears that STRs submitted by legal professionals are often of high quality and lead to further action.

For example, Switzerland reported that 93.5% of STRs from legal professionals were passed to law enforcement, with 62% resulting in proceedings being instituted. In addition, Belgium, Italy, Liechtenstein, Ireland and the United Kingdom commented positively on the general quality of the STRs provided by legal professionals. While the United Kingdom and the Netherlands noted that STRs from legal professionals contributed to both law enforcement activity and prosecutions, as well as assisting in identifying and locating the proceeds of crime for confiscation activity.

A number of case studies contained in Chapter 4 and Annex 6 of this report demonstrate successful prosecutions, where a legal professional has filed an STR.

SUPERVISION OF LEGAL PROFESSIONALS

Box 7: **Recommendation 28**

Countries should ensure that other categories of DNFBPS are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by a) a supervisor or b) by an appropriate SRB, provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a 'fit and proper' test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML.CFT requirements.

APPROACH TO SUPERVISION

Supervisors generally have the opportunity to monitor the conduct of all of their members, irrespective of whether there has been a complaint of potentially criminal conduct or professional misconduct. Therefore, they are a potential source of information on vulnerabilities of a sector, even where the existence or exploitation of the vulnerability has not yet come to the attention of law enforcement agencies. An absence of supervision may aggravate pre-existing vulnerabilities.

The questionnaire responses show a number of different supervisory frameworks which have been implemented for legal professionals:

- Twenty-three countries have allocated supervisory responsibility to SRBs. In many cases there is interaction with either the FIU or a relevant government ministry on the overall approach to supervision.
- Five countries have allocated supervisory responsibility to the FIU. In all cases, the professional bodies are involved in providing advice on compliance to their members.
- Three countries have allocated supervisory responsibility to other external supervisors. In each of those cases the professional bodies liaised with the external supervisor on compliance and education.
- In two countries it was unclear from responses who had supervisory responsibility, and another two countries were in the process of establishing supervisors for the legal profession.

- In three of the four countries that responded to the questionnaire where AML/CFT obligations have not been extended to legal professionals[35], the FIU, relevant government departments and/or professional bodies provide some advice on ML/TF risks. They either have a role in monitoring compliance with professional rules or in monitoring compliance with threshold reporting obligations.

The SRBs generally indicated that they had the ability to refuse membership admission to those persons who either did not meet a fit and proper test or who had relevant criminal convictions.

The SRBs also indicated they had the power to monitor compliance and take disciplinary action, although some mentioned they had very limited resources with which to undertake this role.

A few of the external supervisors/FIUs mentioned that due to constitutional requirements regarding access to the offices of legal professionals, they either undertook their supervisory functions with the consent of the legal professionals or they had delegated the onsite inspections to the professional body.

EDUCATION AND RAISING AWARENESS

Almost all countries that responded to the questionnaire provide education, advice and guidance to legal professionals on AML/CFT compliance, and a number provided links to a large range of detailed educational material.

However, debate is ongoing within some countries about the type of red flag indicators that legal professionals should be educated about:

- Twenty-two countries either did not answer the question or said that there were no specific risks or red flag indicators for legal professionals;
- Two countries have only recently applied the AML/CFT obligations to legal professionals and are in the processes of developing red flag indicator relevant to their country;
- Of the remaining respondents in some cases both the FIU and the SRB or professional body were able to articulate risks to the legal sector and red flag indicators relevant to the activities of legal professionals. In other cases it was only the FIU or the SRB which provided that information.

In one country, the two SRBs who responded, had actively co-operated with the FIU in compiling a very detailed list of red flag indicators for legal professionals, although in their responses they stated that they were not aware of specific risks to their members.

Only one SRB said that the lack of information about warning signs and lack of disciplinary action suggested to them that the potential for misuse of their members was high. On the other hand a number of SRBs who did not provide information on red flag indicators thought that the fact that they did not need to take disciplinary action against their members was an indication that the

35 Australia, Canada and the United States – although the Canadian FIU is the AML/CFT supervisor for the Notaries in British Columbia.

ML/TF risks to their members must be low or that their members were able to deal with the risks adequately.

The questionnaire specifically asked about the interaction between SRBs and professional bodies, and FIUs. Five of the private sector respondents mentioned that they did not have any interaction with the FIU in their country, and four of those were SRBs. A further three SRBs did not respond to the questions about interaction with the FIU. Generally these respondents indicated that they would have welcomed dialogue with the FIU and thought that this would assist them in helping to improve compliance by their members.

DISCIPLINARY AND CRIMINAL SANCTIONS IMPOSED ON LEGAL PROFESSIONALS

Disciplinary and criminal action taken against legal professionals helps to identify areas of vulnerability and provides case studies of both witting and unwitting involvement. The FATF questionnaire specifically looked at disciplinary and criminal action within the preceding five years.

SRBs from ten countries provided advice about disciplinary action taken, however the number of disciplinary cases reported exceeded double figures only in the Netherlands, the United Kingdom and the United States.

Criminal prosecutions were started in sixteen countries, with Austria, Spain, Italy, and Poland joining the Netherlands, the United Kingdom and the United States reaching double figures of prosecutions in the last five years.

For both disciplinary and criminal actions only a small number were substantiated to the relevant standard of proof and resulted in sanctions. The United Kingdom and the United States provided the most examples of successful disciplinary and criminal prosecutions.

The individual case studies provided have been included in both Chapter 4 and Annex 6 of this report and the red flag indicators and other lessons to be learnt from those cases are considered in more detail in those sections. Some also contain details on sanctions imposed, which range from fines to removal from practice to imprisonment.

The case studies clearly demonstrate that criminals still seeking to exploit the vulnerabilities that caused the FATF to call for extending AML/CFT obligations to legal professionals. However, the case studies also show that, at least in some instances, it is now the legal professional who becomes aware of the attempted misuse of their services and submits an STR that then prompts an investigation.

TAKING ENFORCEMENT ACTION AGAINST LEGAL PROFESSIONALS

Within the literature and other typology research, law enforcement often cites “challenges” in successfully prosecuting legal professionals for money laundering as a basis for legal professionals posing a greater risk of ML/TF.

While the actual ML/TF offences are the same for legal professionals as they are for ordinary citizens, a number of potential hurdles to prosecuting legal professionals have been identified.

EVIDENCE GATHERING

Most of the practical issues concerning the investigation of ML/TF by or through legal professionals relate to legal professional privilege or professional secrecy and the process of gathering evidence. FATF Recommendation 31 is relevant as it stipulates that the powers of law enforcement agencies and investigative authorities should include evidence-gathering methods and compulsory measures for the production of records held by DNFBPs. Whether any evidence gathered or created in the course of an investigation is subject to legal professional privilege or professional secrecy is a legal issue that cannot be predicted with certainty. Some of the practical challenges identified in investigating ML/TF by or through legal professionals include: uncertainty about the scope of privilege, the difficult and time-consuming processes for seizing legal professional's documents, and the lack of access to client account information.

DIFFERENCES IN SCOPE OF PRIVILEGE

As outlined in Chapter 2 of this report, legal professional privilege and professional secrecy are considered fundamental human rights and the legal professional is obliged to take steps to protect that privilege. However, the remit of confidentiality, legal professional privilege and professional secrecy varies from one country to another, and the practical basis on which this protection can be overridden is not always clear or easily understood. In some countries, the FIU may have greater powers to access underlying information on which an STR is based, while in other countries it is also possible for law enforcement to have access to such material.

In some countries financial and banking records may be accessed just as easily for legal professionals as for any other individual, while tax information may be accessed easily by some law enforcement agencies. But in other countries this kind of information is also subject to privilege. In some countries, both law enforcement agencies and the private sector have said that they find the lack of clarity on the extent of the reporting duty under the AML/CFT legislation challenging.

DOCUMENTS

Regulatory officials, police, and prosecutors must be careful to respect solicitor-client privilege during the course of their work. This can result in an increase in time and resources required to build a case against a legal professional when compared to other persons or professionals. A number of the questionnaire responses highlighted this point, especially in relation to the seizure of documents from a legal professional's office – whether provided by the client or created by the legal professional.

Claims of legal professional privilege or professional secrecy could impede and delay the criminal investigation. Once a claim of privilege is made over a document obtained pursuant to a search warrant, for example, the document is essentially removed from consideration in the investigation until the claim for legal professional privilege is resolved.

This delay may still occur were the claim is made correctly and in accordance with the law, or if made with the genuine but mistaken belief by the legal professional that privilege or secrecy applies. This may be particularly relevant if there is misunderstanding of the extent of privilege or secrecy in particular circumstances by either the legal professional or law enforcement, or if there is a dispute

as to whether any of the grounds for removing the privilege or secrecy (such as the crime fraud exemption) apply. However, some of the case studies do evidence extremely wide claims of privilege or secrecy being occasionally made which exceed the generally understood provisions of the protections within the relevant country, an experience which was reflected in some of the responses to the questionnaire.

Law enforcement agencies are required by law to have strong evidence from the outset to demonstrate that privilege or secrecy should be removed. In many instances this means that the claim of legal professional privilege or professional secrecy will need to be resolved by a court, which can delay the investigation process for a substantial period of time. As time is a critical factor in pursuing the proceeds of crime, this may influence the decision of investigators of whether to investigate the possible involvement of the legal professional or to seek evidence of their client's activities from alternative sources. .

CLIENT ACCOUNTS

Several countries stated that tax authorities, police and prosecutors do not have the right to investigate transactions that touch legal professionals' client accounts, as these are covered by confidentiality requirements. Sight of such accounts can of course be given voluntarily by those under investigation, but this is a practical solution only where the investigating agency is willing to reveal the fact that they are conducting the investigation.

OTHER CHALLENGES

The use of certain investigative techniques such as intercepting the telephone or electronic communications may be virtually forbidden when those communications involve legal professionals. In some countries, prior consent to the recording by a party to the communication or the subsequent removal of sections of the recorded conversations covered by legal professional privilege or professional secrecy may permit some limited use of this technique.

Some countries noted the special position of the legal professional within a legal community as presenting a challenge in being permitted to investigate legal professionals. Legal professionals and judges will often be well-known to each other and the question has been raised of whether a court is obliged to find a judge who is not known by a defendant or suspect legal professional, and who is therefore demonstrably impartial.

PROSECUTING LEGAL PROFESSIONALS

Legal professionals have professional training, and even if they do not "know" the AML laws, they will generally be sufficiently aware to avoid crossing the line between questionable behaviour and criminality, making it more difficult to prove the relevant mental element in a money laundering prosecution. More importantly, if they do cross that line knowingly and willingly, legal professionals, especially in law firms, have access to employees who can establish companies or accounts (thus, further insulating the legal professional). Legal professionals who cross the line may also have access to other professionals (in both the legal and financial sectors) who can help them layer and conceal the proceeds of crime involved in money laundering transactions. Lastly, being a member of

the bar, affords a certain standing and prestige in society. This may cause others with whom the legal professional interacts, to favour or trust him/her, merely due to his/her status, when they would otherwise look suspiciously upon certain behaviour.

Responses to the questionnaire showed that in some cases, legal professionals were not charged with the criminal offence of money laundering although it was clear to the investigating officers that they were involved in the ML/TF activity. Two main reasons were provided as to why this may be the case:

- Firstly, because of the inability to secure sufficient evidence to prove their complicit involvement in the money laundering schemes. Domestically, access to evidence may have been refused because claims to legal professional privilege or professional secrecy were upheld; or investigators decided not to pursue that evidence because of the more complicated processes involved in seeking access to such evidence and demonstrating that it is appropriate to be released. In the case of an international investigation, the evidence-gathering process can be hindered by the fact that privilege and secrecy varies across the countries that are trying to co-operate.
- Secondly, because they are likely to make useful co-operators, informants, and/or cooperating witnesses. A legal professional has every incentive to co-operate with law enforcement once his/her illegal activity is discovered to avoid reputational harm, loss of license (livelihood), and censure by the bar.

CHAPTER 4

MONEY LAUNDERING TYPOLOGIES

This section of the report looks at case studies which illustrate the ML/TF methods and techniques which involve the services of a legal professional.

FATF recognises that the vast majority of legal professionals seek to comply with the law and their ethical obligations, and will not deliberately seek to assist clients with money laundering or terrorist financing. This report has identified case studies where legal professionals have stopped acting for clients and/or made an STR; although comprehensive information about the extent to which this occurs is not available, especially in the absence of a reporting obligation being imposed at a country level. [36]

However, as identified in Chapter 3, there are a range of legal services which are of interest to criminals because they assist in laundering money and may assist in terrorist financing.

The criminal may seek out the use of a legal professional, because they need expert advice to devise complicated schemes to launder vast amounts of money, and they will either corrupt the legal professional or find one who is already willing to wilfully assist them.

However in many other cases, the criminal will use the legal professional because:

- either by virtue of a legal requirement or custom, a legal professional is used to undertake the otherwise legitimate transaction, which in that instance involves the proceeds of crime;
- the involvement of a legal professional provides an impression of respectability sought in order to dissuade questioning or suspicion from professionals and/or financial institutions; or
- the involvement of a legal professional provides a further step in the chain to frustrate investigation by law enforcement.

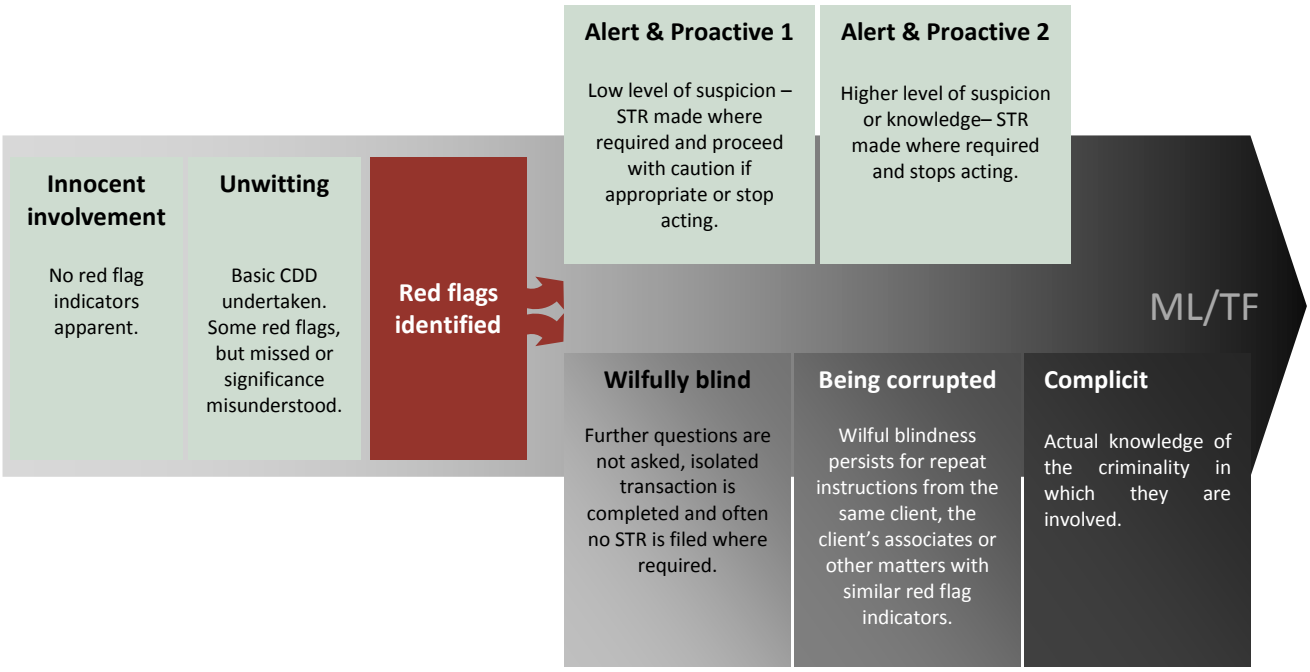
At the outset of this typology exercise, the objective was to identify examples of complicit involvement by legal professionals on the one hand and unknowing involvement on the other. A more detailed review of the case studies has indicated that such a stark distinction is not really appropriate.

The involvement of a legal professional in money laundering may more appropriately be described as a continuum:

[36] It should be noted that legal professionals may cease to act but not make an STR when legal professional privilege or professional secrecy applies.

- Depending on the extent to which the proceeds of crime have already been laundered previously, there may realistically be no red flag indicators apparent to the legal professional during the transaction or the client is able to provide convincing explanations to any generic red flag indicators identified.
- In other cases, red flag indicators may be present, but due to lack of awareness or proper systems, the legal professional genuinely does not see the red flag indicators or appreciate their significance.
- Where the red flag indicators are present and identified by the legal profession, two separate approaches may be taken.
    - In some cases the legal professional, for a variety of reasons may turn a blind eye to the red flag indicators, become more deeply involved in the criminal activity and may in a minority of cases become a future willing accomplice for one or more criminals. Law enforcement has reported that in some cases they may still receive an STR from such a legal professional after the police investigation has commenced.
    - Alternatively, the legal professional may make a STR (where required) and depending on the level of information they have causing the suspicion and their professional obligations in the given circumstances, either proceed with the transaction with caution, or cease acting for the client.

Figure 1. **Involvement of Legal Professionals in money laundering and terrorist financing (ML/TF)**



APPROACH TO CASE STUDIES IN THIS REPORT

For each method and technique identified, this report considers the attractiveness of the method for criminals and a relevant ethical or professional obligation of the legal professional.

Case studies are identified which demonstrate each technique and where possible, case studies have been sourced from both civil and common law countries and show different types of involvement from the legal professionals.

Under each case study, attention is drawn to the red flag indicators which *may* have been apparent to the legal professional and/or to the SRB or law enforcement investigating the transaction. These red flag indicators are drawn from a comprehensive list contained in Chapter 5.

Red flag indicators should always be considered in the context of the specific case. Individual red flag indicators may not be a basis on their own for having a suspicion of money laundering, but they will be a basis to ask questions of a client.[37] The answers to these questions may remove concerns about the source of funds being used in the transaction. Alternatively, the answers or lack of answers may cause a legal professional to be suspicious that his/her services are being misused, especially where there is more than one red flag indicator present.

A table of all case studies, with key methods and techniques is in Annex 5, as individual cases may demonstrate more than one method.

Additional case studies are contained in Annex 6.

[37] This is consistent with the FATF requirements to identify the client, the beneficial owners, understand the source of funds and the nature and the purpose of the business relationship.

METHOD 1: MISUSE OF CLIENT ACCOUNT

While the use of the client account is part of many legitimate transactions undertaken by legal professionals, it may be attractive to criminals as it can:

- be used as part of the first step in converting the cash proceeds of crime into other less suspicious assets;
- permit access to the financial system when the criminal may be otherwise suspicious or undesirable to a financial institution as a customer;
- serve to help hide ownership of criminally derived funds or other assets; and
- be used as an essential link between different money laundering techniques, such as purchasing real estate, setting up shell companies and transferring the proceeds of crime.[38]

[38] Australia, Canada and the United States – although the Canadian FIU is the AML/CFT supervisor for the Notaries in British Columbia.

TECHNIQUE: TRANSFERRING FUNDS WITHOUT PROVIDING LEGAL SERVICES

The majority of legal professionals are required to meet strict obligations when handling client money, including the requirement that they deal with client money only in connection with the provision of legal services and do not simply act as a bank or deposit-taking institution. Failure to comply with these obligations will generally be grounds for disciplinary action.

However, law enforcement and SRBs are still finding cases where legal professionals are simply transferring funds through their client account without providing an underlying legal service. In some cases this could raise questions as to whether a law firm had appropriate procedures or was supervising staff members or junior lawyers appropriately. In discussion with SRBs during the workshops, it was suggested that if legal services are not provided, there may not be a lawyer-client relationship and privilege or secrecy may not apply.

Case 1: **Use of client account without underlying legal services provided – common law country**

An employee working in a very small law firm in Australia received an email from a web-based account referring to a previous telephone conversation confirming that the law firm would act on the person's behalf.

The 'client' asked the employee to accept a deposit of AUD 260 000 for the purchase of machinery in London. The 'client' requested details of the firm's account, provided the surname of two customers of a bank in London, and confirmed the costs could be deducted from the deposit amount.

The details were provided, the funds arrived and the 'client' asked that the money be transferred as soon as possible to the London bank account (details provided) after costs and transfer fees were deducted. The funds were transferred, but no actual legal work was undertaken in relation to the purchase of the machinery. The transfer of the funds to the law firm was an unauthorised withdrawal from a third party's account.

This specific case was brought to the attention of the Office of the Legal Services Commissioner (OLSC) in Australia, which took the view that the law firm had failed to ensure that the identity and contact details of the individual were adequately established. This was particularly important given the individual was not a previous client of the law firm. The employee – proceeding on the basis of instructions received solely via email and telephone without this further verification of identity – was criticised. The OLSC also found that the law firm failed to take reasonable steps to establish the purpose of the transaction and failed to enquire into the basis for the use of the client account. The law firm was reprimanded for their conduct in this case.

Source: Australia (2012) questionnaire response.

Case 1 **Red flag indicators:**	• The client is actively avoiding personal contact without good reason. • Client is willing to pay fees without the requirement for legal work to be undertaken. • Client asks for unexplained speed.

Case 2: **Deliberate misuse of client account without underlying legal transaction – hybrid civil and common law country**

A Quebec lawyer received approximately USD 3 million in American currency from a Montreal businessman, which he deposited into the bank account of his law practice.

The lawyer then had the bank transfer the funds to accounts in Switzerland, the United States, and Panama.

In Switzerland, another lawyer, who was used as part of the laundering process, transferred on one occasion USD 1 760 000 to an account in Panama on the same day he received it from the Canadian lawyer.

When depositing the funds in Canada, the Quebec lawyer completed the large transaction reports as required by the bank, fraudulently indicating that that the funds came from the sale of real estate.

A police investigation into the Quebec lawyer established that these funds were transferred to a reputed Colombian drug trafficker linked to the Cali Cartel. In their attempts to gather further information about the suspicious transactions, bank officials contacted the lawyer about the funds. The lawyer refused to provide any further information, claiming solicitor-client confidentiality.

The bank subsequently informed the lawyer that it could no longer accept his business.

Source: Schneider, S. (2004)

Case 2 **Red flag indicators:**	• Use of a disproportionate amount of cash • Use of client account with no underlying legal work • Funds sent to one or more countries with high levels of secrecy • Client known to have connections with criminals

Case 3: **Disciplinary action taken for use of client account without underlying transaction – common law country**

The Kentucky Supreme Court ordered Attorney Charley Green Dixon be publicly reprimanded for misconduct relating to Dixon's attorney escrow account. Although the trial commissioner of the state bar disciplinary committee found Dixon not guilty on charges of violating two ethics rules, the court elected to review the case despite the fact that no appeal was filed by the committee.

The court found Dixon in violation of: an ethics rule relating to the safekeeping of client property; for his failure to notify corporations that he received funds in which corporations had an interest; and for distributing those funds to a third party. At the time of the misconduct, Dixon was the elected Knox County Attorney. Dixon represented his family friend, a Knox County judge, on and off for 15 years, and the judge asked him to cash cheques, leaving them on Dixon's desk each time and following up with phone calls.

In total, Dixon deposited 11 cheques payable to one of two construction companies into his attorney escrow account and subsequently wrote cheques in corresponding amounts to the judge's brother or sister-in-law. The court noted: "*An FBI investigation uncovered a money laundering scheme perpetrated by [Judge] Raymond Smith and [his brother] Matt Smith. Raymond Smith used his position as Knox County Judge–Executive to create false bids and invoices for county construction projects. He laundered the money through various accounts, including Dixon's attorney escrow account. Raymond*

and Matt Smith pled guilty to federal charges. Evidence before the trial commissioner included an affidavit from the FBI agent on the case, stating that Dixon was not charged with a crime because prosecution of Dixon required Raymond Smith's assistance, which was unlikely."

Despite the absence of a current attorney-client relationship between Dixon and the judge, the Court found that the relevant ethics rule prohibited an attorney from engaging in any conduct involving dishonesty, fraud, deceit, or misrepresentation, even outside of an attorney-client relationship. The Court ordered Dixon to be publicly reprimanded for his violation of the spirit of the ethics rules, the "global appearance of impropriety by Dixon," and his conduct which was deemed serious enough to "bring the Bar into disrepute." The Court held that even though he was not prosecuted for a money laundering offence, Dixon should have known better than to use his "escrow account for 'banking services' for individuals."

Source: United States (2012) questionnaire response Kentucky Bar Ass'n v. Dixon, 373 S.W.3d 444 (Ky. 2012)

Case 3 **Red flag indicators:**	• Use of client account without an underlying legal transaction. • Requests for payments to third parties without substantiating reason or corresponding transaction.

TECHNIQUE: STRUCTURING PAYMENTS

For countries where there are threshold reporting obligations, criminals may seek the advice and assistance of a legal practitioner to structure the payments to avoid those reporting obligations. Such involvement by a legal practitioner would be complicit. Even where threshold reporting is not required, criminals may still seek to structure payments in such a way as to avoid raising the suspicion of the financial institution.

Some of the case studies below show that advice on structuring may also include putting transactions in the names of third parties and getting involved in other financial transactions.

Under professional requirements, a legal professional would need to establish clearly who their client was, ensure they were acting in that person's best interest and that the person providing instructions had clear authority to do so. The failure to establish those factors would at least suggest a breach of professional obligations which warrant disciplinary action. It may also show that the legal professional knew or suspected that he or she was assisting with inappropriate conduct and so deliberately chose not to ask more questions.

Where the legal professional is involved in providing advice on share purchases and handling the funds to facilitate the purchase or is involved in other sorts financial transactions, consideration would need to be given as to whether the legal professional was acting as a financial advisor and/or investment broker rather than as a legal professional. Depending on the country, such conduct may be outside the scope of the legal professional's role and may require separate licensing. This may also mean that privilege/secrecy would not cover that transaction.

Case 4: **Legal professional deliberately structures transactions to avoid reporting threshold in property case – common law country**

An investigation into an individual revealed that an Australian solicitor acting on his behalf was heavily involved in money laundering through property and other transactions. The solicitor

organised conveyancing for the purchase of residential property and carried out structured transactions in an attempt to avoid detection. The solicitor established trust accounts for the individual under investigation and ensured that structured payments were used to purchase properties and pay off mortgages. Some properties were ostensibly purchased for the individual relatives, though the solicitor had no dealings with them. The solicitor also advised the individual on shares he should buy and received structured payments into his trust account for payment

Source: FATF (2007)

Case 4 **Red flag indicators:**	• Purchase of properties for family members where there is a lack of personal contact without good reason gives raises doubts as to the real nature of the transaction. • Third party funding warranting further consideration. • Significant private funding and the transfers are structured so as to avoid the threshold reporting requirements.

Case 5: **Legal professional convicted following structuring and purported stock purchases – common law country**

Criminal defence attorney Jerry Jarrett was convicted for money laundering and illegally structuring financial transactions to avoid reporting requirements. In one instance, Jarrett laundered USD 67 000 in drug proceeds by depositing money through small transactions into the bank account of a dormant business he controlled. He then prepared a backdated stock purchase agreement representing that the drug dealer had invested USD 15 000 in the company. He then wrote a series of cheques to the client for "return on investment." Jarrett organised a series of similar transactions with another drug dealer to launder USD 25 000 in drug proceeds. Both clients testified at trial that Jarrett knew that the cash was drug proceeds. See 447 F.3d 520 (7th Cir. 2006) (reversing district court's post-verdict dismissal of indictment).

Source: United States (2012) questionnaire response United States v. Jarrett, No. 03-cr-87 (N.D. Ind.)

Case 5 **Red flag indicators:**	• Significant private funding and the transfers are structured so as to avoid the threshold reporting requirements. • Client was known to have convictions for acquisitive crime.[1] • Unusual level of investment in a dormant company.

1. Acquisitive crime is any crime which produces proceeds of crime.

Case 6: **Legal professional files STR after noticing structuring and back to back sales by client – civil law country**

Person A purchases two real estate properties in 2007, for a combined price of EUR 150 000. The same properties are sold again in 2010 for a combined price of EUR 413 600 to Person B. The notary asked to see details of the payments between the vendor and the purchaser, before notarising the sale. They were provided with evidence that the funds had been deposited over the previous two months with all of the deposits under the reporting threshold amount of EUR 100 000. There was public information that Person B was associated with frauds in the automobile sector. The notary filed a STR.

Source: Spain (2012) questionnaire response

Case 6 **Red flag indicators:**	• The transaction was unusual in that the price increase was significant by comparison to the normal market changes over the same period. • One of the parties is known to be currently under investigation for acquisitive crime or to have known connections with criminals.

In this case, direct payment between the parties was not a red flag indicator, as this is quite common in Spain.

TECHNIQUE: ABORTED TRANSACTIONS

Some criminals will be aware of the restrictions on the ability of legal professionals to handle client funds without an underlying transaction. Therefore, they will appear to be conducting a legitimate transaction which, for one reason or another, collapses before completion. The client then asks for the money to be returned or paid to multiple recipients, sometimes according to the direction of a third party. [39]

During an economic downturn, the aborting of transactions is not an infrequent occurrence and legal practitioners may find it more difficult to distinguish between legitimate situations and those which were always intended to launder the proceeds of crime.

Third party funding is not unusual in aborted transactions. Under professional obligations, a legal professional must act in the best interests of the client. This means that they need to know who the client is and to understand if the funds they were using were being given to them as a gift or a loan, so that the arrangement and any subsequent ownership interests were properly documented. The failure to do so may suggest a breach of professional requirements or possibly complicity in the scheme.

Case 7: **Legal professional disciplined for sending funds to a third party after an aborted transaction – common law country**

In 2010 a solicitor was fined GBP 3 000 for their involvement in a purported company acquisition which was in fact an investment fraud. In 2005, the solicitor had accepted unsolicited funds directly from investors, but then the purchase of the company did not occur. A third party to the transaction asked for the funds to be paid into an account in Eastern Europe. The solicitor made an STR and received permission to send the funds back to the original source. For reasons which are unclear, the funds were instead transferred to another account controlled by a third party, allowing the proceeds of the fraud to be laundered. The Solicitors Disciplinary Tribunal found that the solicitor was naive rather than reckless.

Source: United Kingdom (2012) questionnaire response

Case 7 **Red flag indicators:**	• The person actually directing the operation is not one of the formal parties to the transaction or their representative • Transaction is aborted after receipt of funds and there is a request to send the funds on to a third party.

[39] This technique was specifically noted in the Australian questionnaire response to this project.

Case 8: **Legal professional removed from practice after ignoring red flag indicators on an aborted transaction – common law country**

In 2011 a solicitor was struck off the roll for acting in a number of property purchases which had all the hallmarks of money laundering. In 2008 the solicitor received instructions from an individual to purchase property on behalf of other clients, who provided funds for the purchase prior to the solicitor indicating the need for the funds to be deposited. The solicitor did not meet the clients, undertake due diligence checks or obtain instructions in writing. The funds came into the client account, the transaction was cancelled and there was a request to provide the funds to a third party – all on the same day.

Source: United Kingdom (2012) questionnaire response

Case 8 **Red flag indicators:**	• Transaction is aborted after receipt of funds and there is a request to send the funds to a third party • The client is acting through an intermediary and avoiding personal contact without good reason • Unusual speed requested.

METHOD 2: PROPERTY PURCHASES

Criminals, like those with legitimate incomes, require a place to live and premises from which to conduct their business activities. Irrespective of economic conditions, real estate investment often remains attractive for criminals and non-criminals alike. Consequently, the purchase of real estate is a common outlet for criminal proceeds. Real estate is generally an appreciating asset and the subsequent sale of the asset can provide a legitimate reason for the appearance of the funds

In many countries a legal professional is either required by law to undertake the transfer of property or their involvement is a matter of custom and practice.

However the specific role of the legal professional in real estate transactions varies significantly from country to country, or even within countries. In some countries, the legal professional will customarily hold and transfer the relevant funds for the purchase. In other countries this will be done by other parties, such as a title insurance agent.

Even if the legal professional is not handling the money, they will be aware of the financial details and in many cases will be in a position to ask further questions about the purchase or sale.

Therefore, real estate transactions are a key area of potential ML/TF vulnerability for legal professionals.

TECHNIQUE: INVESTMENT OF PROCEEDS OF CRIME IN PROPERTY

From the cases obtained, it is clear that some criminals will seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership.

Despite many countries introducing reporting requirements on cash payments, and many professional bodies restricting the amount of cash which legal professionals may receive, some criminals will still seek to use the purchase of real property as a means of placing cash obtained from criminal activity. Increasingly, this is seen as part of the layering process, where the funds have been accumulated in one or more bank accounts and the property purchase is wholly or predominantly funded through private means rather than a mortgage or loan.

There has been extensive publicity about the money laundering risks posed by large amounts of cash or unexplained levels of private funding in relation to property purchases. Where legal professionals are involved and an STR is not made, it is more likely that the legal professional is either complicit in the money laundering, or is being wilfully blind by failing to ask more questions when warning signs are present.

Case 9: **Legal professional files STR after noticing red flag indicators on property transaction – civil law country**

The CTIF-CFI (the Belgium FIU) received a notification from a notary on a person from Eastern Europe, who resided in Belgium and had bought a property there.

The purchase happened by depositing the total purchase price in cash before the document authenticating the purchase was signed. The person claimed that he could not open a bank account

and so had to pay cash for the property.

After the notification of the notary, the FIU learned that the person did have an account at a Belgian bank and that the size of the transaction was not in proportion with his financial situation as he was receiving state benefits. Police sources revealed the person was known for illicit trafficking in goods and merchandise

Source: Cellule de traitement des informations Financières, (2005)

Case 9 **Red flag indicators:**	• Transaction involves a disproportionate amount of private funding/cash, which is inconsistent with the socio-economic profile of the individual • Transaction is unusual because of the manner of execution – in this case it was the depositing of the total purchase price so early in the transaction which was different to normal custom.

Case 10: **Legal professional acts as prosecution witness after failing to notice warning signs relating to a property purchase – common law country**

In 2009 a client approached a United Kingdom solicitor to purchase land for the client's family.

The client deposited GBP 35 000 with the solicitor which they said was from family members as the family were pooling the money together to buy land on which all the family could live.

Further cash amounts were deposited with the solicitor from numerous third parties to fund the rest of the purchase.

The solicitor only spoke with the client, who said they were the only literate member of the family and so was conducting business on the family's behalf.

While the solicitor did not submit an STR, the solicitor was not prosecuted but acted as a witness for the police.

Source: United Kingdom (2012) questionnaire response

Case 10 **Red flag indicators:**	• Significant levels of private funding/cash which is inconsistent with the socio-economic profile of the individual • Funding from third parties requiring further consideration • Request to act for multiple parties without meeting them

Case 11: **Legal professional convicted of money laundering through property purchase involving cash and significant funding from multiple parties – common law country**

Shadab Kahn, a solicitor, assisted in the purchase of a number of properties for a client using the proceeds of crime. The client owned a luxury car business, but was also involved in drug dealing.

The funds for the property purchases were generally provided in cash from the client or from third parties. Almost GBP 600 000 was provided by the client, which was a significant level of private funding despite the client's apparent legitimate business activities.

Mr Khan was convicted in 2009 of money laundering and failing to make an STR, jailed for four years, and struck off the roll by the Solicitors Disciplinary Tribunal in 2011. The court criticised Mr Khan for accepting explanations about the source of funds at face value and not looking behind the claimed cultural customs about the funding arrangements.

Source: United Kingdom (2012) questionnaire response

Case 11 **Red flag indicators:**	• Significant amount of private funding/cash from an individual who was running a cash intensive business. • Involvement of third parties funding without apparent connection or legitimate explanation.

TECHNIQUE: TRANSFERRING VALUE – BACK TO BACK OR ABC SALES

The frequent movement of investments in immovable assets such as property is not common. Quick successive sales of property, either with or without a mortgage, enable criminals to inflate the value of the property, thereby justifying the injection of further criminal funds into the purchase chain and enabling value to be either transferred to other parts of an organised crime group or reinvested within the group. While the frequent changes in ownership may also make it more difficult for law enforcement to follow the funds and link the assets back to the predicate offence.

Case 12: **Legal professional facilitates multiple back to back sales of properties within a group of mortgage fraudsters – civil law country**

An individual in his early 20's who worked as a gardener approached a notary to purchase several real estate properties. The client advised that he was funding the purchases from previous sales of other properties and provided a bank cheque to pay the purchase price.

The client then instructed a different set of notaries to re-sell the properties at a higher price very quickly after the first purchase. The properties were sold to other people that the client knew who were also in their early 20's and had similar low paying jobs.

The client had in fact obtained mortgages using false documents for these properties, generating the proceeds of crime. The multiple sales helped to launder those funds.

Source: France (2012) questionnaire response

Case 12 **Red flag indicators:**	• Disproportionate amount of private funding which is inconsistent with the socio-economic profile of the individual • Transactions are unusual because they are inconsistent with the age and profile of the parties • Multiple appearances of the same parties in transactions over a short period of time. • Back to back (or ABC) property transaction, with rapidly increasing value • Client changes legal advisor a number of times in a short space of time without legitimate reason. • Client provides false documentation.

TECHNIQUE: TRANSFERRING VALUE – SALES WITHIN AN ORGANISED CRIME GROUP

Case 13: **Legal professional facilitates multiple back to back property sales within an organised crime group – civil law country**

The attention of Tracfin was drawn to atypical financial flows relating to real estate purchases undertaken in the regions of Midi-Pyrénées, Languedoc-Roussillon and Provence-Alpes-Côte d'Azur.

The analysis brought to light a possible network of organised criminality involving people who were either current or former members of the Foreign Legion. The individuals were mostly of the same foreign nationality and involved a real estate civil society (property investment scheme).

Between April 2009 and March 2011 the office of a notary public registered 28 deeds of real estate transfer for this group. All the sales, bar one, were officialised by the same notary in the office.

Twelve individuals and six different real estate civil societies (non-trading companies) were listed as the purchaser, while seven individuals and five societies were sellers of the properties.

Of these 28 deeds, 16 were paid in full for EUR 1.925 million; six were financed through loans of EUR 841 149 in total, and the source of financing was not able to be determined for five properties which had a value of EUR 308 200.

Nine of the transactions were paid in full by individuals in the amount of EUR 1.152 million, which was a significant amount given the profession of the clients.

The properties were also resold within relatively short timeframes. For example, one of the properties in Castres was resold every year since 2009 with occasionally significant increases in the sale price. All these sales were registered by the same notary. The real estate civil society thereby multiplied by six the purchase price of this property.

In some instances the sellers claimed the property had increased in value because they had done work on those properties (they hadn't).

The notary registered two further transactions in 2011 which were paid for in cash and were at a significant distance from the notary's office.

Source: France (2012) questionnaire response

Case 13 **Red flag indicators:**	• Disproportionate amount of private funding/cash which is inconsistent with the socio-economic profile of the individual. • Significant increases in value / sale price sometimes realised within a relatively short timescale. • Parties to the transaction are connected without an apparent business reason. • Multiple appearances of the same parties in transactions over a short period of time.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE WITH A FALSE NAME

Criminals who seek to retain the benefit of the proceeds of their crime may seek to obscure the ownership of real property by using false identities. Legal professionals may be complicit in these transactions, but are more likely to be involved unwittingly, especially if the criminal has forged identity documentation of a high quality or if the legal professional is not required in their country to undertake CDD.

The use of false or counterfeited documents should always be a red flag to the legitimacy of the individual and the action they wish to take. While legal professionals are not expected to be forgery experts, with the increased ability of criminals to access such materials through the internet, having some familiarity with identity documents at least within their country, may help them avoid being taken in by obvious forgeries.

Case 14: **Legal Professional facilitates property purchase in a false name – common law country**

Law enforcement investigated a matter involving a drug offender actively growing a large crop of cannabis on a property. When the person of interest (POI) was arrested for this offence, it was established that the person had purchased the block of land under a false name.

Under provisions of Chapter 3 of the Criminal Proceeds Confiscation Act 2002, if the POI had effective control of the land, and used that land to produce dangerous drugs, then the property was liable for forfeiture. Initial inquiries revealed the property was registered as being owned by a different person. Further enquiries made with another government department revealed the person had the same first names as the POI, but a different surname. The date of birth recorded at this department was very similar to the POI with the year and month identical, but the day slightly different.

It was alleged the POI had purchased the property under a false name, as no identification was required by the real estate agent to sign the contract. It is further suspected the POI took the contract to a solicitor for conveyance and had the solicitor sign the transfer documents on the POI's behalf. The sale was executed in 2002, but the final payment (made via a solicitor) was not made until 2004. This payment method was written into the contract.

Source: Australia (2012) questionnaire response

Case 14 **Red flag indicators:**	• Client provides false or counterfeited documentation • There are attempts to disguise the real owner or parties to the transaction • Transaction is unusual because of the manner of execution in terms of the delay in payment well after the contact was executed.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH INTERMEDIARIES

The creation of convincing false identities involves time and expenditure by criminals and there is a risk that the fake identity will be discovered. Another option for obscuring ownership while retaining control is placing the property in the names of family, friends or business associates.

While the purchase of real property for family members may be quite legitimate and a regular occurrence in many cultures, such transactions will usually require detailed documentation to ensure that ownership, inheritance and taxation matters are properly dealt with.

Legal professionals also need to carefully consider who they are acting for, especially where there are a number of parties involved in a purchase. They will need to ensure that they are not in a conflict situation and that they are able to act in the best interests of their client. Failure to ask such questions may be indicative that the legal professional is either complicit or wilfully blind to the money laundering risks.

Case 15: **Family members used as a front for purchasing property – common law country**

A Canadian career criminal, with a record including drug trafficking, fraud, auto theft, and telecommunications theft, deposited cash into a bank account in his parents' name.

The accused purchased a home with the assistance of a lawyer, the title of which was registered to his parents. He financed the home through a mortgage, also registered to his parents. The CAD 320 000 mortgage was paid off in less than six months.

Source: Schneider (2004)

Case 15 **Red flag indicators:**	• Disproportionate amount of private funding/cash which is inconsistent with the known legitimate income of the individual • Client is known to have convictions for acquisitive crime • There are attempts to disguise the real owner or parties to the transaction. • Mortgages repaid significantly prior to the initial agreed maturity date with no logical explanation.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH A COMPANY OR TRUST

The purchasing of real estate through a company or a trust has been identified previously[40] as a technique used to both obscure ownership and frustrate law enforcement activity to pursue the proceeds of crime.

Case 16: **PEP involved in financial wrongdoing purchases expensive properties in foreign country through a corporate vehicle – civil law country**

A foreign client approached a legal professional to buy two properties, one in Alpes-Maritimes (South of France), and the other in Paris, for EUR 11 million.

The purchase price was completely funded by the purchaser (there was no mortgage) and the funds were sent through a bank in an off-shore jurisdiction.

As the contract was about to be signed, there was a change in instructions, and a property investment company was replaced as the purchaser. The two minor children of the client were the shareholders of the company.

The foreign client held an important political function in his country and there was publicly available information about his involvement in financial wrongdoing.

Source: France (2012) questionnaire response

Case 16 **Red flag indicators:**	• The legal professional was located at a distance from the client / transaction, and there was no legitimate or economic reason for using this legal professional over one who was located closer. [1] • Disproportionate amount of private funding which is inconsistent with the socio-economic profile of the individual • Client is using bank accounts from a high risk country

40 FATF (2007) and Schneider (2004).

	• Unexplained changes in instructions, especially last minute • The transaction is unusual in the manner of its execution – in France it is quite unusual for residential property to be purchased via a corporate vehicle or for minors to be shareholders. It should be noted that this approach would be considered normal and prudent estate planning in other countries. • Use of a complicated structure without legitimate reason • Shareholders of the executing party are under legal age • Client holds a public position and is engaged in unusual private business given the characteristics involved.

1. In some jurisdictions it is becoming more frequent for legal services relating to property purchases to be sourced online which may mean that the legal professional is located at a distance from the client or the transaction. However in many civil law countries, where notaries are required to be involved with the purchase, notaries are appointed to a specific location. While non-face to face transactions are no longer listed as automatically requiring enhanced due diligence under the FATF Recommendations, the desire to avoid personal contact without good reason is still an indicator of money laundering or terrorist financing risk

Case 17: **Legal professionals assist with opening bank accounts and investing in property via complex corporate structures – civil law country**

A foreigner residing in Belgium was introduced to a bank by a law firm with a view to him opening an account. This account was credited with large sums by foreign transfers ordered by an unknown counterpart. A civil-law notary wrote bank order cheques from the account, which was then invested in real estate projects in Belgium. In one of these projects the person under suspicion was assisted by other foreign investors in setting up a particularly complex scheme.

The FIU learned from questioning the civil law notary, that he had been engaged by four foreign companies to help set up two holding companies. These two companies had in their turn set up two other Belgian real estate companies. The latter two had then invested in real estate.

The people representing these companies – a lawyer and diamond merchant – acted as intermediaries for the person under suspicion. It turned out the lawyer who had introduced this person to the bank was also involved in other schemes of a similar nature. The address of the registered office of the Belgian companies was also the address of his lawyer's office.

This information showed the important role played by the lawyer in setting up a financial and corporate structure designed to enable funds from unknown foreign principals to be invested in real estate projects in Belgium. On the basis of all these elements the FIU decided to report the file for laundering of the proceeds of organised crime.

Source: Belgium (2012) questionnaire response

Case 17 **Red flag indicators:**	• Creation of complicated ownership structures where there is no legitimate or economic reason. • Client is using an agent or intermediary without good reason. • Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • The source of funds is unusual as there is third party funding with no apparent connection or legitimate explanation and the funds are received from a foreign country where there is no apparent connection between the country and the client.

Case 18: **Legal professional files STR when companies are used to purchase properties to facilitate laundering of drug proceeds and/or terrorist financing – civil law country**

A Spanish married couple of Moroccan origins, who own three properties, incorporate a limited company. They own 100% of the shares between them, the value of which is EUR 12 000 euro.

Within the first five months, the company has undertaken investments of over EUR 260 000, without apparent recourse to external financing. This includes purchasing five properties for over EUR 193 000 in cash. One of the property purchases is from an Islamic community in the south of Spain, the vice-president of which was arrested in 2009 within the context of a Civil Guard anti-drugs trafficking operation.

The couple are found to be associated with other companies which do not file accounts as required under law or receive official gazette notifications. The notary involved in some of the property purchases makes an STR.

According to subsequent information obtained by the Spanish Executive Service of the Commission for Monitoring Exchange Control Offences (SEPBLAC), the transactions could be connected with people possibly related to drug trafficking or terrorist financing.

Source: Spain (2012) questionnaire response

Case 18 **Red flag indicators:**	• The size of the client company was inconsistent with the volume or value of the investments made by the company • The professional profiles of a company's shareholders make it unlikely that the company possessed a lawful source of funds for the scope of investments made • The sum paid out in cash for the properties acquired by the company seems unusual and the company had no corresponding business or operations to justify such a cash outlay • Morocco is geographically located on a route used to introduce drugs into Europe, and this, in connection with the considerable sums of cash being moved from the country to Spain, suggests that the territory should receive particular attention. • One of the persons associated with the operation had been arrested within the context of an anti-drugs trafficking operation.

TECHNIQUE: MORTGAGE FRAUD WITH ANTECEDENT LAUNDERING

While this is a typology on money laundering and terrorist financing – not a report on the involvement of legal professionals in predicate offences – it is relevant to highlight a few cases involving mortgage fraud.

Many of the red flag indicators which would demonstrate money laundering are also present in mortgage frauds, and depending on the specific elements of the money laundering offence, possession of the mortgage funds in the legal professional's client account and subsequent transfer will amount to money laundering.

Case 19: **Legal professional disciplined for failing to notice warning signs of mortgage fraud and handling the proceeds of crime – common law country**

In 2008 a law firm employee was approached by three individuals who were accompanied by a friend to seek a quote to purchase three separate properties. They returned later that day with passports and utility bills and instructed the law firm to act for them in the purchases.

The clients asked for the purchases to be processed quickly and did not want the normal searches undertaken. They did not provide any money to the solicitors for expenses (such funds would normally be provided) but said the seller's solicitors would be covering all fees and expenses. The clients said they had paid the deposit directly to the seller. The mortgages were paid to the law firm, which retained their fees and then sent the funds to a bank account which the law firm employee thought belonged to solicitors acting for the sellers. No due diligence was undertaken.

In fact the actual owners of the property were not selling the properties and had no knowledge of the transaction or the mortgages taken out over their properties. The mortgage funds were paid away to the fraudsters, not to another solicitors firm.

In 2010, the supervising solicitor was fined GBP 10 000 for not properly supervising the employee who allowed the fraud to take place and the proceeds of the funds to be laundered. The solicitor's advanced age was taken into account as a mitigating factor in deciding the penalty.

Source: United Kingdom (2012) questionnaire response

Case 19 **Red flag indicators:**	• Transaction was unusual in terms of all three purchasers attending together with an intermediary to undertake separate transactions; failure to provide any funds for expense in accordance with normal processes; and part of the funds being sent directly between the parties. • Client showed an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory client identification. • Clients asked for short-cuts and unexplained speed in completing a transaction.

Case 20: **Legal professional removed from practice after facilitating multiple mortgage frauds for a number of property developers – common law country**

In 2006 a solicitor was approached by three developers wanting him to act in a number of property transactions. The developers were selling the properties to various companies and investment networks, who were then quickly selling the properties on at significantly inflated prices to other individuals. The solicitor was acting for these individuals, and was introduced to the clients by the other parties to the transaction with the 'deal' already completed.

In 2011 the solicitor was struck off the roll by the Solicitors Disciplinary Tribunal because they had failed to provide full information to the lender (enabling mortgage fraud), had not checked the source of funds for the original transactions or deposits (enabling money laundering) and had not taken notes of their instructions at the time of the transactions, fabricating them during the investigation.

Source: United Kingdom (2012) questionnaire response

Case 20 **Red flag indicators:**	• Back to back (or ABC) property transaction with rapidly increasing purchase price • Transaction is unusual in that there is limited legal work to be undertaken by the legal professional • Unnecessary complexity in the structures and parties involved in the transaction.

METHOD 3: CREATION OF COMPANIES AND TRUSTS

Criminals will often seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and trusts are seen by criminals as potentially useful vehicles to achieve this outcome.

TECHNIQUE: CREATION OF TRUSTS TO OBSCURE OWNERSHIP AND RETAIN CONTROL

Disguising the real owners and parties to the transaction is a necessary requirement for money laundering to be successful and therefore, although there may be legitimate reasons for obscuring ownership it should be considered as a red flag.

Case 21: **Trust established to receive proceeds of tax crime and invest in criminal property**

Two trusts were established in an offshore centre by a law firm. The law firm requested the trustee to accept two payment orders in favour of a bank in order to buy real estate. It appeared that the trust had been used to conceal the identity of the beneficial owners.

Information obtained by the Belgian FIU revealed that the beneficiaries of the trusts were individuals A and B, who were managers of two companies, established in Belgium that were the subject of a judicial investigation regarding serious tax fraud. Part of the funds in these trusts could have originated from criminal activity of the companies.

Source: FATF (2010)

Case 21 **Red flag indicators:**	• Use of an intermediary without good reason. • Attempts to disguise the real owner or parties to the transaction. • Involvement of structures in multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • Client is known to be currently under investigation for acquisitive crimes.

Case 22: **Trust established to enable a criminal to act as a trustee and retain control of property obtained with criminal proceeds – common law country**

A criminal involved in smuggling into the United Kingdom set up a Trust in order to launder the proceeds of his crime, with the assistance of a collusive Independent Financial Adviser (IFA) and a Solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The Trust was discretionary and therefore power over the management of the fund was vested in the Trustees, namely the criminal, his wife and the IFA.

The criminal purchased a garage, which he transferred directly to his daughter (who also happened to be a beneficiary of the Trust). She in turn leased the garage to a company. The garage was eventually sold to this company, with the purchase funded by a loan provided by the Trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the Trust, but in practice to the criminal.

Thus the criminal who had originally owned the garage probably maintained control despite his

daughter's ownership. Through controlling the Trust he was able to funnel funds back to himself through loaning funds from the Trust and receive payments on that loan.

Source: FATF (2010)

Case 22 **Red flag indicators:**	• Creation of a complicated ownership structure when there is no legitimate or economic reason. • The ties between the parties of a family nature generate doubt as to the real nature or reason for the transaction. • Client is known to be currently under investigation for acquisitive crimes.

TECHNIQUE: CREATION OF SHELL COMPANIES TO PLACE OR LAYER

In some countries, a legal professional (usually a notary) must be involved in the creation of a company, so there is an increased risk of unintentional involvement in this laundering method. However, in a number of countries, members of the public are able to register a company themselves directly with the company register. In those countries, if a client simply wants a legal professional to undertake the mechanical aspects of setting up the company, without seeking legal advice on the appropriateness of the company structure and related matters, it may be an indication that the client is seeking to add respectability to the creation of a shell company.

A shell company is a business or corporate entity that does not have any business activities or recognisable assets itself. Shell companies may be used of legitimate purposes such as serving as a transaction vehicle (*e.g.*, an acquiring company sets up a shell company subsidiary that is then merged with a target company, thus making the target company the subsidiary of the acquiring company) or protecting the corporate name from being used by a third party because the incorporation of the shell company under that name blocks any other company from being incorporated with the same name. But criminals often seek to set up shell companies to help obscure beneficial ownership.

Shell companies should be distinguished from shelf companies that are often set up by legal professionals for the purpose of facilitating legitimate transactions. Such companies will be used when it becomes apparent during a transaction that there is a need for a corporate vehicle to be used and there is a legitimate need for speed in the transaction. They will usually be created with the legal professional or their employees as the directors and/or shareholders and are held "on the shelf" until they are needed in the course of a transaction. The legal firm will only have a few of these companies at any one time; in many cases they will only be in existence for a short amount of time and they are sold to the clients in full, with the legal professionals having no further involvement in the management of the company after it is taken down off the shelf. Criminals may seek to misuse shelf companies by seeking access to companies which have been 'sitting on the shelf' for a long time in an attempt to create the impression that the company is reputable and trading well because it has been in existence for many years.

In terms of professional obligations, if a client fails to provide adequate information about the purpose for which the company was set up, this may give rise to concerns as to whether the legal professional would be able to adequately provide advice in the best interests of the client. The

failure to ask such questions may be an indicator that the legal professional is complicit in the scheme.

Case 23: **Legal professional approached over internet to set up multiple companies without information on identity, source of funds or purpose – hybrid common law / civil law country**

A legal professional was approached over the internet to set up companies with limited or no details about the future uses of the company.

Over three years they were asked to set up at least 1 000 such companies in this way.

The people they were asked to list as directors included individuals known to be involved with high level organised crime in that country.

They never met the clients and did not undertake any due diligence.

The companies were used to facilitate money laundering from loan sharking.

Source: Japan (2012) questionnaire response

Case 23 **Red flag indicators:**	• Client is actively avoiding personal contact without good reason. • Transactions are unusual in terms of volume. • Client is overly secretive about the purpose of the transaction. • Parties involved in the transaction have known connections with criminals.

Case 24: **Legal professional sets up multiple international company structures for existing clients – civil law country**

A legal professional in Spain was asked to set up a series of companies for clients for the purpose of purchasing real estate.

Some companies were incorporated in Spain but they were owned by companies which the legal professional also incorporated in an American State.

The legal professional and others in the law firm would constitute the board of directors of the companies incorporated in America. They would later sell these companies to their clients.

The legal professional set up over 300 such companies for clients of the law firm, and continued to administer those companies for the clients.

Many of the clients were known to be involved in international criminal organisations.

Source: FATF (2010)

Case 24 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Involvement of high risk countries. • Client is known to have convictions for acquisitive crime, to be currently under investigation for acquisitive crime or have known connections with criminals.

TECHNIQUE: USE OF BEARER SHARES TO OBSCURE OWNERSHIP

Bearer shares are an equity security that is wholly-owned by whoever holds the physical stock certificate. The issuing firm neither registers the owner of the stock, nor does it track transfers of ownership.

Quite a number of countries have banned the use of bearer shares by legal entities, while in other countries; these types of securities are quite common, even for companies acting legally.

Case 25: **Creation of company with bearer shares to obscure ownership in a property transaction – civil law country**

A Spanish lawyer created several companies for a client on the same day (with ownership through bearer shares, thus hiding the identity of the true owners). One of these companies acquired a property that was an area of undeveloped land. A few weeks later, the area was re-classified by the local authorities where it was located so it could be urbanised.

The lawyer came to the Property Registry and in successive operations, transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions. With each succeeding transfer of the property the price of the land was increased.

The participants in the individual transfers were shell companies controlled by the lawyer. Finally the mortgage was cancelled with a cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as the acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it can be inferred that this company was a front set up merely for the purpose of carrying out the property transactions.

After investigation it was learned that the purchaser and seller were the same person: the leader of a criminal organisation. Money used in the transaction was of illegal origin (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Source: FATF (2007)

Case 25 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime, or have known connections with criminals. • Back to back (or ABC) property transactions, with rapidly increasing value / purchase price. • Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

Case 26: **Creation of complex company structures in multiple countries to launder proceeds of drug trafficking**

A legal professional in Country A was approached to assist in setting up companies for a client.

The legal professional approached a management company in Country B, who in turn approached a trust and company service provider in Country C to incorporate a number of bearer share companies.

Only the details of the trust and company service provider were included in the incorporation

documents as nominee directors and administrators.

The articles of incorporation and the bearer shares were forwarded to the lawyer, via the management company, who provided them to the client.

The client was involved in drug importation. Approximately USD 1.73 million was restrained in combined assets from residential property and bank accounts in relation to those companies

Source: FATF 2010

Case 26 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • Disproportionate private funding which is inconsistent with the socio-economic profile of the individual.

METHOD 4: MANAGEMENT OF COMPANIES AND TRUSTS

While the creation of companies and trusts is a key area of vulnerability for legal professionals, criminals will also often seek to have legal professionals involved in the management of those companies and trusts in order to provide greater respectability and legitimacy to the entity and its activities.

In some countries professional rules preclude a legal professional from acting as a trustee or as a company director. In countries where this is permitted, there are differing rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will affect whether any funds relating to activities by the company or trust can go through the client account.

TECHNIQUE: ACTING AS TRUSTEE – RECEIVING THE PROCEEDS OF CRIME

Where a settlor creates a trust using the proceeds of crime or deposits further assets into the trust which are the proceeds of crime, a legal professional acting as trustee will be facilitating the laundering of those proceeds by managing the trust. Under common law there is an obligation on the trustee to acquaint themselves with all trust property and the FATF standards require that those providing trust services in a business capacity undertake CDD, including ascertaining the source of funds. Such enquiries would assist in minimising the risks of legal professionals who are acting as trustees inadvertently becoming involved in money laundering.

Case 27: **Legal professional uses client account to transfer proceeds of crime into a trust he managed – common law country**

Defendant Paul Monea was convicted of various money laundering counts in connection with his attempt to accept payment for the sale of a large diamond by requiring the purchasers to wire funds, which he knew to be drug proceeds, to his attorney's IOLTA (attorney trust) account and onward to his family trust account, which was managed by the same attorney. It does not appear as if the attorney was prosecuted. *See* 376 F. App'x 531 (6th Cir. 2010), *cert. denied* 131 S. Ct. 356 (2010).

Monea's Family Trust was in possession of a 43-carat flawless yellow diamond that Monea was looking to sell for a profit. Monea was introduced to an undercover federal agent who used the name "Rizzo," and Rizzo volunteered that he knew someone (a drug dealer) who would be interested in purchasing the diamond. Monea explained that he did not want to conduct the sale in cash because of apprehension that he was being "watched" by the government. The court noted that the pair discussed at a meeting: "the best way to conduct the transaction, the problem of receiving cash, Monea's conversations with his attorney about his responsibilities concerning knowledge of the money's source, and whether Monea could use the [Attorney Trust Account] of the attorney representing the Monea Family Trust." On meeting with another undercover agent posing as the buyer's representative, Monea told the man (who he believed to be the associate of the drug dealer-purchaser) that USD19.5 million should be wired into his Attorney's Trust Account. Funds were wired in the amount of USD 100 000 in three instalments when the deal was supposed to close at the attorney's office with a gemmologist present to certify the authenticity of the stone. Rizzo pretended to make a call to have the remainder of the purchase price wired into the Attorney Trust

Account, but instead, he called other law enforcement agents and the scheme was disrupted.

The court held that Monea's "intent to conceal" the nature of the drug dealer's proceeds used to buy the diamond was shown by his desire to use the Attorney Trust Account to funnel the funds to the Monea Family Trust account, which the attorney also managed. Routing the transaction through the Attorney Trust Account was an extra and unnecessary step, not integral to the sale, which should have raised red flags with the attorney.

Furthermore, according to recorded conversations, Monea discussed with the attorney that he did not want the wire transfers "looked at." The attorney allegedly stated that he represented his Attorney Trust Account and Monea's trust, so there was no problem as long as the diamond was sold for fair market value. Monea paraphrased the attorney speaking to him, in a recorded conversation: "you [Monea] don't really have the responsibility or obligation to interview people to find out how they got the money [for the diamond] . . . it's not your responsibility." Monea later stated: "I'll tell you why I want [the money] going into my [Attorney's Trust Account]. Because my attorney represents the [Monea Family Trust]. And my attorney can legitimately represent the [Monea Family Trust] . . . and we're conducting the sale on behalf of the trust. And it keeps me clean." Monea used his attorney and his trust account as intermediaries, and then further used his trust account that was managed by the attorney to conceal drug proceeds and insulate himself by virtue of the attorney-client relationship. *See* 376 F. App'x 531 (6th Cir. 2010), *cert. denied* 131 S. Ct. 356 (2010).

Source: United States (2012) questionnaire response United States v. Monea, No. 07-cr-30 (N.D. Ohio)

Case 27 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • The retainer involves using the client account were this is not required for the provision of legal services

TECHNIQUE: MANAGEMENT OF A COMPANY OR TRUST –APPEARANCE OF LEGITIMACY AND PROVISION OF LEGAL SERVICES

Case 28: **Legal practitioner incorporates companies and acts as front man to launder proceeds of embezzlement**

A money laundering operation involved a massive purchase of derivatives by companies which paid hefty fees to fake intermediaries, then surreptitiously transferred to the bank directors either in cash or on foreign banks accounts.

In this scheme the notary participated by incorporating some of the fake intermediaries, whilst the lawyer appeared as the beneficial owner of such companies and actively participated in a complex scheme of bank transactions put in place to embezzle the funds illicitly obtained. Several bank accounts at different institutions were used, with the involvement of figureheads and shell companies, so as to transfer funds from one account to another by mainly making use of cheques and cash.

Source: Italy (2012) questionnaire response

Case 28 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Creation of complicated ownership structures when there is no legitimate or economic reason.

Case 29: **Legal professional manages trusts used to perpetrate an advanced fraud scheme and launder the proceeds – common law country**

An entity, Euro-American Money Fund Trust, was used to perpetrate an advance-fee scheme. John Voigt created a genealogy for the Trust, claiming it was a long-standing European trust associated with the Catholic Church. He then solicited investments for phony loans. Ralph Anderskow was a partner at a large Chicago firm who managed the Trust and whose credentials were publicised as legitimising the Trust. Although he may not have known that the Trust was fraudulent at first, it was apparent shortly thereafter. Anderskow provided guarantees to borrowers, maintained a client escrow account into which advance fees were deposited, and distributed the deposited fees to Voigt and his associates, which violated the terms of the contracts entered into with the loan applicants and investors. *See* 88 F.3d 245 (3d Cir. 1996) (affirming conviction and 78-month sentence).

Source: United States (2012) questionnaire response United States v. Anderskow, No. 3:93-cr-300 (D.N.J.)

Case 29 **Red flag indicators:**	• Client is using false or fraudulent identity documents for the business entity • Requests to make payments to third parties contrary to contractual obligations

TECHNIQUE: HOLDING SHARES AS AN UNDISCLOSED NOMINEE

Individuals may sometimes have legal professionals or others hold their shares as a nominee, where there is legitimate privacy, safety or commercial concerns. Criminals may also use nominee shareholders to further obscure their ownership of assets. In some countries legal professionals are not permitted to hold shares in entities for whom they provide advice, while in other countries legal

professionals regularly act as nominees. Where a legal professional is asked to act as a nominee, they should understand the reason for this request.

Case 30: **Legal professionals acting as undisclosed nominees in companies suspected as vehicles for organised crime – civil law country**

A lawyer was reported by an Italian banking institution in connection with some banking transactions performed on behalf of companies operating in the wind power sector in which he held a stake. The reporting entities suspected the stake was in fact held on behalf of some clients of his rather than for himself.

The report concerned a company owned by the lawyer who sold his minority stake (acquired two years earlier for a much lower price) to another company authorised to build a wind farm. The majority stake belonged to a firm owned by another lawyer specialising in the renewable energy sector and involved in several law enforcement investigations concerning the infiltration of organised criminal organisations in the sector.

The whole company was purchased by a major corporation operating in the energy sector. Financial flows showed that the parent firm of the company being sold received €59million from the corporation. Although most of the funds were either used in instalments to repay lines of financing previously obtained both from Italian and foreign lenders or transferred to other companies belonging to the same financial group, some funds were credited to the account held in the name of the law firm of which the reported lawyer was a partner. Transfers to other legal professional were also observed.

Source: Italy (2012) questionnaire response

Case 30 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Client is known to have connections with criminals • There is an excessively high price attached to the securities transferred, with regards to circumstances indicating such an excess or with regard to the sum declared in another operation.

METHOD 5: MANAGING CLIENT AFFAIRS AND MAKING INTRODUCTIONS

Because of their ethical and professional obligations, the involvement of legal professionals in a transaction or their referral of a client to other professionals or businesses often provides the activities of the criminal with a veneer of legitimacy.

TECHNIQUE: OPENING BANK ACCOUNTS ON BEHALF OF CLIENTS

Financial institutions who are complying with their AML/CFT obligations may choose not to provide bank accounts to certain individuals who pose a high risk of money laundering or terrorist financing. In the questionnaire responses and literature reviewed, there were cases where legal professionals have either encouraged financial institutions to open accounts (despite being aware of the money laundering risks) or have opened accounts specifically for the use of clients, in such a way as to avoid disclosing to the financial institution the true beneficial owner of the account.

The lack of alleged access to a bank account may be a red flag indicator that the individual is subject to sanctions or a court freezing or restraint order.

Case 31: **Legal professional assisting client to obtain banking services despite warning signs of money laundering by a politically exposed person – common law country**

From 2000 to 2008, Jennifer Douglas, a U.S. citizen and the fourth wife of Atiku Abubakar, former Vice President and former candidate for President of Nigeria, helped her husband bring over USD 40 million in suspect funds into the United States through wire transfers sent by offshore corporations to U.S. bank accounts. In a 2008 civil complaint, the U.S. Securities and Exchange Commission alleged that Ms. Douglas received over USD 2 million in bribe payments in 2001 and 2002 from Siemens AG, a major German corporation.

While Ms. Douglas denies wrongdoing, Siemens has already pled guilty to U.S. criminal charges and settled civil charges related to bribery. Siemens told the Senate Permanent Subcommittee on Investigations that it sent the payments to one of Ms. Douglas' U.S. accounts. In 2007, Mr. Abubakar was the subject of corruption allegations in Nigeria related to the Petroleum Technology Development Fund.

Of the USD 40 million in suspect funds, USD 25 million was wire transferred by offshore corporations into more than 30 U.S. bank accounts opened by Ms. Douglas, primarily by Guernsey Trust Company Nigeria Ltd., LetsGo Ltd. Inc. and Sima Holding Ltd.

The U.S. banks maintaining those accounts were, at times, unaware of her Politically Exposed Person (PEP) status, and they allowed multiple, large offshore wire transfers into her accounts. As each bank began to question the offshore wire transfers, Ms. Douglas indicated that all of the funds came from her husband and professed little familiarity with the offshore corporations actually sending her money. When one bank closed her account due to the offshore wire transfers, her lawyer helped convince other banks to provide a new account.

Source: United States Senate Permanente Subcommittee on Investigations (2010)

Case 31 **Red flag indicators:**	• Client requires introduction to financial institutions to help secure banking facilities • Client has family ties to an individual who held a public position and is engaged in unusual private business given the frequency or

	characteristics involved. • Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Private expenditure is being funded by a company, business or government.

Case 32: **Legal professionals create shell companies and permit transfers through their client account without underlying transactions to help a PEP suspected of corruption to access financial services – common law country**

Teodoro Nguema Obiang Mangue is the son of the President of Equatorial Guinea and the current Minister of Agriculture of that country. He used two attorneys in the U.S. to form shell corporations and launder millions of dollars through accounts held by those corporations to fund real property, living expenses, and other purchases in the U.S.

The shell corporations hid the identity of Obiang as a PEP, and, particularly, a PEP whose family had a reputation for corruption and contributed to the dismemberment and sale of an entire U.S. financial institution, Riggs Bank. Obiang's further use of his attorney's trust accounts to receive wire transfers from Equatorial Guinea, helped to provide an apparently legitimate reason for transfers from a high-risk country

As banks became aware of Obiang's connection to the shell companies and shut down their accounts, the attorneys would open new accounts and new institutions, concealing Obiang's beneficial ownership once again.

The Department of Justice has filed civil forfeiture actions in two district courts in Los Angeles and Washington to forfeit the proceeds of foreign corruption and other domestic offenses laundered through the U.S. *See* U.S. Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Keeping Foreign Corruption out of the United States: Four Case Histories* (Feb. 4, 2010).

Source: United States questionnaire response 2012: United States v. One White Crystal Covered Bad Tour Glove No.11-cv-3582 (C.D. Cal.), and United States v. One Gulfstream G-V Jet Aircraft, No. 11-cv-1874 (D.D.C.)

Case 32 **Red flag indicators:**	• Client required introduction to financial institutions to help secure banking facilities. • Client is a public official and has family ties to a head of state and is engaged in unusual private business given the frequency or characteristics involved • Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Private expenditure is being funded by a company, business or government. • There is an attempt to disguise the real owner or parties to the transaction.

Case 33: **Legal professional coordinates banking activities and sets up companies to assist with laundering – civil law country**

An individual in the Netherlands set up three companies. For one of the companies he held bearer shares. To hide his involvement in the companies he used a front man and a trust and company service provider as legal representatives.

For each of the companies, the legal representatives opened bank accounts with three different banks in different countries. The individual used the three companies to set up a loan-back scheme in order to transfer, layer and integrate his criminal money. He then co-mingled the criminal funds with the funds that originated from the legal activities of one of his companies. Next the front man bought real estate. To finance that transaction he arranged for a loan between the two companies.

Source: FATF (2007)

Case 33 **Red flag indicators:**	• There is an attempt to disguise the real owner or parties to the transaction. • Client required introduction to financial institutions to help secure banking facilities. • The transactions are unusual in that there is unexplained complexity in the structures and the funding arrangements. • Finance is being provided by a lender, other than a credit institution with no logical explanation or economic justification.

TECHNIQUE: INTRODUCTION TO OTHER PROFESSIONALS FOR PARTS OF A TRANSACTION

Other professionals, including other legal professionals, may not ask detailed CDD questions, where a client is referred to them by a legal professional. While making referrals or seeking additional expertise in another field to ensure the client obtains full advice is normal, receiving payment for such referrals may or may not be legal depending on the country.

Case 34: **Legal professional provides cover story for client when providing funds to a notary for a property purchase – civil law country**

Upon executing a deed of sale of a property, a notary received a cheque from the buyer‘s lawyer, Mr. M.

The lawyer pointed out to the notary that the money originated from the sale of a property that belonged to Mr. M‘s family. The cheque was first endorsed in favour of Mr. M‘s family before being endorsed to the notary. The cheque was issued from the lawyer‘s personal account rather than his client account.

Mr M’s bank account was credited by cash deposits, and thereafter, was mainly debited by mortgage repayments. Mr. M was known to the police for organised crime and armed robbery, for which he had already been convicted.

Source: Deloitte (2011)

Case 34 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • The transaction is unusual as while there is a requirement in law for

	the notary to be involved in the transaction, there was no legitimate reason for the funds to be passed through the lawyer, and it would be against client account rules for the lawyer to put client's money into his personal account.

Case 35: **Criminal defence legal professional introduces clients to other professionals to assist with laundering the proceeds of their crime – common law country**

A prominent criminal defence attorney in Boston, Robert A. George helped a former client launder USD 200 000 in proceeds from various crimes, including wire fraud and cocaine distribution. George connected his former client to "his guy" who owned a mortgage company in Massachusetts and who accepted currency in duffel bags from the former client. George's associate then cut cheques to the former client to make the illicit funds appear to be a loan.

George was paid a fee for his part in the laundering scheme and also arranged a fee-splitting agreement with the former client to refer other criminals to him so that George could represent them in federal cases and launder their drug proceeds. Furthermore, George structured a USD 25 000 cash "retainer fee" from an undercover agent posing as a drug dealer into a bank account held in the name of his law firm, and issued a cheque to the apparent drug dealer with a memorandum note meant to conceal the purpose of the transaction. A notice of appeal has been filed in this case.

George was sentenced on October 31, 2012, to three and a half years for money laundering and related crimes following his jury trial in June 2012. George was convicted of money laundering conspiracy, aiding and abetting money laundering, money laundering, and structuring transactions to avoid reporting requirements.

Source: United States (2012) questionnaire response - United States v. George, No. 11-cr-10201-NMG (D. Mass.)

Case 35 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime. • Disproportionate amounts of cash and private funding in terms of the client's known legitimate income. • Legal professional's referral to non-legal professional constitutes professional ethics rule violations

TECHNIQUE: MANAGEMENT OF A CLIENT'S GENERAL AFFAIRS

Another feature of the highlighted cases involves the legal professional undertaking a range of 'management' activities for clients. In some jurisdictions this is referred to as 'man of affairs work' which is permitted in limited circumstances by some professional rules.

Situations where a legal professional may be undertaking these activities legitimately may involve a client who has limited capacity to manage their own affairs, or in other circumstances where the client has limited other options or a clear legitimate rational for seeking the continuing assistance from his/her legal professional. The legal professional, whether acting pursuant to a court order or a power of attorney, may use his/her client account to undertake transactions, but would more typically use accounts held by the client for whom the legal professional is acting.

In reported cases where illicit proceeds were involved, clients have had full capacity to manage their affairs and there is limited justification requiring specialist skills of the legal professional or use of their client account.

From the cases considered during this typology, it is apparent that the legal professional is more likely to be either complicit or wilfully blind to the red flag indicators of money laundering when this technique is employed In order to act in the client's best interests in such situations it is imperative they fully understand the financial and business affairs they are being asked to manage.

Other management activities may raise the question as to whether the legal professional is really acting as a financial advisor and mortgage broker. Such conduct especially when provided without connection to other legal services, may not be within the scope of the activities of a legal professional; may require separate licensing depending on the country; and may not attract professional secrecy/ legal professional privilege.

Case 36: **Criminal defence legal professional introduces clients to other professionals to assist with laundering the proceeds of their crime – common law country**

A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments to mortgages on properties beneficially owned by the drug trafficker.

The lawyer received commissions from the sale of these properties and brokering the mortgages.

While he later admitted to receiving the cash from the trafficker, depositing it into his trust account and administering payments to the trafficker's mortgages, the lawyer denied knowledge of the source of funds.

Source: FATF (2004)

Case 36 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • Disproportionate amounts of cash and private funding in terms of the client's known legitimate income. • Client is using an agent or intermediary without good reason.

Case 37: **Legal professional undertakes financial transaction unrelated to the provision of legal services to hide funds from a bankruptcy**

A trading company, operated by the client's spouse, was declared bankrupt.

Shortly afterwards the client deposited cash (from the bankrupt company) in an account opened in the name of a family member.

The money was immediately paid by cheque to the account of a legal professional.

The legal professional deposited part of the funds back into the family member's account and used the rest to purchase a life assurance policy, via a bank transfer. The policy was immediately cashed in by the family member.

Source: Belgium (2012) questionnaire response

Case 37 **Red flag indicators:**	• Private expenditure is being funded by a company • The transaction is unusual in terms of funding arrangements, who the client is, and the reason for the involvement of the legal professional. • The use of "U-turn" transactions where money is transferred to a legal professional or other entity and then sent back to the originating account in a short timeframe • Insurance policies cashed in shortly after purchase or loans and mortgages paid quickly, in full

METHOD 6: LITIGATION

Litigation is not an activity covered by the FATF Recommendations and, as outlined above, the courts to date have held that its exclusion is important for the protection of the fundamental human right of access to justice. However, in the case of Bowman v Fels[41] – the only case to specifically consider the question in the context of a real case involving clients[42] – the English Court of Appeal held that while genuine litigation should be exempt from the reporting requirements, sham litigation would not as such litigation is an abuse of the court's processes.

Litigation could constitute *sham litigation* if the subject of the dispute was fabricated (for example if there is no actual debt and the funds being transferred are simply the proceeds of crime being passed from one entity to another) or if the subject of the litigation was a contract relating to criminal activity which a court would not enforce.[43]

Case 38: **Legal professionals pursue debts relating to criminal activity – civil law country**

In 2005, two lawyers unsuccessfully defended two clients who were prosecuted for criminal offences. They then assisted those clients to recover debts of over 5 million NOK from other known criminals. Both lawyers were convicted of money laundering.

Source: Norway (2012) questionnaire response

Case 38 **Red flag indicators:**	• Client with known convictions for acquisitive crime • Debts relate to contract based on criminal activity

Case 39: **Legal professional files STR on debt recovery transaction without economic rationale – civil law country**

In 2011, a notary submitted an STR on the unusual movement of funds between companies as a purported debt recovery action. A lawyer acting for Company A created two further limited liability companies in Spain – Company B and Company C.

Within a month, four significant transactions take place on the same day which all required involvement of notary:

1. Mr X (an Italian national, whom the press reported was linked to the Mafia) acknowledges to a notary, a debt of around EUR 440 000 they owned to Company B, but it is not clear on what basis this debt exists.
2. Mr X sells a number of real estate properties to Company B for approximately EUR 460 000, which is paid through an electronic transfer, a bankers draft and a credit agreement.
3. Company A sells the shares for Company B to Company C.
4. The shares in Company C are bought by a Swiss company.

41 [2005] EWCA Civ 226.

42 All of the other cases were constitutional challenges on the legitimacy of legislation in principle.

43 Corbin A.L 1962 Corbin on Contracts West Publishing Co.

Later that year, Company B acknowledges to a notary a debt of around EUR 600 000 to the Swiss Company, who bought Company C. The agreement the notary is asked to confirm involves quarterly payments of EUR 7 500 with the Swiss company obtaining stock options for Company C. The basis of this debt was also unclear.

Source: Spain (2012) questionnaire response

Case 39 **Red flag indicators:**	• There are multiple appearances of the same parties in transactions over a short period of time. • Large financial transactions requested by recently set up companies, not justified by the activity of the client. • Creation of complicated ownership structures where there is no legitimate or economic reason There was no legitimate economic reason to create two companies, where the intention was to sell one to the other in such a short space of time, especially when control over both was passed to a company domiciled in another country at the same time. The creation of the purported debts and significant real estate purchase were designed to give the appearance of commercial business relationships to justify the transfer of value between Italy and Switzerland, via Spain. • A party to the transaction has known links to organised crime.

Case 40: **Legal practitioners receive requests for use of client account to recover debts with little or no legal services to be provided – common law country**

Australian legal practitioners have advised AUSTRAC of receiving unusual requests from prospective clients, particularly targeted at passing funds through solicitors' trust accounts. This included a foreign company requesting legal services involving debt recovery, with the legal firm receiving substantial payments into its trust account from purported debtors (both in Australia and overseas) with little debt recovery work actually being required to be undertaken by the firm.

These types of approaches to legal professionals have been noted by FIUs and SRBs in a number of countries, although no detailed case studies were provided.

Source: AUSTRAC (2011)

Case 40 **Red flag indicators:**	• Client and/or debtor are located at a distance from the legal professional • The type of debt recovery is unusual work for the legal professional • The client has written a pre-action letter to the debtor naming the legal professional and providing the legal professional's client account details • The litigation is settled very quickly, sometimes before the legal professional has actually written to the debtor • Client is unconcerned about the level of fees • There is a request for the funds received from the debtor to be paid out very quickly, sometimes to third parties.

METHOD 7: OTHER METHODS

TECHNIQUE: USE OF SPECIALISED LEGAL SKILLS

Legal professionals possess a range of specialised legal skills which may be of interest to criminals, in order to enable them to transfer value obtained from criminal activity between parties and obscure ownership.

These specialised skills include the creation of financial instruments, advice on and drafting of contractual arrangements, and the creation of powers of attorney.

In other areas of legal specialisation, such as probate (succession) and insolvency or bankruptcy work, the legal professional may simply come across information giving rise to a suspicion that the deceased or insolvent individual previously engaged in criminal activity or that parties may be hiding assets to avoid payment to legitimate creditors. Countries differ on how unexpected sums of cash are treated in relation to probate or insolvency cases, in some a threshold report will be made and the government becomes a super-creditor able to recover the money before any other beneficiary; in other countries this would give rise to a suspicion of money laundering, requiring a STR to be filed and possibly putting the executor or the legal professional at risk of money laundering.

Depending on the complexity of the arrangement, a legal professional could be unwittingly involved in the money laundering, complicit or wilfully blind through failing to ask further questions about suspicious instructions.

Case 41: **Legal professional prepares a power of attorney to dispose of all assets belonging to a client facing drug trafficking charges**

A legal professional was asked to prepare a power of attorney for a client to give control of all of his assets to his girlfriend, including power to dispose of those assets.

The legal professional then prepared a deed of conveyance under which the girlfriend transferred all of the property to the client's brother and sister.

The legal professional had just secured bail for the client in relation to a drug trafficking charge.

The legal professional was acquitted of money laundering.

Source: Trinidad & Tobago (2012) questionnaire response

Case 41 **Red flag indicators:**	• A power of attorney is sought for the disposal of assets under conditions which are unusual and where there is no logical explanation – it would have to be very exceptional circumstances for it to be in the client's best interests to allow them to make themselves impecunious. • Unexplained speed and complexity in the transaction. • Client is known to be under investigation for acquisitive crime.

Case 42: **Legal professional submits STR on commercial arrangement which has not economic rationale – civil law country**

In 2008 a Spanish citizen (Mr A) and a citizen from a Middle East country (Mr B) attended a notary office to formalise a contract which provided:

1. Mr A is the holder of a Gold Import Licence from an African Republic.
2. Mr B will fund the gold importation by making a payment of EUR 8 000, through a promissory note of EUR 6 000 maturing later that year and the remaining EUR 2 000 in cash three days after the promissory note matures.
3. Mr A will make payments of EUR 4 000 per month to Mr B, on the 22nd of each month for an indefinite period to represent the profits of the gold import activity.
4. Either party may terminate the agreement, with Mr A refunding the EUR 8 000 to Mr B and an agreement that the termination will be accepted without question.

These are new clients for the notary, Mr A refuses to provide certain identification information requested by the notary and no records supporting any business activity of any kind by either party are provided. The notary submitted an STR.

Source: Spain (2012) questionnaire response

Case 42 **Red flag indicators:**	• The client is reluctant to provide information usually required in order to enable the execution of the transaction. • There are a number of high risk countries involved in the transaction • The transaction makes no economic sense given the evident imbalance suffered by Mr A. • The transaction was unusual for this notary, given their unfamiliarity with the parties, the gold import business and the international elements of the transaction.

Case 43: **Legal professionals uncover funds tainted by criminal activity during administration of an estate – common law country**

A firm of solicitors was instructed to act in the administration of a deceased person's estate.

When attending the deceased's property a large amount of cash was found.

In addition, the individual had a savings account holding GBP 20 000.

As part of the administration of the estate the solicitor subsequently identified that the individual was receiving state benefits, to which they would not have been entitled if the hidden assets had been known, thus meaning that the entire estate of the client was now tainted by this criminality

The solicitor filed an STR.

Source: United Kingdom (2012) presentation at typologies workshop

Case 43 **Red flag indicators:**	• Disproportionate levels of private funding and cash which is inconsistent with the socio-economic profile of the individual. • Information suggesting involvement in acquisitive criminal activity.

Case 44: **Legal professional's attention drawn to unusual purchases of assets during the administration of a bankruptcy – civil law country**

In a bankruptcy case where A and B were guarantors, a notary was appointed by the court to proceed with the public sale of different goods of the parties concerned. In the context of the public sale. The attention of the notary was drawn to the fact that several of the goods were purchased by X, the daughter of A and B. Additionally, the total amount of the purchases was significant and was not commensurate with the socio-economic status of X, who was unemployed.

The purchased goods were partially funded by a cheque of a mortgage loan that a bank granted to X. The balance came from an account which was opened in the name of a third person, C.

This account had received several deposits in cash and transfers from a company of which both C and B were partners. B had been a partner in different companies that were declared bankrupt and for which he was known to the judicial authorities. Further, the daughter who had purchased the goods was not a director of this company, was not subject to VAT in Belgium and her official income consisted only of unemployment benefits.

With this information the FIU research indicated that the funds that were deposited on the accounts of C in cash may have come from funds that B had taken without permission to help his daughter to buy a part of his own real estate. C and B knew each other as they were partners in the same company.

In this case, the account of C was used as inadvertent account to conceal the illegal origin of the funds. Taking the above elements the various purchases of X can therefore be associated with a crime relating to the bankruptcy. A law enforcement investigation started.

Source: Cellule de traitement des informations Financières (2006)

Case 44 **Red flag indicators:**	• The ties between the parties are of a family nature, which generate doubts as to the real nature or reason for the transaction. • Disproportionate private funding which was inconsistent with the socio-economic profile of the individual. • Third party funding with no apparent connection or legitimate explanation

TECHNIQUE: PAYMENT OF LEGAL FEES AND ASSOCIATED EXPENSES

In some countries there are specific exemptions to enable legal practitioners to be paid with the proceeds of crime for defence purposes, provided that the defence fees are reasonable to the services rendered and that any remaining funds are not returned to the client or to third parties. In other countries this would still constitute money laundering and the fees paid would be amenable to confiscation proceedings.

Case 45: **Legal practitioner uses known criminal funds to pay for expenses of client who was in prison – common law country**

Miguel Rodriguez-Orejuela was a leader of the Cali Cartel who required and enforced a vow of silence from his associates and employees. In return for this vow of silence regarding his association

with drug trafficking, Rodriguez-Orejuela agreed to pay the defence expenses of any of his associates and to compensate their families while they were in prison.

Through his law firm, Michael Abbell facilitated the payments to family and prison commissary accounts on behalf Rodriguez-Orejuela. The funds Abbell accepted to reimburse these payments came from Rodriguez-Orejuela, who had no legitimate form of income (all his businesses were in fact funded by narco-trafficking). Abbell would make the payments, often using money orders paid for by the law firm, and then bill Rodriguez-Orejuela for reimbursement and fees. The transactions were designed to conceal the fact that Rodriguez-Orejuela was funding the payments and was associated with drug activity.

After two trials, a jury convicted Abbell of money laundering and racketeering charges. *See* 271 F.3d 1286 (11th Cir. 2001) (affirming convictions and reversing district court's grant of judgment of acquittal on racketeering-related counts). Abbell was sentenced to 97 months' incarceration.

Source: United States (2012) questionnaire response United States v. Abbell, No. 93-cr-470(17) (S.D. Fla.)

Case 45 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income. • There is an attempt to disguise the real owner or parties to the transactions.

Case 46: **Legal practitioner accepted large amounts of cash from a known criminal to pay for legal fees – common law country**

Defense attorney Donald Ferguson was indicted on four counts of money laundering, and one count of conspiring to launder money. Ferguson accepted four large sums of cash totalling USD 566 400 from Salvador Magluta. Ferguson deposited the cash payments into his attorney trust accounts, supposedly as payment for the defence of an associate of Magluta. Ferguson ultimately pleaded guilty to one count of money laundering and consented to the forfeiture of the full amount of the payments. He was sentenced to five years' probation. *See* 142 F. Supp. 2d 1350 (S.D. Fla. 2000) (declining to dismiss indictment).

Source: United States (2012) questionnaire response United States v. Ferguson, No. 99-cr-116 (S.D. Fla.)

Case 46 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income.

Case 47: **Legal practitioner paid 'salary' by organised criminals to be available to represent their needs, irrespective of whether legal services were provided – civil law country**

In July 1999 La Stampa reported a criminal lawyer and accountant arrested by DIA,17 (Anti-mafia Investigation Department), who were charged with facilitating funds from illicit sources on the French Riviera. The arrests were the consequence of investigations and electronic surveillance

(phone and environmental wiretapping), corroborated by the lawyer's confession. The lawyer's office was the operational base for the criminal activities of two high-profile mafia bosses. According to the indictment, the lawyer was paid a monthly salary of about EUR 6 000 to be always available for the needs of the mafia family.

Source: Di Nicola, A. and Zoffi, P. (2004)

Case 47 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income. • Payment of a general retainer rather than fees for specific services, where professional rules require the provision of itemised bills.

TECHNIQUE: PROVIDING LEGAL SERVICES FOR CHARITIES

Legal professionals may be involved in setting up charities or other non-profit entities, acting as a trustee, and providing advice on legal matters pertaining to the charity, including advising on internal investigations.

Like many other businesses, charities can be victims of fraud from trustees, employees and volunteers or be set up as vehicles for fraud, which will involve the proceeds of crime and subsequent money laundering. FATF typologies have also identified a particular vulnerability for charities in the financing of terrorism. [44]

Case 48: **Legal professional sets up charity to provide funding to individuals convicted of terrorist activities – civil law country**

This case has been brought to the attention of the Dutch Bureau for Supervision. A Foundation was established by a person related to a member of an organization whose purpose is committing terrorist offences. This person was herself not designated on international sanctions. The goal for the foundation was to provide help to persons convicted of terrorist activities. A first notary refused to establish the foundation, while a second notary agreed to do so.

Providing this form of financial assistance to a person convicted of terrorist activities, given the specific circumstances of the case, did not constitute an offence of financing terrorism, so no prosecutions were brought.

Source: Netherlands (2012) questionnaire response

Case 48 **Red flag indicators:**	• Client is related to a person listed as having involvement with a known terrorist organisation • Funding is to be provided to a person convicted of terrorist activities

44 FATF (2008b); FATF typology 2002-2003.

Case 49: **Legal professional sets up charities to undertake criminal activity and deal with the proceeds of that crime – common law country**

Attorney and lobbyist Jack Abramoff pleaded guilty in 2006 to three counts including conspiracy to defraud the United States, tax evasion, and "honest services" fraud (a corruption offense), upon the filing of a criminal information in the U.S. District Court for the District of Columbia. While working for two law and lobbying firms between 1999 and 2004, Abramoff solicited and lobbied for various groups and businesses, including Native American tribal governments operating or interested in operating casinos.

Abramoff conspired with former Congressional staff member Michael Scanlon to: defraud his lobbying clients by pocketing approximately USD 50 million; misuse his charitable organization by using it to finance a lavish golf trip to Scotland for public officials and others; and to provide numerous "things of value" to public officials in exchange for benefits to his clients.

In one set of schemes, Abramoff employed a non-profit that he founded called Capital Athletic Foundation. The Foundation was intended to fundraise for a non-profit school and it was granted tax-exempt status from the Internal Revenue Service, however, Abramoff used it as a personal slush fund. One congressional staffer solicited a contribution from a Russian distilled beverage company and Abramoff client on behalf of the Foundation. Abramoff used the Russian client's donation for personal and professional benefit, namely, to finance a trip to Scotland attended by members of Congress that cost the Foundation approximately USD 166 000.

Another Abramoff client, a wireless company, was solicited to make a contribution of at least USD 50 000 to the Foundation, in exchange for Abramoff securing a license for the company without charging his firm's usual lobbying fee or even informing his firm of the arrangement. According to the criminal information, Abramoff also concealed assets and sources of income from the Internal Revenue Service through the use of nominees, some of which were tax-exempt organizations.

Although not detailed in the court filings in this case, it was widely reported at the time that a congressional staff member's spouse received USD 50 000 from another non-profit affiliated with Abramoff, which in turn, received money from Abramoff clients interested in internet gambling and postal rate issues before Congress. Further, the Capital Athletic Foundation allegedly donated USD 25 000 to Representative and House Majority Leader Tom DeLay's Foundation for Kids. These are just a few examples of Abramoff's misuse of non-profits, some of which were founded by him and some of which existed previously and accepted contributions from Abramoff, Scanlon, or their clients, often due to Abramoff's personal relationships with the heads of such charities.

Abramoff was also indicted in 2005 in the Southern District of Florida in connection with a massive fraud that he conducted involving his purchase of a casino and cruise company. Abramoff pleaded guilty to two more counts of conspiracy and wire fraud in the Florida case, which did not involve the misuse of tax-exempt entities. He was never charged with money laundering.

Source: United States (2012) questionnaire response - United States v. Abramoff, No. 06-cr-00001 (D.D.C.)

Case 49 **Red flag indicators:**	• Non-profit organisation engages in transactions not compatible with those declared and not typical for that body • There are attempts to disguise the real owner or parties to the transactions

CHAPTER 5

RED FLAG INDICATORS

As outlined in Chapter 4 the methods and techniques used by criminals to launder money may also be used by clients with legitimate means for legitimate purposes.

Because of this, red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation.

These red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements of knowing who their client and the beneficial owners are, understanding the nature and the purpose of the business relationship, and understanding the source of funds being used in a retainer. Where there are a number of red flag indicators, it is more likely that a legal professional should have a suspicion that ML or TF is occurring.

SRBs and law enforcement may also find these red flag indicators to be useful when monitoring the professional conduct of or investigating legal professionals or their clients. Where a legal professional has information about a red flag indicator and has failed to ask questions of the client, this may be relevant in assessing whether their conduct was complicit or unwitting.

This chapter contains a collection of red flag indicators identified through the case studies, literature reviewed, and existing advice published by FIUs and SRBs which were provided in response to the questionnaire.

RED FLAGS ABOUT THE CLIENT

- Red flag 1: The client is overly secret or evasive about:
  - who the client is
  - who the beneficial owner is
  - where the money is coming from
  - why they are doing this transaction this way
  - what the big picture is.
- Red flag 2: The client:
  - is using an agent or intermediary without good reason.
  - is actively avoiding personal contact without good reason.

- is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution
- holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved.
- provides false or counterfeited documentation
- is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact.
- is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals
- is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities.
- shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries and suspicious transaction reports – that is – asks repeated questions on the procedures for applying the ordinary standards.

- Red flag 3: The parties:
  - The parties or their representatives (and, where applicable, the real owners or intermediary companies in the chain of ownership of legal entities), are native to, resident in or incorporated in a high-risk country
  - The parties to the transaction are connected without an apparent business reason.
  - The ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason for the transaction.
  - There are multiple appearances of the same parties in transactions over a short period of time.
  - The age of the executing parties is unusual for the transaction, especially if they are under legal age, or the executing parties

are incapacitated, and there is no logical explanation for their involvement.

- There are attempts to disguise the real owner or parties to the transaction.
- The person actually directing the operation is not one of the formal parties to the transaction or their representative.
- The natural person acting as a director or representative does not appear a suitable representative.

RED FLAGS IN THE SOURCE OF FUNDS

- Red Flag 4: The transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.
- Red flag 5: The client or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation.
- Red flag 6: The source of funds is unusual:
  - third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation
  - funds received from or sent to a foreign country when there is no apparent connection between the country and the client
  - funds received from or sent to high-risk countries.
- Red flag 7: The client is using multiple bank accounts or foreign accounts without good reason.
- Red flag 8: Private expenditure is funded by a company, business or government.
- Red flag 9: Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation.
- Red flag 10: An unusually short repayment period has been set without logical explanation.
- Red flag 11: Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.
- Red flag 12: The asset is purchased with cash and then rapidly used as collateral for a loan.

- Red flag 13: There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested which are not appropriate for the common practice used for the ordered transaction.
- Red Flag 14: Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.
- Red Flag 15: The collateral being provided for the transaction is currently located in a high-risk country.
- Red flag 16: There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.
- Red flag 17: There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.
- Red flag 18: The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation.
- Red flag 19: There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (*e.g.* volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.

- Red flag 20: Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons.

RED FLAGS IN THE CHOICE OF LAWYER

- Red flag 21: Instruction of a legal professional at a distance from the client or transaction without legitimate or economic reason.
- Red flag 22: Instruction of a legal professional without experience in a particular specialty or without experience in providing services in complicated or especially large transactions..
- Red flag 23: The client is prepared to pay substantially higher fees than usual, without legitimate reason.
- Red flag 24: The client has changed advisor a number of times in a short space of time or engaged multiple legal advisers without legitimate reason

- Red flag 25: The required service was refused by another professional or the relationship with another professional was terminated.

RED FLAGS IN THE NATURE OF THE RETAINER

- Red flag 26: The transaction is unusual, *e.g.*:
    - the type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting
    - the transactions are unusual because of their size, nature, frequency, or manner of execution
    - there are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional
    - a non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body.
- Red flag 27: The client:
    - is involved in transactions which do not correspond to his normal professional or business activities
    - shows he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested
    - wishes to establish or take over a legal person or entity with a dubious description of the aim, or a description of the aim which is not related to his normal professional or commercial activities or his other activities, or with a description of the aim for which a license is required, while the customer does not have the intention to obtain such a licence
    - frequently changes legal structures and/or managers of legal persons
    - asks for short-cuts or unexplained speed in completing a transaction
    - appears very disinterested in the outcome of the retainer
    - requires introduction to financial institutions to help secure banking facilities

- Red flag 28: Creation of complicated ownership structures when there is no legitimate or economic reason.
- Red flag 29: Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason.
- Red flag 30: Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short period of time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation.
- Red flag 31: There is an absence of documentation to support the client's story, previous transactions, or company activities.
- Red flag 32: There are several elements in common between a number of transactions in a short period of time without logical explanations.
- Red flag 33: Back to back (or ABC) property transactions, with rapidly increasing value or purchase price.
- Red flag 34: Abandoned transactions with no concern for the fee level or after receipt of funds.
- Red flag 35: There are unexplained changes in instructions, especially at the last minute.
- Red flag 36: The retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services.
- Red flag 37 There is a lack of sensible commercial/financial/tax or legal reason for the transaction.
- Red flag 38 There is increased complexity in the transaction or the structures used for the transaction which results in higher taxes and fees than apparently necessary.
- Red flag 39: A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation.
- Red flag 40: Investment in immovable property, in the absence of any links with the place where the property is located and/ or of any financial advantage from the investment.
- Red flag 41: Litigation is settled too easily or quickly, with little/no involvement by the legal professional retained.
- Red flag 42: Requests for payments to third parties without substantiating reason or corresponding transaction.

CHAPTER 6

CONCLUSIONS

KEY FINDINGS

This typology has found evidence that criminals seek out the involvement of legal professionals in their money laundering schemes, sometimes because the involvement of a legal professional is required to carry out certain types of activities, and sometimes because access to specialised legal and notarial skills and services may assist the laundering of the proceeds of crime and the funding of terrorism.

Case studies, STRs and literature point to the following legal services being vulnerable to misuse for the purpose of ML/TF:

- client accounts (administered by the legal professional)
- purchase of real property
- creation of trusts and companies
- management of trusts and companies
- setting up and managing charities
- administration of deceased estates
- providing insolvency services
- providing tax advice
- preparing powers of attorney
- engaging in litigation – where the underlying dispute is a sham or the debt involves the proceeds of crime.

Not all legal professionals are involved in providing these types of legitimate legal services that criminals may seek to abuse, but in some cases a legal professional may need to be involved. This makes the use of legal professionals carrying out these activities uniquely exposed to criminality, irrespective of the attitude of the legal professional to the criminality.

It is accepted that the vast majority of legal professionals seek to comply with the law and their professional requirements, and they have no desire to be involved in ML/TF activity. The legal profession is highly regulated. Furthermore, ethical obligations, professional rules and guidance on ML/TF provided by SRBs and professional bodies should cause legal professionals to refuse to act for clients who seek to misuse legal services for ML/TF purposes.

To keep legal professionals from becoming involved in ML/TF however, the above factors rely on the legal professionals:

- being alert to red flags indicating that the client is seeking to involve them in criminal activity
- choosing to abide by their ethical obligations and applicable professional rules; and
- discerning legitimate client wishes from transactions and structures intended to conceal or promote criminal activity or thwart law enforcement.

Equally, the application of FATF Recommendations to legal professionals over the last decade should provide the legal sector with tools to better identify situations where criminals are seeking to misuse legal services.

Some SRBs and professional bodies are quite active in educating their members on the ML/TF vulnerabilities they face and the red flag indicators which could alert them to a suspicious transaction. STRs from legal professionals have also assisted law enforcement in detecting and prosecuting criminals engaged in ML/TF activity.

However, not all legal professionals are undertaking the CDD measures required by the FATF Recommendations, and not all SRBs and professional bodies have a clear understanding of information on ML/TF vulnerabilities specific to the legal sector to provide to their members.

A lack of awareness and/or lack of education of ML/TF vulnerabilities and red flag indicators reduces the likelihood that legal professionals would be in a position prevent the misuse of their services and avoid a breach of their professional obligations.

This typology research recognises that investigating a legal professional presents more practical challenges than investigating other professionals, due to the important protections for fundamental human rights which attach to the discharge of a legal professional's activities. However, the research has also confirmed that neither legal professional privilege nor professional secrecy would ever permit a legal professional to continue to act for a client who was engaging in criminal activity.

The scope of legal professional privilege/professional secrecy depends on the constitutional and legal framework of each country, and in some federal systems, in each state within the country. Practically, this diversity and differing interpretations by legal professionals and law enforcement on what information is actually covered by legal professional privilege / professional secrecy has, at times provided a disincentive for law enforcement to take action against legal professionals suspected of being complicit in or wilfully blind to ML/TF activity.

OPPORTUNITIES FOR FUTURE ACTION

This typology study should be used to increase awareness of the red flag indicators for potential misuse of legal professionals for ML/TF purposes and in particular for:

- **Legal professionals –** as this would assist in reducing their unwitting involvement in ML/TF activities undertaken by their clients and promote the filing of STRs where appropriate;
- **Financial institutions and other DFNBPs** – as this may alert them to situations where legal professionals are complicit in their client's ML/TF activity or are not aware of the red flag indicators to promote the filing of STRs where appropriate;
- **SRBs and professional bodies** – as this will assist in developing training programmes and guidance which focus not just on the law but the practical application of the law to everyday legal practice and assist in identifying both witting and unwitting involvement in ML/TF activities as part of their monitoring of professional conduct; and
- **Competent authorities and partner law enforcement agencies –** to assist in their investigation of ML/TF where legal services are a method used and to inform the assessment of whether it is likely that the legal professional is involved wittingly or unwittingly, so that appropriate action can be taken.

Potentially, the increased education of legal professionals on ML/TF vulnerabilities may include a discussion of AML/CFT risks and obligations in the course of the legal education or licensing of legal new professionals. Initially, this education can take place in the context of ethics and professionalism in courses and law schools, and later, through continuing education curricula.

Competent authorities, SRBs and professional bodies should review the case examples in this typology study and fit them to the specific roles and vulnerabilities of their members.

Increased interaction between competent authorities, supervisors and professional bodies in terms of sharing information on trends and vulnerabilities, as well as notifying each other of instances where legal professionals are failing to meet their ethical and legal obligations in an AML/CFT context, may also assist in reducing misuse of legal professionals. SRBs and professional bodies may find the red flag indicators in this report useful when monitoring their members' conduct against professional and client account rules.

There will be many factors taken into consideration when deciding whether to criminally prosecute a legal professional for money laundering of failing to submit an STR where required. In some instances, it will be more appropriate and effective for the SRB or professional body to take disciplinary or remedial action where the legal professional's conduct falls short of professional requirements and permits money laundering to occur, but was not intended to aid in money laundering. This shared approach to enforcement not only helps to combat ML / TF, but also helps to ensure that legal professionals uphold the rule of law and do not bring the wider profession into disrepute.

Competent authorities, SRBs and professional bodies should work to ensure that there is a clear and shared understanding of the remit of confidentiality, legal professional privilege and/or professional secrecy in their own country. A clear understanding of the remit of these principles and the procedures for investigating a legal professional will assist in reducing mistrust from both

parties during this process and may help to dispel the perception that privilege or secrecy is designed to protect criminals. It may also assist in more prompt investigation and prosecution of those who would misuse the services of legal professionals or abuse their role as a legal professional, while reducing the concern of legal professionals that they may be sanctioned for breaching privilege or secrecy when complying with their AML/CFT obligations.

Finally, this typology found that the analysis of STRs made about legal professionals and the types of assets being confiscated provided useful information on the AML/CFT risks posed by the legal sector. Member states may wish to consider using these sources of information when assessing risks for the purpose of completing the national risk assessment in line with FATF Recommendation 1. FATF can also consider this work, in consultation with the legal sector, when updating its RBA Guidance for Legal Professionals and other DNFBPs.

ANNEX 1
BIBLIOGRAPHY

FATF (2004), Report on Money Laundering Typologies 2003-2004, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf

FATF (2006), *Misuse of Corporate Vehicles Including Trust and Company Service Providers*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf

FATF (2007), *Money Laundering and Terrorist Financing through the Real Estate Sector,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf

FATF (2008a) *Risk Based Approach Guidance for the Legal Sector, FATF, Paris,* www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf

FATF (2008b) *Terrorist Financing and Typologies Report,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

FATF (2010), *Money Laundering Using Trust and Company Service Providers*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf

FATF (2011), *Laundering the Proceeds of Corruption*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf

FATF (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations, FATF, Paris,* www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

AUSTRAC (2011) *Money laundering in Australia 2011*, Austrac, Australia, http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf

Cellule de traitement des information Financieres (2005), *Doorgemelde dossiers in verband met corruptie, typologische aspecten* (*files reported in connection with corruption, typological aspects*), Cellule de traitement des information Financieres, Belgium

Cellule de traitement des information Financieres (2006), *Notarissen en witwasbestrijding* (*Notaries and combating money laundering*), Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2007), *Jaarverslag 2007* (annual report 2007) Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2008), *Jaarverslag 2008* (annual report 2008) Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2009), *Jaarverslag 2009* (annual report 2009) Cellule de traitement des information Financieres, Brussels

Cummings, L. and Stepnowsky, P.T. (2011), *My Brother's Keeper: An Empirical Study of Attorney Facilitation of Money Laundering through Commercial Transactions*, University of Maryland Legal Studies Research Paper No. 2010-32, University of Maryland, College Park

Deloitte (2011), *Final Study on the Application of the Anti-Money Laundering Directive: Commissioned by the European Commission*, Deloitte DG Internal Market and Services – Budget, European Commission, Brussels

Dodek, A. (2011), *Solicitor-Client Privilege in Canada: Challenges for the 21st Century,* The Canadian Bar Association, Ottawa

Does, van der, E. et al. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It, Stolen Asset Recovery Initiative (StAR)*, World Bank/UNODC, Washington, D.C.

European Commission (2006), *The application to the legal profession of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering*, European Commission, Brussels

Gallant, M. (2010), *Uncertainties Collide: Lawyers and Money Laundering, Terrorist Finance Regulation*, Journal of Financial Crime, Vol. 16, University of Manitoba, Winnipeg

Global Witness (2009), *The Secret Life of a Shopaholic: How an African Dictator's Playboy Son Went on a Multi-million Dollar Shopping Spree in the US*, Global Witness, London, www.globalwitness.org/sites/default/files/pdfs/gw_obiang_low.pdf

IBA, OECD and UNODC (2010), *Risks and Threats of Corruption and the Legal Profession Survey*, IBA, OECD and UNODC, at www.oecd.org/investment/anti-bribery/46137847.pdf

International Bar Association (2011), *IBA International Principles on Conduct for the Legal Profession (IBA International Principles)*, London www.ibanet.org/Article/Detail.aspx?ArticleUid=BC99FD2C-D253-4BFE-A3B9-C13F196D9E60

International Union of Notaries (2004), *Principles of Notarial Ethics*, Rome http://uinl.net/presentacion.asp?idioma=ing&submenu=DEONTOLOGIA

Journal of Crime, Law & Social Change (2004), Vol. 42, Springer, Boston

- Levi, M. *et al.* (2004), "Lawyers as crime facilitators in Europe: An introduction and overview"

- Middleton, D.J. (2004), "The legal and regulatory response to solicitors involved in serious fraud"

- Middleton D.J. and Levi, M. (2004), "The role of solicitors in facilitating organised crime: situational crime opportunities and their regulation"

- Lankhorst, F. and Nelen, H. (2004), "Professional services and organised crime in the Netherlands"

- Chevrier, E., "The French government's will to fight organised crime and clean up the legal professions: the awkward compromise between professional secrecy and mandatory reporting"

- Di Nicola, A. and Zoffi, P. (2004), "Italian lawyers and criminal clients: Risks and countermeasures"

Parlementaire enquête-commissie opsporings-methoden (*parliamentary hearing regarding methods of investigation*) (1996), *Inzake Opsporing* ("Regarding investigation"), The Hague

Schneider, S. (2004), *Money Laundering in Canada: An analysis of RCMP cases*, Nathan Centre for the Study of Organized Crime and Corruption, Toronto, https://www.ncjrs.gov/App/publications/Abstract.aspx?id=232379

Tavares, C., et al. (2010), *Money Laundering in Europe: Report of Work Carried Out by Eurostat and DG Home Affairs*, Eurostat, Brussels

United States Senate Permanent Subcommittee on Investigations (2010), *Keeping Foreign Corruption Out of the United States: Four Case Histories*, United States Senate, Washington, D.C. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=2de71520-5901-4a31-98ad-5138aebc49c2

Van Dijken, A. (2009), *Verdachte transacties bij advocaten en juridisch adviseurs, een analyse van verdachte transacties uit 2009 gemeld door advocaten en juridisch adviseurs* (*Suspicious transactions at lawyers and legal advisers, an analysis of suspicious transactions reported by lawyers and legal advisers from 2009*), FIU-Netherlands, The Hague

Van Duyne, P.C., et al. Eds., (2007), *Crime business and crime money in Europe: the dirty linen of illicit enterprise,* Wolf Legal Publishers, Nijmegen

World Economic Forum (2012), *Organised Crime Enablers*, World Economic Forum, Geneva, www3.weforum.org/docs/WEF_GAC_OrganizedCrimeEnablers_Report_2012.pdf

Other Resources:

American Bar Association (2010), *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing, American Bar Association, Washington, D.C.,* www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_taskforce_gtfgoodpracticesguidance.authcheckdam.pdf

IBA Anti-Money Laundering Forum www.anti-moneylaundering.org/

Law Society of England and Wales (2012) Anti-Money Laundering Practice Note, Law Society, London www.lawsociety.org.uk/advice/anti-money-laundering/

Federation of Law Societies Canada Model Rules to Fighting Money Laundering and Terrorist Financing www.lawsociety.org.uk/advice/anti-money-laundering/

Law Council of Australia (2009) Anti-Money Laundering Guide for legal practitioners, Law Council, Canberra, www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=8FCE74BF-1E4F-17FA-D2A2-C549BD6656B4&siteName=lca

ANNEX 2
RESPONDENTS TO THE QUESTIONNAIRE

RESPONSES RECEIVED FROM MEMBER STATES AND ASSOCIATE MEMBER STATES:

Australia	Austria	Belgium
Canada	Denmark	Finland
France	Japan	Ireland
Italy	Japan	Netherlands
Norway	Portugal	Spain
Sweden	Switzerland	Turkey
United Kingdom	United States	Bermuda
Curacao	St Vincent & the Grenadines	Trinidad & Tobago
Gibraltar	Jordan	Liechtenstein
Montenegro		

RESPONSES RECEIVED FROM SRBS OR PROFESSIONAL BODIES IN THE FOLLOWING COUNTRIES:

Australia	Austria	Belgium
Canada	Denmark	France
Germany	Ireland	Italy
Japan	Luxembourg	Netherlands
Norway	Portugal	South Africa
Spain	Sweden	Switzerland
United Kingdom	United States	Bermuda
Curacao	Namibia	Saint Vincent & the Grenadines
Trinidad & Tobago	Malawi	Cyprus
Czech Republic	Estonia	Hungary
Montenegro	Poland	Slovakia
Slovenia	Swaziland	

ANNEX 3
DEFINITIONS

Mechanism: An ML/TF mechanism is a system or element that carries out part of the ML/TF process. Examples of ML/TF mechanisms include financial institutions, legal professionals, legal entities and legal arrangements.

Method: In the ML/TF context, a method is a discrete procedure or process used to carry out ML/TF activities. It may combine various techniques, mechanisms and instruments, and it may or may not represent a typology in and of its self.

Scheme: An ML/TF scheme is a specific operation or case of money laundering or terrorist financing that combines various methods (techniques, mechanisms and instruments) into a single structure.

Technique: An ML/TF technique is a particular action or practice for carrying out ML/TF activity. Examples of ML/TF techniques include structuring financial transactions, co-mingling of legal and illegal funds, over and under valuing merchandise, transmission of funds by wire transfer, etc.

Typology: An ML/TF typology is a pattern or series of similar types of money laundering or terrorist financing schemes or methods.

Legal professional: Lawyers, notaries and other independent legal professionals – this refers to sole practitioners, partners, or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

Legal professionals are covered by the FATF Recommendations when they prepare for or carry out transactions for their client concerning the following activities:

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

SRB: Self-regulatory body – is a body that represents a profession (*e.g.* lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing in the profession.

ANNEX 4
TYPES OF LEGAL PROFESSIONALS

The Risk Based Approach Guidance for Legal Professionals, produced by FATF, in consultation with the legal sector in 2008, provided high level definitions of the legal professionals in terms of Lawyers and Notaries.[45]

In summary these definitions highlighted the regulated nature of these professions, their important role in promoting adherence to the rule of law, providing impartial and independent legal advice on complex rights and obligations, and/or authenticating documents.

For this typology research, greater focus was on the actual areas of law and specific tasks in which different types of legal professionals provided services, to obtain a clearer understanding of which vulnerabilities may be more relevant to which legal professionals.

The questionnaire sent to SRBs specifically asked for information on whether their members:

- engaged in activities covered by the FATF Recommendations;
- only provided legal and advice and representation;
- held exclusive licences for a particular legal services; and
- held client money

From the many responses received a number of trends were identifiable:

1. Lawyers

   Legal professionals who would fall within the RBA Guidance category of lawyer may actually be referred to in their home country as: Advocate, Advogardo, Attorney, Barrister, Lawyer, Legal Practitioner, Rechtsanwalt, Solicitor, Trial Attorney, etc.[46]

   Between countries however, the exact legal services provided by legal practitioners with the same title and restrictions on their activities also differed.

   In some countries legal professionals within this category were predominantly listed as providing legal advice and representing their clients, often in court, sometimes in negotiations. While in other countries they provided legal advice and assisted their

45 www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf

46 For example the European Directive to facilitate practice of the profession of a lawyer on a permanent basis in a member state other than that in which the qualification was obtained provides a useful overview of lawyers in the European union. See the CCBE website for more information www.ccbe.eu/index.php?id=94&id_comite=8&L=0

clients with the preparation of documents and carrying out of transactions, as well as representing those clients in court and negotiations.

In many countries legal professionals in this category held an exclusive licence for representation in court, but generally they did not hold an exclusive licence for legal services covered by the FATF Recommendations.[47]

In most countries all legal professionals in this category were able to receive clients directly[48] and were able to hold client money, either in specified accounts or accounts held by their professional body.

Both confidentiality and either legal professional privilege or professional secrecy reportedly applied to many or all of the activities of legal professionals within this category.

2. Notaries[49]

There is a distinction between civil law notaries and common law 'notaries public', with the latter certifying signatures and documents and the former having the status of a qualified legal professional and of public office holders in terms of establishing authentic instruments in the area of preventative justice.[50]

Civil law notaries often have an exclusive licence in relation to their role in the following areas:

1. the law relating to real property, such as the preparation and registering of contracts and/or deeds transferring real property from one party to another.

2. the law relating to legal persons, such as incorporating companies, issuing shares and registering their transfer.

3. the law relating to persons and families, such as the preparation of prenuptial agreements, property agreements following a divorce and drafting wills.

In some countries the notary is appointed to a specific geographical area and it would be atypical of them to undertake notarial work for transactions relating to other geographic areas.

---

47 There are exceptions to this, for example in Bermuda barristers have an exclusive licence in relation to legal work involving the transfer of real property and in Hungary attorneys are the only legal professionals able to undertake legal work relating to real property and the formation of companies

48 An exception to this was found in some common law countries, where a barrister will usually only act for a client who has been referred to them by a solicitor. The barrister is also precluded from holding client funds.

49 In Japan the category of notary is not known, although similar activities are undertaken by Judicial Scriveners and Certified Administrative Procedures Specialists.

50 In addition to the information about the role of civil and common law notaries in the FATF RBA guidance, the Council of Notariats of the European Union provide information on the role of notaries on their website: www.notaries-of-europe.eu/notary-s-role/overview

These legal professionals would occasionally hold client money or facilitate the transfer of a monetary instrument such as a cheque between parties, always in a traceable and recorded way. They would deal with the clients (or an authorised representative) directly, but sometimes on referral from another legal professional.

Confidentiality generally applied to these legal professionals. Some SRBS advised that legal professional privilege or professional secrecy also applied to these legal professionals, but others said that it would not.

ANNEX 5
SCHEDULE OF CASES

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
1	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Financial Institution	Disciplinary sanction imposed	2, 23, 27
2	**Canada**	Misuse of Client Account	Transferring funds without providing legal services	Illicit Drug Trafficking	Financial Institution	No information	2, 3, 4, 36
3	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Corruption	Financial Institution	Disciplinary sanction imposed	36, 42
4	**Australia**	Misuse of Client Account	Structuring payments	Unspecified	Financial Institution, Real Estate	No information	2, 4, 5
5	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 18
6	**Spain**	Misuse of Client Account	Structuring payments	Fraud	Real Estate	STR filed by legal professional	2, 26
7	**United Kingdom**	Misuse of Client Account	Aborted transactions	Fraud	Company	Disciplinary sanction imposed	3, 34
8	**United Kingdom**	Misuse of Client Account	Aborted transactions	Unspecified	Real Estate	Removed from practice	2, 27, 34
9	**Belgium**	Property Purchases	Investment of proceeds of crime in property	Illicit trafficking in goods and merchandise	Real Estate	STR filed by legal professional	4, 26
10	**United Kingdom**	Property Purchases	Investment of proceeds of crime in property	Unspecified	Real Estate	Legal professional acted as prosecution witness	2, 4, 5

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
11	**United Kingdom**	Property Purchases	Investment of proceeds of crime in property	Illicit Drug Trafficking	Real Estate	Criminal conviction	4, 5
12	**France**	Property Purchases	Transferring value - back to back or ABC sales	Unspecified	Financial Institution, Real Estate	No information	2, 3, 4, 24, 33
13	**France**	Property Purchases	Transferring value - sales within an organised crime group	Organised Crime	Real Estate	No information	3, 4, 26
14	**Australia**	Property Purchases	Obscuring ownership - purchase with false name / counterfeit documents	Illicit Drug Trafficking	Real Estate	No information	2, 26
15	**Canada**	Property Purchases	Obscuring ownership - purchasing [purchase] through intermediaries	Illicit Drug Trafficking, Fraud or Theft	Financial Institution, Real Estate	No information	2, 4, 11
16	**France**	Property Purchases	Obscuring ownership - purchase through a company or trust	Corruption (?)	Company, Financial Institution, Real Estate	No information	2, 3, 4, 21, 26, 28, 35
17	**Belgium**	Property Purchases	Obscuring ownership - purchase through a company or trust	Organised Crime (?)	Company, Financial Institution, Real Estate	Investigation commenced	2, 6, 28, 29
18	**Spain**	Property Purchases	Obscuring ownership - purchase through a company or trust	Illicit Drug Trafficking	Company, Real Estate	STR filed by legal professional	2, 3, 4, 19,20
19	**United Kingdom**	Property Purchases	Mortgage fraud with antecedent laundering	Fraud	Financial Institution, Real Estate	Disciplinary sanction imposed	2, 26, 27
20	**United Kingdom**	Property Purchases	Mortgage fraud with antecedent laundering	Unspecified	Financial Institution, Real Estate	Removed from practice	26, 28, 33

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
21	**Belgium**	Creation of Companies and Trusts	Creation of trusts to obscure ownership and retain control	Tax Fraud (?)	Company, Financial Institution, Real Estate, Trust	No information	2, 29
22	**FATF**	Creation of Companies and Trusts, Misuse of Client Account	Creation of trusts to obscure ownership and retain control	Smuggling	Company, Financial Institution, Trust, Real Estate	No information	2, 3, 28
23	**Japan**	Creation of Companies and Trusts	Creation of shell companies to place or layer	Loan Sharking	Company	No information	1, 2, 26
24	**Spain**	Creation of Companies and Trusts	Creation of shell companies to place or layer, Management of a company or trust - creation of legitimacy and provision of legal services	Organised Crime	Company	No information	2, 3, 29
25	**Spain**	Creation of Companies and Trusts, Management of Companies and Trusts	Use of bearer shares to obscure ownership, Creation of shell companies to place or layer	Unspecified	Company, Financial Institution, Real Estate	No information	2, 11, 33
26	**Jersey**	Creation of Companies and Trusts	Use of bearer shares to obscure ownership	Illicit Drug Trafficking	Company, Financial Institution	No information	2, 4, 29
27	**United States**	Management of Companies and Trusts	Acting as trustee - receiving the proceeds of crime	Illicit Drug Trafficking	Trust	Decision not to prosecute legal practitioner	3, 36
28	**Italy**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Money laundering operation	Company, Financial Institution	No information	2, 19
29	**United States**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Advance-fee scheme	Company, Financial Institution	Criminal conviction	2, 42

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
30	**Italy**	Management of Companies and Trusts	Holding shares as an undisclosed nominee	Organised Crime (?)	Company, Financial Institution	No information	2, 19
31	**United States**	Management of Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company, Financial Institution	No information	2, 8, 27, 29
32	**United States**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company, Financial Institution Real Estate	No information	2, 8, 27
33	**Netherlands**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Unspecified	Company, Financial Institution	No information	2, 14, 26, 27
34	**Egmont**	Managing Client Affairs and Making Introductions	Introduction of other professionals for parts of a transaction	Organised Crime	Financial Institution, Real Estate	No information	2, 26
35	**United States**	Managing Client Affairs and Making Introductions	Introduction of other professionals for parts of a transaction	Illicit Drug Trafficking	Company, Financial Institution	Criminal conviction	2, 4, 26
36	**FATF**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of a client's general affairs	Illicit Drug Trafficking	Financial Institution, Real Estate	No information	2, 4
37	**Belgium**	Managing Client Affairs and Making Introductions	Management of a client's general affairs	Fraud	Financial Institution, Insurance	No information	8, 11, 26
38	**Norway**	Litigation	Sham litigation	Unspecified	Unspecified	Criminal conviction	2, 41
39	**Spain**	Litigation	Sham litigation	Organised Crime (?)	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 3, 20
40	**Australia**	Litigation	Sham litigation	Unspecified	Company	STR filed by legal professional	21, 22, 27, 38, 41

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
41	**Trinidad & Tobago**	Other Methods	Use of specialised legal skills	Illicit Drug Trafficking	Real Estate	Legal professional acquitted	2, 27, 39
42	**Spain**	Other Methods	Use of specialised legal skills	Unspecified	Unspecified	STR filed by legal professional	2, 3, 22, 37
43	**United Kingdom**	Other Methods	Use of specialised legal skills	Fraud	Unspecified	STR filed by legal professional	2, 4
44	**Belgium**	Other Methods	Use of specialised legal skills	Fraud	Company, Financial Institution	Investigation commenced	3, 4, 5
45	**United States**	Other Methods	Payment of legal fees and associated expenses	Illicit Drug Trafficking	Financial Institution / Money or value transfer service	Criminal conviction	2, 4
46	**United States**	Other Methods	Payment of legal fees and associated expenses	Illicit Drug Trafficking	Unspecified	Criminal conviction	2, 4
47	**Italy**	Other Methods	Payment of legal fees and associated expenses	Organised Crime	Unspecified	Legal professional charged	2, 4, 26
48	**Netherlands**	Other Methods	Providing legal services for charities	Terrorism	Company (Foundation)	Decision not to prosecute legal practitioner	2, 25
49	**United States**	Other Methods	Providing legal services for charities	Fraud	Company (Foundation)	Criminal conviction (for predicate offences)	2, 26
50	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	No information	7, 26, 28
51	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Financial Institution	No information	4, 8, 36
52	**Belgium**	Misuse of Client Account	Transferring funds without providing legal services	Tax Evasion	Company, Financial Institution	No information	29, 36

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
53	**Belgium**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Company, Financial Institution	Investigation commenced	2, 29, 36
54	**Canada**	Misuse of Client Account	Transferring funds without providing legal services	Illicit Drug Trafficking	Financial Institution	No information	2, 4, 26, 36
55	**South Africa**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	No information	3, 4, 36
56	**United Kingdom**	Misuse of Client Account	Transferring funds without providing legal services	Tax Fraud	Unspecified	Criminal conviction	3, 36
57	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Sale of Stolen Goods	Unspecified	Criminal conviction, new trial granted on appeal which is currently being appealed	3, 36
58	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Company, Financial Institution	Criminal conviction	36
59	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	Criminal conviction	29, 36
60	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking	Company	Criminal conviction	3, 4, 26
61	**United States**	Misuse of Client Account	Structuring payments	Fraud	Financial Institution, Real Estate	Criminal conviction	4, 26
62	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking (Undercover Operation)	Real Estate (Undercover Operation)	Criminal conviction	2, 3, 26, 28
63	**United Kingdom**	Misuse of Client Account	Aborted transactions	Fraud (?)	Real Estate	Removed from practice	26, 34, 36
64	**FATF**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Company, Financial Institution, Real Estate, Trust	No information	4, 26, 28, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
65	**Belgium**	Purchase of Real Property	Investment of proceeds of crime in property	Unspecified	Financial Institution, Real Estate	No information	4, 5
66	**Belgium**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4
67	**Canada**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Real Estate	No information	4, 26
68	**Canada**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	No information	2, 4, 7, 26
69	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	Criminal conviction	2, 4
70	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	Legal professional acted as prosecution witness	4
71	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Fraud	Real Estate	One legal professional removed from practice and two received disciplinary sanctions	2, 3, 26, 36
72	**France**	Purchase of Real Property	Obscuring ownership - purchasing through intermediaries	Illicit Drug Trafficking	Financial Institution, Real Estate	Criminal conviction	2, 4, 7
73	**United States**	Purchase of Real Property	Obscuring ownership - purchasing through intermediaries	Illicit Drug Trafficking	Real Estate	Criminal conviction	2, 4
74	**FATF**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Embezzlement	Company, Financial Institution, Real Estate	No information	28, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
75	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4, 29
76	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	Investigation commenced	2, 4, 28, 29
77	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Company, Financial Institution, Real Estate	Investigation commenced	28, 29
78	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Organised Crime	Company, Financial Institution, Real Estate	No information	4, 28, 29
79	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Organised crime	Company, Financial Institution, Real Estate	No information	17, 26, 37
80	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 5, 26
81	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4, 26
82	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	No information	2, 3, 26, 36

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
83	**Spain**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Company, Financial Institution, Real Estate	No information	2, 8, 20, 26, 37
84	**Switzerland**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Corruption (?)	Company ["yet to be established"], Financial Institution, Real Estate	No information	2, 4, 26
85	**United Kingdom**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Real Estate	Decision not to prosecute legal practitioner	26
86	**United Kingdom**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Housing illegal immigrants	Company, Real Estate	Criminal conviction	29
87	**France**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud	Financial Institution, Real Estate	Prosecution commenced	3, 8, 26
88	**United Kingdom**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud, Organised Crime	Real Estate	Criminal conviction	2
89	**United Kingdom**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud	Real Estate	Disciplinary sanction imposed	2, 26, 35
90	**FATF**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	Decision not to prosecute legal practitioner	2, 29, 36
91	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Tax Fraud (?)	Company, Financial Institution	Investigation commenced	17, 28, 29, 30
92	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Organised Crime	Company	Investigation commenced	29, 30

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
93	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	26, 30
94	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	No information	2, 29, 30
95	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	No information	4, 24
96	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company	No information	2, 30
97	**Spain**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	3, 19, 27
98	**Spain**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	18, 29, 30
99	**Netherlands**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud	Company, Financial Institution	No information	2, 4, 26, 29
100	**Netherlands**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud	Company	No information	24, 28
101	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud, Tax Fraud	Company, Financial Institution	Criminal conviction	2, 4, 29, 36
102	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 3, 8

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
103	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption, Fraud	Company, Financial Institution, Real Estate	Criminal conviction (currently under appeal)	2, 3, 4, 8
104	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	Prosecution commenced	2, 7, 29, 36
105	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking (Undercover Operation)	Company, Financial Institution	Criminal conviction	27, 29, 36
106	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption	Company	Criminal conviction	2, 4, 26
107	**Austria**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Fraud, Breach of Trust	Company, Financial Institution	Criminal conviction	7, 26, 29
108	**Canada**	Management of Companies and Trusts	Management of a company or trust - creation of legitimacy and provision of legal services	Smuggling	Company, Financial Institution	No information	2, 4, 24, 30, 36
109	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Organised Crime	Financial Institution	No information	27
110	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company / Trust, Financial Institution	No information	2, 8, 27
111	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Fraud	Company, Financial Institution	No information	2, 27, 29
112	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Opening bank accounts on behalf of clients	Fraud	Company, Financial Institution	Criminal conviction	26, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
113	**United States**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Unspecified	Company, Financial Institution	Criminal conviction	7, 26, 27, 30
114	**Australia**	Managing Client Affairs and Making Introductions	Management of client's general affairs through client account	Unspecified	Financial Institution, Insurance	No information	5, 26, 36
115	**Belgium**	Managing Client Affairs and Making Introductions	Management of client's general affairs through client account	Illicit Drug Trafficking, Organised Crime	Company, Financial Institution	No information	5, 14, 21, 40
116	**Canada**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Company, Financial Institution	No information	4, 24, 30, 36
117	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Fraud	Company, Financial Institution	Removed from practice	2, 26, 27, 36
118	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 5, 36
119	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 26, 36
120	**Netherlands**	Use of Specialised Legal Skills		Illicit Drug Trafficking	Financial Institution	Legal professional arrested	2, 7, 39
121	**Trinidad & Tobago**	Use of Specialised Legal Skills, Misuse of Client Account		Fraud	Company, Financial Institution	Prosecution commenced	7, 27, 30
122	**United Kingdom**	Use of Specialised Legal Skills		Fraud	(Art)	Criminal conviction	2, 4, 36
123	**United States**	Use of Specialised Legal Skills		Illicit Drug Trafficking	Company, Financial Institution	Criminal conviction	2, 4, 26, 27

ANNEX 6
ADDITIONAL CASE STUDIES

METHOD: MISUSE OF CLIENT ACCOUNT

TECHNIQUE: TRANSFERRING FUNDS WITHOUT PROVIDING LEGAL SERVICES

Case 50: **Legal professional acts as cash courier and makes international transfers without underlying legal transaction – common law country**

An Australian-based solicitor structured funds to an offshore account in Hong Kong. At times it was believed he actually carried cash to Hong Kong. His colleague, a Hong Kong-based solicitor, arranged for the creation of offshore companies in the British Virgin Islands and bank accounts in Hong Kong to receive structured funds from Australia. These funds were then transferred to other countries by the Hong Kong-based solicitor to hide from authorities or returned to Australia in order to appear legitimate.

Source: Australia (2012) questionnaire response

Case 50 **Red flag indicators:**	• Creation of complicated ownership structures without legitimate or economic reason • U-turn transactions • Use of multiple foreign accounts without good reason

Case 51: **Legal professional participates in u-turn payments to cover up fraud – common law country**

A person in control of a corporation's financial affairs abused this position of trust by defrauding the company. The person authorised and instructed staff to make electronic funds transfers from the company to his bookmakers' accounts. He then instructed the bookmakers to direct excess funds and winnings from their accounts to his account or third party accounts, and instructed bank officers to transfer funds from his accounts internationally.

In order to layer and disguise the fraud, he instructed his lawyer to contact the beneficiary of the original international transfers to return the payments via wire transfers into the lawyer's trust account. Approximately AUD 450 000 was returned in one international transfer to the lawyer's trust account. The lawyer then transferred AUD 350 000 to a church fund in an attempt to further hide the assets. To access these funds the person made structured withdrawals of AUD 9 000 each within a nine day period.

The suspect was charged with fraud-related offences for stealing more than AUD 22 million from the

company. He was sentenced to 14 years imprisonment, with a nine-and-a-half-year non-parole period.

Source: Australia (2012) questionnaire response

Case 51 **Red flag indicators:**	• Use of corporate funds for private expenditure • Use of the client account without an underlying transaction • Structuring of payments

Case 52: **Legal professional processes transfers between companies through client account without provision of legal services – civil law jurisdiction**

A bank disclosed suspicious international transfers to the Belgian FIU. Substantial sums from investment companies from Country A were credited on the third party account of a Belgian law firm to the benefit of the Belgian company X. The third party account was subsequently debited by means of money transfers to a company established in Country B. The total sum of these transactions amounted to several million euros.

The FIU's analysis revealed that the third party account clearly served as a transit account to make the construction less transparent. There was no justification to pass these funds through this third party account given that the Belgian company X already owned several accounts with Belgian banks. Furthermore, the majority of the managing directors of company X resided in Asia and were in no way connected to Belgium, whereas the shares of the company were owned by the investment company in Country A. Company X acted as a front company to cover up the relation between the origin and the destination of the funds.

Tax intelligence obtained by the FIU showed that, because of the intervention of company X, the investment companies from Country A (the clients of the international transfers) could relieve the tax burden for important investments in Country B.

Source: Belgium (2012) questionnaire response

Case 52 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason • Use of the client account without an underlying transaction

Case 53: **Legal professional transfers the proceeds of a fraud through client account and attempts to purchase foreign currency to further disguise the origin of the funds – civil law country**

An exchange office disclosed the purchase of a considerable amount of GBP by a foreigner for the account of company X established in Belgium. The funds for this purchase had been transferred to the exchange office's account at the request of a lawyer with a Belgian bank account. The Unit questioned the bank where the lawyer/client held his account. This revealed that the funds on the account of the exchange office had been transferred to the lawyer's account in order of company Y established abroad. The funds that had been transferred by company Y were used to issue a cheque

to the order of company X.

The Unit was informed by the bank that the transfer order was false. Based on this information the bank countermanded the cheque issued by the lawyer, and further investigation by the Unit showed that company X was managed by a foreign national who had performed the exchange transaction. This transaction for company X's account did not have any known economic justification. Information by the tax administration indicated the company had not made its tax returns for quite some time.

Police intelligence revealed that company X, its managing director and its lawyer were on record for fraud. Part of the proceeds of this fraud was used to finance the purchase of GBP by a foreign national on behalf of company X. The Unit reported this file for financial fraud related money laundering.

Source: Belgium (2012) questionnaire response

Case 53 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason • Use of the client account with no underlying transaction • Use of false documents • The client is known to have convictions for acquisitive crime

Case 54: **Legal professional accepts transfers into client account and acts as cash courier – common law country**

An Ontario-based drug trafficker admitted to police that he purposely used legal trust accounts to help block access to information about the true ownership of the funds in the account. He confessed that he would provide cash to his lawyer, who would then deposit the funds into the law firm's trust account. Every few days, the lawyer would withdraw the money from the trust account and deposit the funds into the various bank accounts controlled by the drug trafficker. This was often done by issuing cheques against the trust account, which would be payable to a company associated with the trafficker. Most cheques were in the amount of CAD 2 000 to avoid suspicion.

The small deposits and withdrawals, combined with the use of cheques issued from his lawyer's trust account, helped to circumvent cash or suspicious transaction declarations at financial institutions.

Source: Schneider, S. (2004)

Case 54 **Red flag indicators:**	• Cash payments not consistent with the client's known legitimate income • Use of the client account with no underlying transaction • Structuring of payments • The client is known to have convictions for acquisitive crime or to be currently under investigation for acquisitive crime

Case 55: **Legal professional uses client account as a banking facility for clients and applies their funds to his personal credit card – common law country**

The South African FIU received several STRs about an attorney who appeared to be abusing his attorney trust facility. The suspicious transactions in the reports pointed out the following:

i) Multiple large sums of money were being deposited into the trust account by different people and companies over a period exceeding two years

ii) These funds were used to make payments to other depositors in South Africa and abroad

iii) Funds from this account were being remitted to foreign countries deemed to be tax havens

iv) Money was transferred to the attorney's personal credit card; his practice expenses were also paid directly from the trust account.

Source: Deloitte (2011)

Case 55 **Red flag indicators:**	• Use of the client account without an underlying transaction • Payment of funds to a high risk country • Possibly disproportionate private funding and/or payments from third parties

Case 56: **Legal professional convicted after transferring funds to a criminal client's mistress – common law country**

In 2008, Mr Krestin, a solicitor was convicted of entering into an arrangement to facilitate money laundering after making a payment of EUR 14 000 euro to his client's mistress. There was no underlying transaction supporting the payment. The solicitor had received a production order relating to the client which outlined allegations of Tax (MTIC) fraud against the client. The first jury had not been able to reach a verdict, and the judge concluded that the second jury must have convicted the solicitor on the basis that he suspected that the funds were the proceeds of crime, rather than that he knew they were. The solicitor was fined GBP 5 000. When his conduct was considered by the Solicitors Disciplinary Tribunal, in light of the sentencing judge's comments he was reprimanded, but allowed to keep practicing as a lawyer, subject to restrictions.

Source: United Kingdom (2012) questionnaire response

Case 56 **Red flag indicators:**	• No underlying transaction for use of the client account • The is known to be currently under investigation of acquisitive crime

Case 57: **Legal professional disperses funds to criminal client's family members and keeps fee – common law country**

Attorney Jamie Harmon accepted the proceeds of the sale of stolen goods from her client, Christian Pantages. Harmon deposited the funds into her attorney trust account and then dispersed the funds

to Pantages and his wife, keeping a fee for herself.

Pantages pleaded guilty to all counts against him and testified against Harmon at trial. Following a guilty verdict on five counts of money laundering, the district court granted Harmon a new trial based on an improper jury instruction. In so doing, the judge expressed concern regarding the difficulties defence counsel face when accepting fees from clients that may be criminal proceeds.

See 2011 WL 7937876, at *5 n.12 (N.D. Cal. Aug. 18, 2011) (denying motion for judgment of acquittal but granting motion for a new trial based on improper jury instruction). The government's appeal of the grant of a new trial is pending.

Source: United States (2012) questionnaire response – United States v Harmon, No. 08-cr-938 (ND Cal)

Case 57 **Red flag indicators:**	• Use of client account without an underlying transaction

Case 58: **Legal professional convicted for creating secret client accounts to transfer the proceeds of fraud – common law country**

Attorney Jonathan Bristol pleaded guilty to conspiracy to commit money laundering for his role in laundering more than $18m in fraud proceeds through two attorney escrow accounts on behalf of Kenneth Starr and his fraudulent investment enterprises. At the time, Bristol was an attorney at a large, international law firm in New York.

Bristol created two attorney escrow accounts, without informing his law firm, into which Starr's investment advisory clients deposited their investment funds. Bristol then transferred the funds to Starr, members of his family, and his entities. Bristol also used the clandestine attorney escrow accounts to pay his law firm on behalf of Starr.

Bristol is currently awaiting sentencing. Following disciplinary action, the Court accepted his resignation for reasons of judicial economy and ordered Bristol's name be immediately struck from the roll of attorneys.

Source: United States (2012) questionnaire response United States v. Bristol, No. 10-cr-1239 (S.D.N.Y.)

Case 58 **Red flag indicators:**	• Use of client account without an underlying transaction • Payment of funds intended for corporate purposes to private accounts • Payments to third parties with no legitimate explanation

Case 59: **Legal professional creates complicated foreign structures and transfers funds through client account while claiming privilege would prevent discovery – common law country**

Attorney David Foster was indicted on charges of money laundering and ultimately pleaded guilty to one count of causing a financial institution to fail to file a currency transaction report. Foster assured undercover agents that their money laundering transactions through his client trust account would be protected by attorney-client privilege. After the funds were deposited in the trust

account, he transferred the money to a corporation and bank accounts in Liechtenstein that he had established. See 868 F. Supp. 213 (E.D. Mich. 1994) (holding that Foster's sentence calculation should be increased because of an enhancement for use of "special skills").

Source: United States (2012) questionnaire response United States v Foster No 93-cr-80141 (Ed Mich)

Case 59 **Red flag indicators:**	• Use of client account without an underlying transaction • Involvement of structures and countries where there is no legitimate reason

TECHNIQUE: STRUCTURING PAYMENTS

Case 60: **Legal professional creates companies, false legal documentation and advises on structuring payments to avoid reporting requirements – common law country**

Attorney George Rorrer was convicted by a jury of conspiracy to commit money laundering. Rorrer helped to invest the drug proceeds of client John Caporale by forming a corporation in the name of the client's wife and arranging a loan from the corporation to another (non-criminal) client, Robin Hawkins. Rorrer then drafted a phony construction-work contract, making the repayment of the loan appear to be payment for construction work performed by the Caporales. Rorrer instructed Hawkins to give the construction receipts to the Caporales to legitimise the payment.

Rorrer also drew up a promissory note, which the wife signed, but did not provide copies of the note to either party. Rorrer advised Hawkins how to deposit the cash loan without triggering reporting requirements. The appeals court upheld Rorrer's conviction but remanded him for resentencing after finding that the district court abused its discretion by not applying a sentencing enhancement based on Rorrer's use of "special skills" (legal skills) in committing the offenses of conviction. See United States v. Robertson, 67 F. App'x 257 (6th Cir. 2003).

Source: United States (2012) questionnaire response United States v. Rorrer, No. 99-cr-139(7) (W.D. Ky.)

Case 60 **Red flag indicators:**	• Significant private funding and the transfers are structured so as to avoid the threshold requirements • The ties between the parties are of a family, employment, corporate or other nature such as to generate doubts as to the real nature or reason for the transaction • Structuring of payments

Case 61: **Legal professional structures payments for property to avoid threshold reporting requirements – common law country**

Attorney Michael Sinko was convicted of conspiracy to commit money laundering and aiding and abetting money laundering. Sinko owned a condominium project that was financed by NOVA Bank, of which Sinko was the outside counsel. John Palmer, who had fraudulently obtained funds from his employer, wished to launder money by buying a condominium from Sinko. Sinko structured the purchase agreement in a way that avoided disclosure of cash payments. See 394 F. App'x 843 (3d

Cir. 2010) (affirming sentence).

Source: United States (2012) questionnaire response United States v. Sinko, No. 07-cr-703 (E.D. Pa.)

Case 61 **Red flag indicators:**	• Structuring of payments • Significant private funding / cash payments disproportionate to known legitimate income

Case 62: **Legal professional structures payments on property purchase and creates false documentation to launder proceeds of crime – common law country**

Defence attorney Victor Arditti advised an undercover agent posing as a cocaine dealer on how to structure cash in order to purchase real estate. Later, Arditti told the agent he would draft documents memorialising a sham loan to legitimise cash drug proceeds and then establish an escrow account to receive the proceeds and then invest it in an Oklahoma oil deal. When the escrow account idea failed to work, Arditti set up a trust account to funnel the drug proceeds to the oil deal, keeping the undercover agent's alias off all bank records.

No trust agreement was prepared, and Arditti had sole signature authority on the account. Subsequent deposits were made to the trust account using cashier's cheques from a Mexican money exchanger. A grand jury indicted Arditti on charges of conspiracy to launder money and to avoid currency reporting requirements. A jury found Arditti guilty on all counts, and the district court denied judgment of acquittal.

Source: United States (2012) questionnaire response United States v. Arditti, 955 F.2d 331 (5th Cir.), cert. denied, 506 U.S. 998 (1992)

Case 62 **Red flag indicators:**	• Structuring of payments • Client with purported convictions for acquisitive crime • Use of complicated structures for no legitimate reasons • Funds received from high risk countries

TECHNIQUE: ABORTED TRANSACTIONS

Case 63: **Legal professional facilitates laundering of the proceeds of mortgage fraud following aborted property transactions – common law country**

In 2010 a solicitor was stuck off after having allowed a large property company to use the client account as a banking facility, when the transactions were suddenly aborted They had also dissipated the funds received from a number of properties, rather than paying out the mortgage on the property.

Source: United Kingdom (2012) questionnaire response

Case 63 **Red flag indicators:**	• Large payments to the client account without an underlying legal transaction • Transaction unexpectedly aborted after funds had been received

	• Transaction were large for the particular practice

METHOD: PURCHASE OF REAL PROPERTY

TECHNIQUE: INVESTMENT OF PROCEEDS OF CRIME IN PROPERTY

Case 64: **Legal professional creates complex structures to purchase property with drug proceeds - common law country**

Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and bank drafts on behalf of a drug trafficking syndicate who were importing 24kg of heroin into Country Z. Bank drafts purchased from different financial institutions in country Y (the drug source country) were then used to purchase real estate in Country Z. A firm of solicitors was also used by the syndicate to purchase the property using the bank drafts that had been purchased overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors.

Source: FATF (2004)

Case 64 **Red flag indicators:**	• Possible structuring of payments • Significant funding disproportionate to the known legitimate income of the client • Involvement of structures and accounts in multiple countries with no legitimate reasons • Use of complicated ownership structures for no legitimate reason

Case 65: **Legal professional instructed in property purchase by a foreign national with multiple third parties contributing to funding – civil law country**

A bank's suspicions were raised after a bank cheque was issued to the order of a notary upon request of an Asian national for purchasing real estate. Analysis of the account transactions showed that the account received several transfers from Asians residing abroad and was known through an investigation regarding a network of Asian immigrants. The analysis showed that the account had been used as a transit account by other Asian nationals for the purchase of real estate.

Source: FATF (2007)

Case 65 **Red flag indicators:**	• Third party funding with no legitimate explanation • Significant levels of private funding which may have been disproportionate to the socio-economic profile of the client

Case 66: **Legal professional makes STR after client attempts to purchase property with cash – civil law country**

A notary did a notification to the FIU on a company, represented by the Managing Director, who had

purchased a property in Belgium. The notary got suspicious when the buyer wished to pay the total price in cash. When the notary refused the Managing Director asked where the nearest bank Agency was. He came back to the Office of the notary with a cheque from the bank after he had run a deposit in cash. The suspicions of the notary were further enhanced when the company which he represented was the subject of a criminal investigation. Research by the FIU revealed that the person was already the subject of a dossier that was been sent by the FIU in connection with illicit drug trafficking. After the notification from the FIU a law enforcement investigation commenced.

Source: Cellule de traitement des information Financieres (2006)

Case 66 **Red flag indicators:**	• Significant amounts of cash not consistent with known legitimate income • The client is currently under investigation for acquisitive crimes

Case 67: **Legal professional acts as a depository institution and then purchases property for client with no known legitimate income – common law country**

A BC man used the proceeds from the sale of cocaine, marijuana and steroids to purchase several homes throughout British Columbia. The trafficker would regularly provide cash to his lawyer who would deposit the funds into his law firm's bank account in amounts averaging CAD 4 000 to CAD 5 000. When the balance of the amount reached a certain level the funds would be applied to the purchase of property (mostly homes used as marijuana grow-ups).

Source: Schneider, S. (2004)

Case 67 **Red flag indicators:**	• Significant private funding and cash not consistent with known legitimate income • Structuring of payments • Transactions not consistent with legitimate socio-economic profile of the client

Case 68: **Legal professional accepts over 130 transactions in 8 months to purchase property for drug trafficker – common law country**

Between January and August 1994, more than 130 transactions were conducted through a trust account of a law firm that represented a drug trafficker in the purchase of a $650,000 home in Toronto. The accused was convicted of drug trafficking and police were also able to prove that the funds used to purchase the property were derived from his illegal activities. During a two week period preceding his purchase of the real estate, the accused provided the law firm with numerous bank drafts obtained from a number of different financial institutions. The vast majority of these bank drafts were between CAD 3 000 and CAD 5 000 in value. The highest amount was CAD 9 000. Between March 17 and March 25, 1994, 76 bank drafts were deposited on behalf of the accused in the law firm's trust account. On March 17 alone, 18 different bank drafts were deposited into the account. The bank drafts were purchased from eight different deposit institutions.

Source: Schneider, S. (2004)

Case 68 **Red flag indicators:**	• Client known to have convictions for acquisitive crime • Structuring of payments • Significant private funding not consistent with known legitimate income • Use of multiple bank accounts and financial institutions for no legitimate reason

Case 69: **Legal professionals co-opted into laundering activity by his brother – common law country**

In 2009, Mr Farid a solicitor was convicted of failing to make a suspicious transaction report after acting in a number of property transactions on behalf of a drug dealer. Mr Farid was introduced to the client by the Mr Farid's brother and a mortgage broker. The mortgage broker had assisted in identity theft to facilitate fraudulent mortgage applications, with the transactions being processed by the solicitor, after large cash deposits were made. Mr Farid was sentenced to 9 months jail and in 2011 the Solicitors Disciplinary Tribunal ordered that he should not be re-employed within a law firm without permission from the regulator.

Source: United Kingdom (2012) questionnaire response

Case 69 **Red flag indicators:**	• Disproportionate amounts of cash • Use of false identities

Case 70: **Legal professional acts as prosecution witness after wrongly assuming funds were clean because they have come from a bank account – common law country**

In 2008/09 an international drug trafficker laundered over GBP 300 000 through bank accounts. This was then paid from the bank via cheque to a solicitor who acted as legal professional in a house purchase, where the house was bought for approximately GBP 450 000 with no mortgage. The solicitor had assumed because the money was transferred from a bank account, the funds had already been checked. The solicitor was not charged and acted as a witness for the police.

Source: United Kingdom (2012) questionnaire response

Case 70 **Red flag indicators:**	• Disproportionate level of private funding not consistent with the known legitimate income

Case 71: **Three legal professionals engage in money laundering through a property transaction for convicted fraudster husband of senior partner – common law jurisdiction**

In March 2006, a law firm acted for a small company in the purchase of a property for GBP 123 000. The director of the company was Mr A, the husband of one of the solicitors and a convicted fraudster. In September 2006, the law firm acted for Mr A who purchased the same property from the company for GBP 195 000. In February 2007, the firm then acted for Mr A's step son who

purchased the same property for GBP 230 000. In December 2006, the small company provided the firm with a payment of GBP 25 000 and GBP 20 000. The amount of GBP 25 000 was noted as covering a shortfall for the property, but there was no shortfall. The amount of £20,000 was said to be a loan to another client, but there were not documents to support the loan. The Solicitors Disciplinary Tribunal considered the conduct of three solicitors in relation to the matter. One was struck off, one was given an indefinite suspension from practice and the other was fined GBP 10 000.

Source: United Kingdom (2012) questionnaire response

Case 71 **Red flag indicators:**	• Director of client was known to have criminal convictions • Rapidly increasing value on the property that was not consistent with the market • Connection between the parties giving rise to questions about the underlying nature of the transaction • Use of client account without underlying transaction

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASING THROUGH INTERMEDIARIES

Case 72: **Legal professional turns a blind eye to false documents when helping partner of drug trafficker buy property with criminal proceeds – civil law country**

In 1995 a notary was found guilty of money laundering as he helped the sexual partner of a drug trafficker, who had been arrested to buy a property and advise her to pay the price with international wire transfers. The court decided that the notary could not have been ignorant of the fact that some documents had been falsified.

Source: Chevrier, E. (2005)

Case 72 **Red flag indicators:**	• Use of false documents • Client known to have close connections with a person under investigation for acquisitive crimes • Use of foreign accounts with no legitimate reason • Significant private funding possibly not consistent with known legitimate income

Case 73: **Legal professional convicted for creating property portfolio for drug trafficking friend – common law country**

Attorney James Nesser was convicted of conspiracy to distribute drugs, conspiracy to launder money, money laundering, and engaging in illegal monetary transactions. Nesser handled property transactions for a client and sometimes social acquaintance Ronald Whethers. Nesser laundered Whethers' drug proceeds through the purchase of a farm, the sham sale of a house, and the masked purchase of another real property. Nesser's conviction on drug conspiracy charges was upheld because the laundering promoted the drug conspiracy and prevented its discovery by concealing the

origin of the proceeds. See 939 F. Supp. 417 (W.D. Penn. 1996) (affirming conviction).

Source: United States (2012) questionnaire response - United States v. Nesser, No. 95-cr-36 (W.D. Penn.)

Case 73 **Red flag indicators:**	• Client known to be involved in criminal activity • There are attempts to disguise the real owner or parties to a transaction • Significant private funding not consistent with known legitimate income

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH A COMPANY OR TRUST

Case 74: **Legal professional assists in creating property investment countries to hide millions derived from fraud**

A director of several industrial companies embezzled several million dollars using the bank accounts of offshore companies. Part of the embezzled funds were then invested in Country Y by means of non-trading real estate investment companies managed by associates of the person who committed the principal offence. The investigations conducted in Country Y, following a report from the FIU established that the creation and implementation of this money laundering channel had been facilitated by accounting and legal professionals – gatekeepers. The gatekeepers had helped organise a number of loans and helped set up the different legal arrangements made, in particular by creating the non-trading real estate investment companies used to purchase the real estate. The professionals also took part in managing the structures set up in Country Y.

Source: FATF (2004)

Case 74 **Red flag indicators:**	• Creation of complicated ownership structures with no legitimate reason • Involvement of structures with multiple countries with no legitimate reason

Case 75: **Legal professionals help obscure beneficial ownership through complicated international corporate structures – civil law country**

A notary disclosed a real estate purchase by the company RICH, established in an off-shore centre. For this purchase the company was represented by a Belgian lawyer. The payment for the property took place in two stages. Prior to drafting the deed a substantial advance was paid in cash. The balance was paid by means of an international transfer on the notary‘s account.

Analysis revealed the following.

The balance was paid on the notary‘s account with an international transfer from an account opened in name of a lawyer‘s office established in Asia. The principal of this transfer was not the company RICH but a Mr. Wall. Ms. Wall, ex-wife of Mr.Wall resided at the address of the property in question. Police sources revealed that Mr. Wall was known for fraud abroad.

These elements seemed to indicate that Mr. Wall wanted to remain in the background of the

transaction. That is why he used an off-shore company, represented by a lawyer in Belgium and channelled the money through a lawyer's office abroad to launder money from fraud by investing in real estate.

Source: Deloitte (2011)

Case 75 **Red flag indicators:**	• Use of multiple countries, including higher risk countries, without legitimate reason • There are attempts to disguise the real owner or parties to the transaction • Significant amounts of cash and private funding possibly not consistent with the known legitimate income of the client

Case 76: **Legal professional involved in unusual transfers of property without apparent economic or other legitimate justification – civil law country**

A bank reported a person whose account has remained inactive for a long time, but who suddenly was filled with several deposits in cash and international transfers. These funds were then used for the issuance of a cheque to order of a notary for the purchase of a property. Research by the FIU revealed that the ultimate purchaser of the property not was the person involved, but an offshore company. The person concerned had first bought the property in his own name and then left to the listed company by a command statement for the notary. Examination of the dossier revealed that the person who was connected to a bankrupt company, acted as hand to buy property with disadvantage of his creditors. The person concerned also practiced no known professional activity and received state benefits. On these grounds and police intelligence the FIU reported the dossier for money laundering in connection with fraudulent bankruptcy. A judicial inquiry is currently underway.

Source: Cellule de traitement des information Financieres (2006)

Case 76 **Red flag indicators:**	• Involvement of a complicated ownership structure without legitimate reason • Funding not consistent with known legitimate income • There are attempts to disguise the real owner or parties to the transaction • Involvement of foreign countries with no legitimate reason

Case 77: **Legal professional involved in creating complex foreign corporate structure to purchase properties to facilitate laundering – civil law country**

The bank account of a person was credited by substantial transfers from abroad. These funds were used as banking cheques to order of a notary to purchase real estate. The investigation of the FIU revealed that the person had set up a highly complex corporate structure for this investment. Interrogation of the notary and the Constitutive Act of the companies showed that the two holdings companies in Belgium were founded at this notary in Belgium by four foreign companies. Then

those two companies founded two other companies in the real estate sector. Then the intermediary of these two last companies made investments in real estate. This dossier is currently subject of a judicial inquiry.

Source: Cellule de traitement des information Financieres (2006)

Case 77 **Red flag indicators:**	• Use of a complicated ownership structure without legitimate reason • Involvement of multiple countries without legitimate reason

Case 78: **Legal professionals makes STR after unusually high money transfers received from foreign country with no connection to the parties or the transaction – civil law country**

A Russian couple, living in Belgium, controlled the company OIL that was located in Singapore and that was active in the oil and gas sector. A company in the British Virgin Islands was the only shareholder of OIL. On their accounts significant transfers were made regarding OIL. The money was then transferred to accounts on their name in Singapore or withdrawn in cash. The use of foreign accounts and the intervention of off shore companies attracted the attention of the banks. In addition, the couple invested several million euros in immovable property in Belgium. The notary found such substantial investments and that they were paid through transfers from Singapore suspicious. Police source revealed that these stakeholders were heads of a Russian crime syndicate. They practiced no commercial activities in Belgium that could justify the transactions on their accounts. The Belgian financial system was apparently only used for the purpose of money laundering.

Source: Cellule de traitement des information Financieres (2009)

Case 78 **Red flag indicators:**	• Involvement of multiple countries without legitimate reason, including high risk countries • Significant private funding not consistent with the company's economic profile • Complicated ownership structure without legitimate reason

Case 79: **Legal professional used in U-turn property transaction designed to legitimise funds from organised crime – civil law country**

An East European was acting under an alias as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients".

The funds were then used to issue a cheque to a notary for the purchase of a property. The attention of the notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross border transaction and wire transfers to launder money that, according to police sources, came

from activities related to organised crime.

It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Source: FATF (2007)

Case 79 **Red flag indicators:**	• Sale of property in a non-arm's length transaction (i.e. a director selling to his company) • Resale back to the original seller at a reduced price • There has been an increase in capital from a foreign country, where there is no clear connection

Case 80: **Legal professional makes STR after unusual third party funding of a property purchase**

The FIU received a suspicious transaction report from notary A on one of his clients, person B, a foreigner without an address in Belgium, who in his office had set up a company for letting real estate. The sole manager and shareholder of this company was a family member of B, who also resided abroad. Shortly after its creation the company bought a property in Belgium. The formal property transfer was carried out at notary A's office. The property was paid for through the account of notary A by means of several transfers, not from company X, but from another foreign company about which individual B did not provide any details. The establishment of a company managed by a family member with the aim of offering real estate for let and paid by a foreign company disguised the link between the origin and the destination of the money. Police intelligence revealed that the individual was known for financial fraud. The investment in the property was apparently financed by the fraud.

Source: FATF (2007)

Case 80 **Red flag indicators:**	• Funds received from third parties, in a foreign country, with no legitimate reason • The client is evasive about the source of funds • The transaction is unusual – there is limited connection between the client and the country in which the transaction takes place and the client does not have ownership or formal control over the entity on whose behalf he is conducting the transaction. • The client has convictions for acquisitive crimes

Case 81: **Legal professional makes STR after unusual cash payments made in relation to a property purchase – civil law country**

The company ANDI, managed by Mr. Oxo, sold a property to the company BARA, managed by Mr. Rya, for a significant amount for which the deposit was paid in cash. A large part of the price was also paid in cash. When the notary who had executed the act noticed these transactions he sent a disclosure to the FIU based on article 10bis of the Law of 11 January 1993.

Analysis revealed the following elements:

• The notary deed showed that money for the cheque to the notary was put on the account of the company ANDI by a cash deposit two days before the cheque was issued.

• Information from the bank showed that the company ANDI and Mr. Oxo's personal account were credited by substantial cash deposits. This money was used for, among other things, reimbursing a mortgage loan, and was withdrawn in cash.

• Police sources revealed that Mr. Oxo and Mr. Rya were the subject of a judicial inquiry into money laundering with regard to trafficking in narcotics. They were suspected of having invested their money for purchasing several properties in Belgium through their companies.

All of these elements showed that the cash used for purchasing property probably originated from trafficking in narcotics for which they were on record.

Source: Deloitte (2011)

Case 81 **Red flag indicators:**	• Significant cash deposits • Sale of property in a non-arm's length transaction • Clients currently under investigation for acquisitive crimes

Case 82: **Legal professional receives multiple deposits from various sources for property transaction – civil law jurisdiction**

A company purchased property by using a notary's client account. Apart from a considerable number of cheques that were regularly cashed or issued, which were at first sight linked to the notary's professional activities, there were also various transfers from the company to his account. By using the company and the notary's client account, money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions. Police sources revealed that the sole shareholder of this company was a known drug trafficker.

Source: FATF (2007)

Case 82 **Red flag indicators:**	• The funding appears unusual in terms of multiple deposits being made towards the property purchase over a period • Use of the client account without an underlying transaction • The company only has one shareholder • A beneficial owner has convictions for acquisitive crime

Case 83: **Legal professional assists PEPs to purchase expensive foreign property though a company with a later transfer to a family member without genuine payment – civil law country**

A company is incorporated with a capital stock of EUR 3 050 by a Spanish lawyer, who then creates a general power of attorney over the company for a relative of the Head of State of an African country. Half the stock in the company is then transferred to another national of the same African country, who claims to be a businessman.

The company purchases of a plot of land within an urban development in Spain on which a detached house has been built. The property is valued at EUR 5 700 000, the price being paid through transfers between accounts at the same Spanish credit institution.

The company transfers the recently purchased property, in the following deed, to the relative of the Head of State, specifying the same price as set for the first purchase, while deferring payment of the entire sum.

Source: Spain (2012) questionnaire response

Case 83 **Red flag indicators:**	• The client and beneficial owner have family and personal ties to an individual who holds a public position in a high risk country. • The company makes a significant purchase which is disproportionate to the initial capital in the company and its economic profile • Company funds are used to make a private purchase • The transaction does not make economic sense in that the company divests itself of its largest asset without making a profit and with payment being deferred, • The transfer of the property is a non-arm's length transaction (i.e. company sells to its director)

Case 84: **Legal professional accepts tens of millions of euros from a PEP as a gift to his children to purchase property despite warnings of the corruption risks – civil law country**

Following the payment of a sum of money to the account of a notary's office, a bank sent a STR to the FIU. The STR referred to the payment of several tens of millions credited to the account of the notary. As the transaction appeared unusual, in particular because of the amount, the financial intermediary requested its client to clarify matters. The notary explained that the payment was a gift from a high-ranking government official or president of a country on the African continent to his children residing in Switzerland. The funds were destined for the purchase, via the intermediary of a public limited company yet to be established, of an apartment in the town in question.

As the funds originated from a politically exposed person (PEP), the degree of corruption in the African country in question was assessed as high and the Swiss Federal Banking Commission (SFBC) had issued warnings regarding this country, the financial intermediary reported the case.

Following investigations carried out by the FIU, it became apparent that the extremely high price of the property in question was in no proportion to the normal price for this type of object. Furthermore, open sources revealed that a third country was already carrying out investigations

into corruption and money laundering by the government official in question and members of his family.

Source: Deloitte (2011)

Case 84 **Red flag indicators:**	• Disproportionate private funding given known legitimate income • There are attempts to disguise the real owner or parties to the transaction • The client holds a public position in a high risk country • There is a remarkable high and significant difference between the purchase price and the known value of properties in the area • The client is currently under investigation for acquisitive crimes

Case 85: **Legal professional unaware that funds used to purchase property through a trust were proceeds of crime – common law country**

Between 2004 and 2008 a legal professional who conducted property transactions, assisted the subject by drafting a Deed of Trust and the purchase of a property. The property was bought at a discounted rate by the client and then transferred to third party. No action was taken against the legal professional as the law enforcement agency was unable to prove that legal professional had known or suspected that they were dealing with the proceeds of crime.

Source: United Kingdom (2012) questionnaire response

Case 85 **Red flag indicators:**	• Unusual transaction involving transfer of property at significant undervalue. • Complex property transactions

Case 86: **Legal professional convicted after transferring hotels at undervalue to offshore company – common law country**

In 2010, Mr Wilcock, a solicitor was convicted of failing to make a suspicious transaction report and fined GBP 2 515. He was acting for a client who ran a chain of properties in Southport, England which housed illegal immigrants. He was asked to transfer the ownership of the hotels to an offshore company at a significant undervalue. It was not clear if Mr Wilcock knew his client was being investigated by police at the time of the transaction, but in pleading guilty he acknowledged that he should have been suspicious as to the source of the funds used to purchase the hotels in the first place.

Source: United Kingdom (2012) questionnaire response

Case 86 **Red flag indicators:**	• Significant undervalue • Involvement of complex ownership in a country with which there was limited connection

TECHNIQUE: MORTGAGE FRAUD WITH ANTECEDENT LAUNDERING

Case 87: **Legal professional investigated for acting in unusual property transactions - including selling maid's rooms for 8 times their original value – civil law country**

Judicial investigations are in progress into the facts surrounding credit frauds to the detriment of a bank: 6 fraudulent real estate files of financing were presented to the agency on the basis of the production of false pay slips and false bank statements, for a loss at first estimated esteemed at EUR 505 000.

The first investigations led by the police confirmed that the loan files were presented to the bank systematically by the same client adviser and systematically by the same real estate agent for six different borrowers. They confirmed also that the loss finally amounted to about EUR 5 million as more loans which had deceitfully been obtained by those 6 borrowers were uncovered.

Searches of the offenders' residences led to the discovery of numerous documents, and a lifestyle out of proportion to their legitimate income.

However, the destination of the lent funds could only be partially determined because 5 of the 6 involved borrowers had acquired real property in Luxembourg.

The investigation also identified the complicity of two agents of the defrauded bank and the assistant director of this bank who indicated they let pass at least 9 files which they knew were based on false documents and that the borrowers were involved in the fraud.

The lent funds stemming from frauds allowed the purchase of properties in France and in Luxembourg. All of the purchases involved a single solicitor and his clerk, who were complicit of the organised fraud.

Searches of the office of the notary revealed approximately sixty notarial acts drafted on the basis of falsified documents. The notary recognized that he had failed to make in-depth searches on the buyers. He explained that some requests of his customers were not clear, in particular when he was reselling four maid's rooms in Paris of less than 10 m^2 for EUR 250 000 each while they had been initially bought for EUR 30 000 euro each..

He admitted making two transfers on bank accounts in Luxembourg belonging to two of presumed fraudsters by knowing perfectly that these are French resident and are not supposed to hold of bank accounts in Luxembourg.

He finally confirmed having realised all the notarial acts by having knowledge that the properties were bought on the basis of loans obtained thanks to forgery documents and internal complicities of the bank.

Without the intervention of this notary, this vast swindle would not have been so extensive

The notary is at present being prosecuted for complicity of money laundering and complicity of organised fraud.

Source: France (2012) questionnaire response

Case 87 **Red flag indicators:**	• Use of false documents • There are multiple appearances of the same parties in transactions over a short period of time • There are remarkable and highly significant differences between he

	declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional • The client holds bank accounts in a foreign country when this is prohibited by law

Case 88: **Legal professional provides a wide range of legal services to three organised crime groups – common law country**

In 2008, Ms Shah a legal executive working within a law firm provided services to three separate Organised Crime Groups (OCGs) by:

facilitating false immigration applications using false or improperly obtained identity documents

securing criminal assets by creating and falsely dating a Deed of Trust on behalf of a subject (who had been sentenced to 14 years imprisonment for drug trafficking) to hide assets from confiscation proceedings

facilitating mortgage fraud and the subsequent disbursement of funds to multiple individuals and companies on behalf of the OCG.

Within a short timeframe, approximately GBP 1 million was paid into the client account from five different mortgage companies, which was then paid out to numerous third parties.

In 2011 Ms Shah was sentenced to five years imprisonment (four years for six counts of fraud and 11 counts of money laundering in relation to the mortgage frauds and subsequent disbursements of funds; and one year for one count of perverting the course of justice in relation to immigration applications).

Source: United Kingdom (2012) questionnaire response

Case 88 **Red flag indicators:**	• Client seeks false or counterfeited documentation • Client is known to have convictions for acquisitive crime

Case 89: **Legal professional facilitates significant property fraud and laundering of the proceeds by ignoring multiple warning signs of fraud and money laundering – common law country**

Between 2009 and 2010 a solicitor acted for sellers in the purchase of a number of properties. Sellers were all introduced to solicitor by a company – these people where engaging in fraud by attempting to sell properties they did not own. Some purchases aborted and funds where then sent to third parties, in other cases the purchaser changed part way through the transaction and the purchase price reduced for no reason. The solicitor did not meet the clients and the dates of birth on the due diligence material provided showed that the person could not have been the same person who owned the property (i.e. they would have been too young to have legally purchased the property). The solicitor received a fine of GBP 5 000 from the Solicitors Disciplinary Tribunal, who noted the fact that solicitor was seriously ill at the time of his failings and did not make a finding of dishonesty.

Source: United Kingdom (2012) questionnaire response

Case 89 **Red flag indicators:**	• Changes in instructions • False identification documents • Unusual reductions in the purchase price.

METHOD: CREATION OF COMPANIES AND TRUSTS

TECHNIQUE: CREATION OF SHELL COMPANIES TO PLACE OR LAYER

Case 90: **Legal professional creates complex multijurisdictional corporate structures to launder funds**

Mr S headed an organisation importing narcotics into country A, from country B. A lawyer was employed by Mr S to launder the proceeds of this operation.

To launder the proceeds of the narcotics importing operation, the lawyer established a web of offshore corporate entities. These entities were incorporated in Country C, where scrutiny of ownership, records and finances was not strong. A local management company in Country D administered these companies. These entities were used to camouflage movement of illicit funds, acquisition of assets and financing criminal activities. Mr S was the holder of 100% of the bearer share capital of these offshore entities. Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Country A.

When they were approached by law enforcement during the investigation, many of these lawyers cited privilege in their refusal to cooperate. Concurrently, the lawyer established a separate similar network (which included other lawyers' trust accounts) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity. The lawyer has not been convicted of any crime in Country A.

Source: FATF (2007)

Case 90 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Use of a complicated ownership structure and multiple countries, including high risk countries, without legitimate reasons • There is only one shareholder of a company • Use of the client account without an underlying transaction

Case 91: **Legal professional creates, dissolves and re-creates corporate entities to assist in laundering the proceeds of large-scale tax evasion – civil law country**

The FIU received a disclosure from a bank on one of its clients, an investment company. This company was initially established in an offshore centre and had moved its registered office to become a limited company under Belgian law. It had consulted a lawyer for this transition.

Shortly afterwards the company was dissolved and several other companies were established taking

over the first company's activities. The whole operation was executed with the assistance of accounting and tax advisors.

The first investment company had opened an account in Belgium that received an important flow of funds from foreign companies. The funds were later transferred to accounts opened with the same bank for new companies. These accounts also directly received funds from the same foreign companies. Part of it was invested on a long-term basis and the remainder was transferred to various individuals abroad, including the former shareholders of the investment company.

The FIU's analysis revealed that the investment company's account and those of its various spin-offs, were used as transit accounts for considerable transfers abroad. The transformation of the investment company into a limited company under Belgian law, shortly followed by the split into several new companies, obscured the financial construction.

The scale of the suspicious transactions, the international character of the construction only partly situated in Belgium, the use of company structures from offshore centres, consulting judicial, financial and fiscal experts, and the fact that there was no economic justification for the transactions all pointed to money laundering related to serious and organised tax fraud, using complex mechanisms or procedures with an international dimension.

Additionally, the managing directors of the investment company had featured in another file that the FIU had forwarded on serious and organised tax fraud. The FIU forwarded this file for money laundering related to serious and organised tax fraud using complex mechanisms or procedures with an international dimension.

Source: Belgium (2012) questionnaire response

Case 91 **Red flag indicators:**	• Creation of complicated ownership structures where there is no legitimate or economic reason, including in high risk countries. • Incorporation and/or purchase of stock or securities of several companies within a short period of time with elements in common and with no logical explanation • There is an increase in capital from foreign countries with limited information as to the connection or basis for the payments.

Case 92: **Legal professional establishes 20 companies for one client on the same day – which are then used to launder the proceeds of organised crime – civil law country**

In a dossier on organised crime, the person concerned was a company director of some twenty companies. Ten of these companies had gone bankrupt. These companies were founded by the same notary. Several suspicious elements led to a notification to the FIU: all companies were founded on the same day, by the same persons and with a very broad social purpose. In addition, these companies had the same address but their company directors live in different countries. This dossier is subject of a judicial inquiry

Source: Cellule de traitement des informations financières (2006)

Case 92 **Red flag indicators:**	• Incorporations of multiple companies in a short period of time with elements in common with no logical explanation • Involvement of individuals from multiple countries as directors of a

	company, without legitimate reason

Case 93: **Legal professionals set up companies which promptly recycled the start up capital to establish new companies to help obscure ownership and layer criminal funds – civil law country**

Several notaries were involved in the setting up of a large number of companies over a number of years. Only the legal minimum of capital was paid up, it was then almost entirely withdrawn in cash and used again to establish new companies. The seat of some companies was also located at the address of an accounting firm and they were led by front men. Several cases showed that the head of the accounting firm himself had raised money for the capital. The established companies were then sold to third parties and used in the context of illegal activities.

Source: Cellule de traitement des informations financières (2009)

Case 93 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation • The transaction is unusual in that a company divests itself almost entirely of capital in order to set up other companies.

Case 94: **Junior legal professional involves law firm in laundering proceeds of drug crime – common law country**

A junior lawyer with a Calgary law firm incorporated numerous shell companies in Canada and off-shore on behalf of a client who was involved in a large scale drug importation conspiracy. One shell company incorporated by the lawyer was used to channel more than CAD 6m of funds provided by members of the criminal organisation to other assets. On one occasion the lawyer issued a CAD 7 000 cheque from this shell company to a Vancouver brokerage firm to purchase stock.

Source: Schneider, S. (2004)

Case 94 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation, including incorporation in high risk countries • Client is known to have involvement in criminal activity

Case 95: **Three lawyers investigated for establishing companies and purchasing properties on behalf of drug traffickers – common law country**

During one proceeds of crime investigation into three Alberta-based cocaine and marijuana traffickers – Mark Steyne, Pitt Crawley, and George Obsorne – police identified three lawyers who helped the accused establish and operates companies, which were eventually proven to be nothing more than money laundering vehicles.

Documents seized by the RCMP indicated that Becky Sharp acted as legal counsel on behalf of Steyne in the incorporation and preparation of annual returns for Vanity Fair Investments Inc., a public

company in which Steyne and Crawley each held 50 percent voting shares. The corporate address listed for this company was Sharp's law office.

Documents seized by police from the law office of Sharp also showed that she represented Steyne in the purchase of real estate, the title of which was registered in the name of Vanity Fair Investments Inc. Among the documents seized by police were letters from Sharp, addressed to the Vanity Fair Investments, which included certificates of incorporation, bank statements for commercial accounts, and documents showing that Steyne and Crawley were directors and shareholders of the company.

Another lawyer acted on behalf of Steyne and companies he controlled, providing such services as incorporating numbered companies, conducting real estate transactions, purchasing a car wash, and preparing lease agreements between Steyne and the tenants of a home that was used for a marijuana grow operation. Finally, documents seized by police indicated that Majah Dobbin, a partner in a local law firm, acted on behalf of Crawley and Osborne in the incorporation of three other Alberta companies.

Source: Schneider, S. (2004)

Case 95 **Red flag indicators:**	• Use of multiple legal advisors for different businesses without good reasons • Significant funding for companies not consistent with known legitimate income

Case 96: **Legal professional provides office address and acts as director for 17 companies they set up for drug traffickers – common law country**

Public documents seized as part of a police investigation into an international drug trafficking group based in Ontario showed that a Toronto lawyer incorporated 17 different businesses that were eventually traced to members of the crime group. Upon further investigation, police discovered that the office of the law firm was listed as the corporate address for many of the companies. The lawyer was also a director of two of the businesses he helped establish. During their investigation, police learned that two members of this crime group were to go to their lawyer's office —to sign for the new companies. Records obtained from the Ontario Ministry of Consumers and Corporate Relations show that a week later, two limited companies were incorporated listing both as directors.

Source: Schneider, S. (2004)

Case 96 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation, including incorporation in high risk countries • Client is known to have involvement in criminal activity

Case 97: **Legal professional creates companies to provide cover story for international travel and movement of funds – civil law country**

A number of Iranian citizens were involved in the incorporation or subsequent purchase of stock in companies. On occasion they attended in person, having travelled from Tehran, while on other occasions they are represented by a German citizen or, more typically, a fellow Iranian citizen resident in Spain.

In 2007 and 2008 Company A was incorporated by an Iranian citizen and the German citizen or by other Iranians citizens acting under their guidance, and the shares of the company were sold to various Iranian citizens, in each transaction for low prices (*e.g.* EUR 25).

In 2009 and 2010 Company B was incorporated directly by Iranian citizens, with the representative or director of the company incorporated either one of the Iranian citizens or the German, appearing in all cases as interpreter.

In both the purchase of stock and the incorporation of companies, the Iranian citizens travel to Spain on occasion, while on other occasions they provide a power of attorney for this purpose executed before a notary in Tehran.

There was no information about the intended business of the companies and the creation of two companies in the same regional area made it unlikely that the companies would be implementing a normal business or economic project. The FIU were of the view that the creation of the companies and involvement of such a wide range of Iranian nationals was to enable them to obtain visas for entry into Spain and therefore to travel through the European Union, for which they receive substantial sums of money, thereby constituting a criminal activity generating funds to be laundered.

Source: Spain (2012) questionnaire response

Case 97 **Red flag indicators:**	• The parties or their representatives are native to and resident in a high risk country and there is no clear connection with the country in which the transaction is happening • A large number of securities are issued at a low price which is not consistent with genuine capital raising purposes • The objects of the company are vague and there appears to be limited commercial viability for both companies

Case 98: **Legal professional assists in creating multijurisdictional web of companies with no legitimate reason for the complexity – civil law jurisdiction**

A Spanish citizen is listed as the director of numerous Spanish limited liability companies with a wide range of corporate purposes (from renewable energies to aquaculture to information technology), although it is not clear whether these companies are genuinely operational.

Within a short space of time these Spanish companies are transferred to recently incorporated Luxembourg-registered companies, for a purchase price of several million euros. Following the transfer of stock, rights issues, involving very considerable sums are performed.

The Luxembourg-registered companies which purchased the stock in the Spanish companies

invested by means of the subscription of corporate stakes in the stock issues of Spanish companies. The foreign purchaser companies were based in Uruguay, Gibraltar, Seychelles, Panama, British Virgin Islands and Portugal. Several of the directors of the purchasing companies are also listed as representatives or directors of some of the transferred companies.

The representatives of the foreign purchaser companies declare that there is no beneficial owner (a natural person with a controlling stake above 25%).

Spanish notaries are required to be involved in all company incorporations and share sales.

Source: Spain (2012) questionnaire response

Case 98 **Red flag indicators:**	• Creation of complicated ownership structures, including multiple countries some of which are high risk, without legitimate reason • Incorporation and/or purchase of stock or securities of several companies within a short period of time with elements in common with no logical explanation. • The company receives an injection of capital which is notably high in comparison with the business size and market value of the company, with no logical explanation.

Case 99: **Legal professional secures banking services for yet to be created companies with significant funds deposited into the accounts and to be transferred between the companies without any apparent underlying economic activity – civil law country**

A lawyer opens bank accounts in the Netherlands in the name of various foreign companies yet to be established. In one of those accounts is deposited an amount of almost 20 million guilders. The intention was that between the accounts of the companies transactions would seem to take place. Per transaction would be a (fictitious) profit of approximately half a million guilders. The bank examines these arrangements and concludes that the lawyer is organising a money laundering scam. The bank refuses further cooperation and sends the money back. The money comes from a large-scale international fraudster.

Source: Netherlands (1996)

Case 99 **Red flag indicators:**	• Involvement of multiple countries without legitimate reason • Significant private funding not consistent with known legitimate income • The transaction is unusual given the amount of profit likely to be generated • Client has been convicted of acquisitive crimes

Case 100: **Legal professional continues to establish corporate entities and conduct share transactions which launder funds despite concerns – civil law country**

Notary Klaas regularly establishes legal entities at the request of client Joep and also conducts share

transactions. Client Joep trades fraudulently in companies. At one point, given the dubious circumstances surrounding the transactions, Klaas consults with a colleague notary who has previously rendered services to Joep. Although they are not able to discover anything suspicious, notary Klaas is left with a 'gut-feeling' that his services are being abused. Klaas does not conduct any deeper investigation into the background of his client and allows himself to be misled on the basis of the documents. He continues to render services without further question. During the police interrogation, Joep states that he used the services of Klaas because the notary worked fast and did not ask tricky questions.

Source: Lankhorst, F. and Nelen, H. (2005

Case 100 **Red flag indicators:**	• Incorporation of multiple companies for a single client, without clear economic justification • Use of multiple legal advisors

Case 101: **Legal professional convicted for allowing client account and personal account to be used by a client engaged in tax fraud – common law country**

In 2002, Mr Hyde, a solicitor assisted a client who had engaged in tax (MTIC) fraud and property development fraud to set up shell companies with off shore accounts, and wittingly allowed his client account and a personal account in the Isle of Man to be used to transfer funds. Over GBP 2m in criminal proceeds were laundered in this way. The solicitor was convicted in 2007 of concealing or disguising criminal property. He was jailed for three and a half years and in 2008 was stuck off.

Source: United Kingdom (2012) questionnaire response

Case 101 **Red flag indicators:**	• Disproportionate amounts of private funding • Complex companies with unnecessary foreign element • Use of client account without underlying transaction • Client known to be involved in criminal activity

Case 102: **Legal professional launders millions through companies for a corrupt PEP due to the mistaken belief that money laundering only involved cash – common law country**

A United Kingdom solicitor who assisted with laundering funds removed from Zambia by a former President. Funds allegedly for defence purposes were transferred through companies which the solicitor had set up, but were then used to fund property purchases, tuition fees and other luxury goods purchases. The solicitor ultimately made a STR and was not prosecuted. The solicitor was also found not to be liable in a civil claim for knowing assistance as dishonesty was not proven. This was on the basis that the claimant did not sufficiently controvert the solicitor's evidence that he had genuinely believed that money laundering only occurred when cash was used and not when money came through a bank. The case related to conduct between 1999 and 2001.

Source: United Kingdom (2012) questionnaire response

Case 102 **Red flag indicators:**	• Client holds a public position in a high risk country • Use of company and government funds to pay for private purchases • There are attempts to obscure the real owners or parties to the transaction

Case 103: **Legal professional convicted for assisting a corrupt PEP to purchase property, vehicles and private jets – common law country**

In 2006, Bhadresh Gohil, a solicitor acted for an African governor. He helped to set up shell companies, transferred funds to foreign accounts, opened bank accounts, purchased property, cars and a private jet for the client. The transactions involved amounts far in excess of the client's income as a governor or other legitimate income. Mr Gohil was convicted in 2010 of entering into arrangements to facilitate money laundering and concealing criminal property and was sentenced to 7 years jail. He was subsequently struck off in 2012. The criminal conviction is currently the subject of an appeal. The governor was convicted of fraud in 2012.

Source: United Kingdom (2012) questionnaire response

Case 103 **Red flag indicators:**	• Client holds a public position in a high risk country • Disproportionate private funding in light of known legitimate income • Use of company and government funds to pay for private purchases

Case 104: **Legal professional prosecuted for allegedly creating companies and otherwise assisting the laundering of the proceeds of drug trafficking – common law jurisdiction**

On November 5, 2012, an indictment was unsealed in the Western District of Texas charging an El Paso attorney, Marco Antonio Delgado, with conspiracy to launder the proceeds of a foreign drug trafficking organization, Cartel de los Valencia (AKA the Milenio Cartel), based in Jalisco, Mexico. Delgado was a principal in his own international law firm, Delgado and Associates, and is alleged to have laundered around USD 2 million, although he reportedly was asked to launder an amount exceeding $600 million.

Between July 2007 and September 2008, Delgado is accused of, among other things: establishing shell companies in the Turks and Caicos for the purpose of laundering drug proceeds; employing couriers to deliver shipments of currency and drawing up fraudulent court documents to provide the couriers with a back story should they be stopped by authorities; arranging a bulk cash smuggling operation unknown to law enforcement while simultaneously "cooperating" with the Government; and attempting to utilize his girlfriend's bank account to launder drug proceeds, although, ultimately, Delgado deposited the funds into his attorney trust account at a U.S. bank.

On February 27, 2013, a second indictment was handed down in the Western District of Texas charging Delgado with wire fraud and money laundering. This prosecution involves a scheme separate and distinct from the drug money laundering above. Here, Delgado defrauded a Nevada company and a Mexican state-owned utility (the *Comision Federal de Electricidad*), in connection a USD 121 million contract to provide heavy equipment and maintenance services for such equipment to a power plant located in Agua Prieta, Sonora, Mexico. FGG Enterprises, LLC ("FGG") is owned and

solely managed by "F.J.G," an unnamed third party. FGG won the contract described above, and payments on the contract were supposed to be directed, by the Mexican utility, through Banco Nacional de Comercio Exterior, to an account owned by FGG at Wells Fargo Bank in El Paso, Texas. Delgado sent a letter to the legal representative of the Mexican utility, instructing the representative to make the payments meant for FGG to a bank account in the Turks and Caicos Islands controlled by Delgado. This letter was sent without the knowledge and consent of F.J.G., the owner of FGG. In total, USD 32 million was wired into the Turks and Caicos account for Delgado's personal enrichment. These funds were subsequently laundered back into the United States to accounts controlled by Delgado.

Furthermore, in a related civil forfeiture action, prosecutors have frozen the proceeds of Delgado's fraud that were sent to the benefit of "Delgado & Associates LLC" from the Mexican utility. The account holding the funds is actually a client account belonging to a local law firm in the Turks & Caicos. The funds belonging to Delgado have been segregated and restrained, as the law firm filed a petition the Turks and Caicos court to modify the initial restraint. Evidently, the legal representatives of Delgado & Associates LLC were unaware that their client account was being used for criminal purposes, as they were informed that the purpose of the Delgado & Associates legal structure was to assist in receiving and disbursing funds related to a client's subcontract to sell turbines to Mexico.

Source: United States (2012) questionnaire response: United States v. Delgado, *No. 3:12-cr-02106-DB (W.D. Tex.) (drug money laundering);* United States v. Delgado, *No. 3:13-cr-00370-DB (W.D. Tex.) (Mexican utility scheme); and* United States v. Any and All Contents of FirstCaribbean International Bank Account Number 10286872, *No. EP 12-cv-0479 (W.D. Tex.).*

Case 104 **Red flag indicators:**	• Clients are known to be under investigation for acquisitive crimes • Involvement of multiple foreign bank accounts and foreign companies without legitimate reasons • Use of the client account without underlying transactions

Case 105: **Legal professional convicted for setting up a sham company and helping to create a cover story to launder the proceeds of crime – common law country**

In a government sting operation, an undercover agent approached attorney Angela Nolan-Cooper, who was suspected of helping launder criminal proceeds for clients, seeking help in laundering supposed drug proceeds. Nolan-Cooper agreed to help, and did so by establishing a sham entity, a purported production company, and hiding the proceeds in Bahamian bank accounts. Nolan-Cooper told the undercover agent that funnelling his money through a corporation would make it appear legitimate because it would establish a source of income and facilitate filing false tax returns that would legitimise the money.

Nolan-Cooper later arranged for an accountant to help draw up false corporation papers and corporate tax returns, although it appears the conspiracy was intercepted before this could occur. Nolan-Cooper also facilitated the deposit of large sums of cash into a Cayman Island account at the direction of the undercover agent, who told her that he needed the money in that account to complete a drug transaction. Nolan-Cooper entered a conditional plea to multiple counts of money laundering. Upon resentencing on remand, Nolan-Cooper was sentenced to 72 months incarceration and three years' supervised release. See 155 F.3d 221 (3rd Cir. 1998) (affirming denial of motion to dismiss and vacating sentence); see also United States v. Carter, 966 F. Supp. 336 (E.D. Pa. 1997)

(reversing the district court's grant of judgment of acquittal).

Source: United States (2012) questionnaire response: United States v. Nolan-Cooper, *No. 95-cr-435-1 (E.D. Pa.)*

Case 105 **Red flag indicators:**	• Involvement of structures and bank accounts in multiple high risk countries with no legitimate reason • Creation of a company whose main purpose is to engage in activities within an industry with which neither the shareholders or the managers have experience or connection • Use of client account without an underlying transaction

Case 106: **Legal professional convicted of setting up companies to launder proceeds of corruption – common law country**

Attorney Jerome Jay Allen pleaded guilty to conspiring to commit money laundering in connection with his assistance in laundering the proceeds of a fraudulent kickback scheme. The scheme involved two employees of a steel processing company who caused their company to overpay commission on certain contracts. A portion of the inflated commission was then funnelled back to the employees through shell companies created by Allen. See United States v. Graham, 484 F.3d 413 (6th Cir. 2007).

Source: United States questionnaire response 2012: United States v. Allen, *No. 5:03-cr-90014 (E.D. Mich.)*

Case 106 **Red flag indicators:**	• Source of funds not consistent with known legitimate income • There are attempts to disguise the real owners or parties to the transactions • U-turn transactions

METHOD: MANAGEMENT OF COMPANIES AND TRUSTS

TECHNIQUE: MANAGEMENT OF A COMPANY OR TRUST – CREATION OF LEGITIMACY AND PROVISION OF LEGAL SERVICES

Case 107: **Legal professional involved in managing an offshore company which was laundering the proceeds of a pyramid scheme – civil law country**

In 2004 the A-FIU received several STRs. The reporting entities have mentioned that some suspects were using several bank accounts (personal bank accounts, company bank accounts and bank accounts from offshore companies). After the analysis the A-FIU assumed that the origin of the money is from fraud and pyramid schemes. The A-FIU disseminated the case to a national law enforcement authority and coordinated the case on international level. The A-FIU requested information from abroad (using Interpol channel, Egmont channel and L/O). The results proved that the Austrian lawyer was a co-perpetrator because he was managing an involved offshore company and the bank account of the company. These results were also disseminated to the national law enforcement agency. The investigation revealed approximately 4000 victims with a total damage of app. EUR 20 mil. The public prosecutor's office issued two international arrest warrants. In 2008

four suspects were convicted for breach of trust. Also the lawyer was convicted for breach of trust with a penalty of 3 years.

Source: Austria (2012) questionnaire response

Case 107 **Red flag indicators:**	• Use of foreign bank accounts and companies without a legitimate reason • Payments made were not consistent with contractual terms

Case 108: **Legal professionals set up companies and accept multiple deposits to launder proceeds of liquor smuggling – hybrid common / civil law country**

A police investigation into Joseph Yossarian, a Quebec liquor smuggler, revealed that he invested money into and eventually purchased a company for which lawyer Pierre Clevingier was the founder, president, director, and sole shareholder. Clevingier was also the comptroller for the company and was listed as a shareholder of three other numbered companies, which police traced to Yossarian. Yet another company, registered in the name of Yossarian's sister, was used as a front for Joseph's investment into a housing development. This company was incorporated by lawyer Robert Heller, who had established other shell companies registered in the name of the sister and used by her brother to launder money. Heller was also involved in transactions relating to companies that he set up for the benefit of Yossarian, including issuing and transferring shares in these companies and lending money between the different companies. Yossarian invested CAD 18 000 in another housing development in Montreal through a company established by Quebec real estate lawyer Albert Tappman. Records seized by police during a search of Tappman's law office established that he had received cash and cheques from Yossarian, including a deposit of CAD 95 000 (CAD 35 000 of which was cash), which he deposited for Yossarian in trust. Police also found copies of two cheques, in the amount of CAD 110 000 and CAD 40 000, drawn on Tappman's bank account, and made payable to the order of a company he created on behalf of Yossarian. Tappman used a numbered company, for which another lawyer was the director and founder, as the intermediary through which Yossarian and others invested in housing developments.

Source: Schneider, S. (2004)

Case 108 **Red flag indicators:**	• Incorporation of several companies in a short period of time with elements in common with no logical reason • Use of multiple legal advisors without legitimate reasons • Significant cash deposits • There are attempts to disguise the real owners of or parties to the transactions • Potential use of a client account without underlying transactions

METHOD: MANAGING CLIENT AFFAIRS AND MAKING INTRODUCTIONS

TECHNIQUE: OPENING BANK ACCOUNTS ON BEHALF OF CLIENTS

Case 109: **Legal professional assists organised criminal to open bank account – civil law country**

A foreigner residing in Belgium was introduced to a bank by a Belgian lawyer's office in order to open an account. This account was then credited by substantial transfers from abroad that were used for purchasing immovable goods. The FIU's analysis revealed that the funds originated from organised crime.

Source: Belgium (2012) questionnaire response

Case 109 **Red flag indicators:**	• Client requires introduction to financial institutions to help secure banking facilities

Case 110: **Legal professional assists foreign PEP to open bank accounts – civil law country**

In a file regarding corruption, a politically exposed person (PEP) was the main beneficial owner of companies and trusts abroad. Accounts in Belgium of these companies received considerable amounts from the government of an African country. The FIU's analysis revealed that the individual had been introduced to the financial institution by a lawyer. It turned out that the lawyer was also involved in other schemes of a similar nature in other judicial investigations.

Source: Belgium (2012) questionnaire response

Case 110 **Red flag indicators:**	• Client holds a public position and is the beneficial owner of multiple companies and trusts in foreign countries • Government funds being used to pay for private or commercial expenses • Client requires introduction to financial institutions to help secure banking facilities

Case 111: **Legal professional assists front company to open bank account – civil law country**

One file regarded a company established in an offshore centre, which was quoted on the stock exchange. Information obtained by the Unit revealed that the stock exchange supervisor had published an official notice stating that the stock of this company had been suspended due to an investigation into fraudulent accounting by this company.

A network of offshore companies was used to intentionally circulate false information regarding this stock in order to manipulate the price. In the meantime a procedure had been initiated by the American stock exchange supervisor to cancel this stock. Information obtained by the Unit revealed that the main stockholder of this company had laundered money from this stock exchange offence by transferring money to an account that he held in a tax haven. In addition, it also became clear that he had called upon a lawyer in Belgium to request opening a bank account in name of a front

company, and to also represent this company in order to facilitate money laundering.

Source: Belgium (2012) questionnaire response

Case 111 **Red flag indicators:**	• Client currently under investigation for acquisitive crime • Involvement of structures with multiple countries, some of which were high risk, without legitimate reason • Client requires introduction to financial institutions to help secure banking facilities

Case 112: **Legal professional convicted for providing laundering services to a criminal group undertaking a Ponzi scheme – common law country**

Six defendants were indicted on 89 counts related to a Treasury bill-leasing Ponzi scheme perpetrated through the corporation K-7. Subsequently, the group's attorney, Louis Oberhauser, was added as a defendant in a superseding indictment. Oberhauser had held some of the invested funds in an attorney trust account designated for K-7 pursuant to an escrow agreement he had drafted. He also had helped to incorporate K-7 and arrange lines of credit on K-7's behalf, as well as entered into contracts with investors on behalf of his law firm that authorized Oberhauser to act on behalf of the investors in entering into a trading program. All defendants excepting Oberhauser and one other co-conspirator pleaded guilty. In a joint trial, the co-conspirator was convicted of 68 counts, and Oberhauser acquitted on 62 of 66 counts and convicted on two counts of money laundering. The district court granted judgment of acquittal, but the appeals court reversed that decision. Oberhauser was sentenced to 15 months' incarceration, two years' supervised release, community service, and restitution in an amount of USD 160 000. *See* 284 F.3d 827 (8th Cir. 2002).

Source: United States (2012) questionnaire response United States v. Oberhauser, No. 99-cr-20(7) (D. Minn.)

Case 112 **Red flag indicators:**	• Legal professional acting in a potential conflict of interest situation • Client requires introduction to financial institutions to help secure banking facilities

Case 113: **Legal professional convicted after setting up companies, structuring deposits and maintaining the company accounts to launder funds – common law country**

Attorney Luis Flores was convicted of one count of conspiracy to commit money laundering, three counts of money laundering, and one count of structuring currency transactions to avoid reporting requirements. A client approached Flores representing himself to be an Ecuadoran food importer/exporter. Flores opened several corporations for the client and established several business accounts. Flores maintained the accounts for a USD 2,000 weekly salary. Flores held himself out as the president of the corporations and was the only authorized signatory on the corporation accounts. Cash deposits into the accounts always totalled less than USD 10 000. As banks closed accounts due to suspicious activity, Flores would open new accounts. He also laundered cash through brokerages on the black market peso exchange. See 454 F.3d 149 (3rd Cir. 2006) (affirming conviction and 32-month sentence).

Source: United States (2012) questionnaire response United States v. Flores, No. 3:04-cr-21 (D.N.J.)

Case 113 **Red flag indicators:**	• Incorporation of multiple corporations and use of multiple bank accounts within a short space of time where there are elements in common with no logical explanation. • Attorney fees disproportionate to the income of the companies. • Structuring of payments • Client requires introduction to financial institutions to help secure banking facilities

TECHNIQUE: MANAGEMENT OF CLIENT'S GENERAL AFFAIRS THROUGH CLIENT ACCOUNT

Case 114: **Legal professional helps to hide cash from a bankruptcy through a life insurance policy – common law country**

A bankrupt individual used the name of a family member to pay cash into an account and to draw a cheque to the value of the cash. He provided the cheque to a lawyer. The lawyer provided a cheque to the family member for part of the sum and then deposited the remainder of the funds into the person's premium life policy which was immediately surrendered. The surrender value was paid into the family member's account.

Source: Australia (2012) questionnaire response

Case 114 **Red flag indicators:**	• Legal professional involved in a U turn transaction • Provision of financial services not in connection with an underlying transaction • Provision of funds from a third party without legitimate reason • Use of client account without an underlying transaction

Case 115: **Legal professional creates web of fake loans and contracts between companies of which he was a director to launder the proceeds of crime – civil law country**

Company A established abroad, with very vague corporate goals and directors residing abroad, had opened an account with a bank in Belgium. This company had been granted a very large investment loan for purchasing a real estate company in Belgium. This loan was regularly repaid by international transfers from the account of Z, one of company A's directors, who was a lawyer. The money did not originate from company A's activities in Belgium. Furthermore, the loan was covered by a bank guarantee by a private bank in North America. This bank guarantee was taken over by a bank established in a tax haven shortly afterwards. Consequently, the financial structure involved a large number of countries, including offshore jurisdictions. The aim was probably to complicate any future investigations on the origin of the money. Furthermore, company A's account was credited by an international transfer with an unknown principal. Shortly afterwards the money was withdrawn in cash by lawyer Z, without an official address in Belgium. Information from the FIU's foreign counterparts revealed that the lawyer's office of which Z was an associate, was suspected of being involved in the financial management of obscure funds. One of the other directors of company A was known for trafficking in narcotics and money laundering. All of these elements indicated that

company A and its directors were part of an international financial structure that was set up to launder money from criminal origin linked to trafficking in narcotics and organised crime.

Source: Belgium (2012) questionnaire response

Case 115 **Red flag indicators:**	• Investment in immovable property, in the absence of links with the place where the property is located • Funding from a private bank in a country not connected with either the location of the company or the location of the property being purchased • Instruction of a legal professional at a distance from the transaction • Third party funding without apparent legitimate connection and withdrawal of that funding in cash shortly after deposit

Case 116: **Lawyer accepts cash, creates companies and purchases property for drug trafficker – common law country**

While an Alberta-based drug trafficker used numerous law firms to facilitate his money laundering activity, he appeared to have preferred one firm over all the others. On numerous occasions, a partner in this preferred law firm accepted cash from the drug trafficker, which was then deposited by the lawyer for his client, in trust. According to deposit slips seized by police, between August 19, 1999 and October 1, 2000 a total of USD 265 500 in cash was deposited by the lawyer in trust for this client. The funds would then be withdrawn to purchase assets, including real estate and cars. The drug trafficker often used shell and active companies to facilitate his money laundering activities. Documents seized by the RCMP showed that on November 9, 1999, the lawyer witnessed the incorporation a company, of which the drug trafficker was a director. Along with the brother of the lawyer, the drug trafficker was also listed as a director of another company and police later identified cash deposits of USD 118 000 into the legal trust account on behalf of this company. The deposit slips were signed by the lawyer. Funds were also transferred between the various trust account files the lawyer established for this client and his companies. In one transaction under the lawyer‘s signature, USD 83 000 was transferred from this client‘s trust account file to the latter company he incorporated on behalf of this client.

Source: Schneider, S. (2004)

Case 116 **Red flag indicators:**	• Use of multiple legal advisors without legitimate reason • Significant deposits of cash not consistent with known legitimate income • Incorporation of multiple companies without legitimate business purposes • Use of client account without an underlying transaction

Case 117: **Legal professional convicted and removed from practice for laundering the proceeds of fraud through his client account and personal account – common law jurisdiction**

The Louisiana Office of Disciplinary Counsel (ODC) filed a petition to permanently disbar attorney Derrick D.T. Shepherd. In April 2008, a federal grand jury indicted Shepherd, who was then serving as a Louisiana state senator, on charges of mail fraud, conspiracy to commit mail and wire fraud, and conspiracy to commit money laundering. The indictment alleged that Shepherd helped a convicted bond broker launder nearly USD 141 000 in fraudulently generated bond fees, and in October 2008, Shepherd pleaded guilty to the money laundering charge. Shepherd admitted to helping broker Gwendolyn Moyo launder construction bond premiums paid to AA Communications, Inc., long after the company was banned from engaging in the insurance business and its accounts were seized by state regulators. Specifically, in December 2006, Shepherd deposited into his client trust account USD 140 686 in checks related to bond premiums and made payable to AA Communications. He then wrote checks totalling USD 75 000 payable to the broker and her associates. Of the remaining funds, Shepherd transferred USD 55 000 to his law firm's operating account and deposited USD 15 000 into his personal checking account. He then moved USD 8 000 from the operating account back into his client trust account. On December 21, 2006, respondent paid off USD 20 000 in campaign debt from his operating account, writing "AA Communications" on the memo line of the check. To conceal this activity, respondent created false invoices and time sheets reflecting work purportedly done by his law firm on behalf of the Ms. Moyo.

Upon investigating Shepherd for multiple ethical violations, the ODC obtained copies of Shepherd's client trust account statements and determined that he had converted client funds on numerous occasions, frequently to mask negative balances in the account. He also commingled client and personal funds and failed to account for disbursements made to clients.

Shepherd submitted untimely evidence to the Court documenting his "substantial assistance to the government in criminal investigations," but the Court found Shepherd's money laundering, which promoted his co-conspirators' unlawful activity and benefitted him personally, to be reprehensible and deserving of the harshest sanction. Despite Shepherd's contention that his federal conviction was not "final" and his denial of any misconduct, the Court permanently disbarred Shepherd from the practice of law.

Source: United States (2012) questionnaire response In re Shepherd, 91 So.3d 283 (La. 2012)

Case 117 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • Client company is engaging in businesses without a relevant licence / having been banned from engaging in that business • Client is unable to access financial services • Use of client account without underlying transactions, contrary to client account rules • Legal professional acting in potential conflict of interest situation – by making payments into personal accounts

Case 118: **Legal professional convicted for helping ex-police officer launder drug money by accepting cash through his client account for the purchase of stocks – common law jurisdiction**

Defence attorney Scott Crawford was convicted of laundering drug proceeds through his escrow account. Patrick Maxwell, an ex-police officer turned drug dealer, wanted to invest his drug proceeds in the stock market, but wanted to avoid suspicion that would arise if he deposited two large amounts of cash in a bank account. A third party would give Maxwell's cash to Crawford, who would then deposit it in his legal practice's escrow account. From that account, Crawford drew cashier's checks payable to Prudential Securities. The checks were then deposited in a brokerage account controlled by Maxwell. See 281 F. App'x 444 (6th Cir. 2008) (affirming 71-month sentence).

Source: United States (2012) questionnaire response United States v. Crawford, No. 2:04-cr-20150 (W.D. Tenn.)

Case 118 **Red flag indicators:**	• Significant level of cash deposits not consistent with known legitimate income • Payments via a third party in an attempt to disguise the true parties to the transaction • Use of the client account without an underlying legal transaction

Case 119: **Legal professional convicted of money laundering after safe keeping cash obtained from clients he represented in relation to drug charges – common law country**

Attorney Juan Carlos Elso was convicted of money laundering and conspiracy to launder money by engaging in a transaction designed to conceal the origin of drug proceeds and by conspiring to engage in a financial transaction involving drug proceeds so as to avoid reporting requirements. With respect to the money laundering offense, Elso agreed to launder the proceeds of a former client, who he had represented in a drug case and who had paid attorney and investigator fees in cash. Elso retrieved USD 266 800 in cash from the client's house for safekeeping (in case of search by law enforcement). On the way back to his office with the cash, Elso was stopped and arrested. The conspiracy count was based upon a wire transfer Elso made on behalf of the wife of another former drug client. The wife, who was given USD 200 000 to launder, brought Elso USD 10 000, which he deposited into his law firm's trust account and then wired USD 9 800 to an account affiliated with Colombian drug suppliers. Elso did not file federally required reports in conjunction with this transaction. See 422 F.3d 1305 (11th Cir. 2005) (affirming Elso's conviction and 121-month sentence).

Source: United States questionnaire response 2012: United States v. Elso, No. 03-cr-20272 (S.D. Fla.)

Case 119 **Red flag indicators:**	• Client is known to be under investigation / prosecution for acquisitive crimes • Disproportionate amounts of cash not consistent with known legitimate income • Use of the client account without an underlying legal transaction • Structuring of payments

METHOD: USE OF SPECIALISED LEGAL SKILLS

Case 120: **Legal professional arrested after attempting to clear a drug dealers accounts subject to a power of attorney – civil law jurisdiction**

A drug dealer is in detention. He fears that the Prosecutor/judge will confiscate his bank accounts in Luxembourg. The lawyer also approaches a colleague in Luxembourg and asks him how the relationship between the dealer and the money can be broken. The lawyer obtains a power of attorney over the account and attends the bank to withdraw all of the assets from the bank. The lawyer was arrested in his efforts to retrieve the money from the bank.

Source: The Netherlands (1996)

Case 120 **Red flag indicators:**	• Client is known to be under investigation / have convictions for acquisitive crime • Use of foreign bank accounts without legitimate reasons • A power of attorney is sought for the administration or disposal of assets under conditions which are unusual.

Case 121: **Legal professional prosecuted for allegedly creating a range of entities and accounts to launder proceeds of fraud – common law country**

The predicate offence was fraud involving several persons, one of whom was an attorney-at-law and several companies. The offence was committed during the period 1997 to 2000 and the subjects were arrested and charged in 2002.

The attorney-at-law was instrumental in creating different types of financial vehicles such as loans, bonds, shares, trusteeships and a myriad of personal, business and client accounts to facilitate the illicit activity which started with the loan-back method being used to purchase bonds.

It was alleged that the attorney designed documents and transactions to facilitate the laundering of proceeds of the offence, namely obtaining money by false pretences contrary to section 46 of the Proceeds of Crime Act 2000. This matter is before the Courts of Trinidad and Tobago.

Source: Trinidad & Tobago (2012) questionnaire response

Case 121 **Red flag indicators:**	• Involvement of multiple entities, arrangements and bank accounts with elements in common with no legitimate explanation • Client requires introduction to a financial institution to secure banking facilities

Case 122: **Legal professional accepts large amounts of cash for safekeeping and paying bail from criminals he is defending – common law country**

Between 1993 and 2006 a solicitor, Anthony Blok, acted for a number of clients facilitating money laundering. In one case he entered into negotiations to sell a painting he knew clients had stolen and to have it removed from the arts theft register. In another case he received and paid

GBP 75 000 in cash for bail where he was acting for a client whose only source of income had been fraud and money laundering, and lied as to where the money had come from when asked by investigators. Finally, he had large amounts of unexplained cash in envelopes in the office with the names of clients on them – who he was defending in criminal matters. The Court accepted that if the funds had been for the payment of fees, they should have been banked, and absent any explanation as to the reason for holding those funds, the jury conclude that Mr Blok must have been concealing the proceeds of crime on behalf of the clients. In 2009 Mr Blok was convicted of transferring criminal property, possessing criminal property, entering into an arrangement to facilitate money laundering and failure to disclose, 4 years jail. In 2011 he was stuck off the roll.

Source: United Kingdom (2012) survey response

Case 122 **Red flag indicators:**	• Client is known to be under investigation for acquisitive crimes • The holding of large deposits of money without the provision of legal services • Significant amounts of cash not consistent with known legitimate income levels

Case 123: **Legal professional convicted for assisting in laundering the proceeds of a drug deal found in a safe through a real estate investment company – common law country**

Walter Blair was convicted of laundering drug proceeds obtained from a client. His client had possession of a safe containing the drug proceeds of a Jamaican drug organization. After the head of the organization (who owned the safe) was murdered, Blair helped his client to launder the money by inventing an investment scheme based on the Jamaican tradition of cash-based "partners money," setting up a real estate corporation in the name of the client's son, opening an account in the corporation's name, and obtaining loans on behalf of the corporation to make real estate investments. Blair misrepresented the amount of currency in the safe to his client and retained some of the funds in addition to withholding fees for his legal services. See 661 F.3d 755 (4th Cir. 2011), cert. denied 132 S. Ct. 2740 (2012) (affirming conviction and sentence).

Source: United States questionnaire response 2012: United States v. Blair, No. 8:08-cr-505 (D. Md.)

Case 123 **Red flag indicators:**	• Client is known to have connections with criminals • There are attempts to disguise the real owners or parties to the transaction • Source of funds is not consistent with known legitimate income • Client requires introduction to financial institutions to help secure banking facilities • Legal professional is acting in a conflict of interest situation

Appendix 3

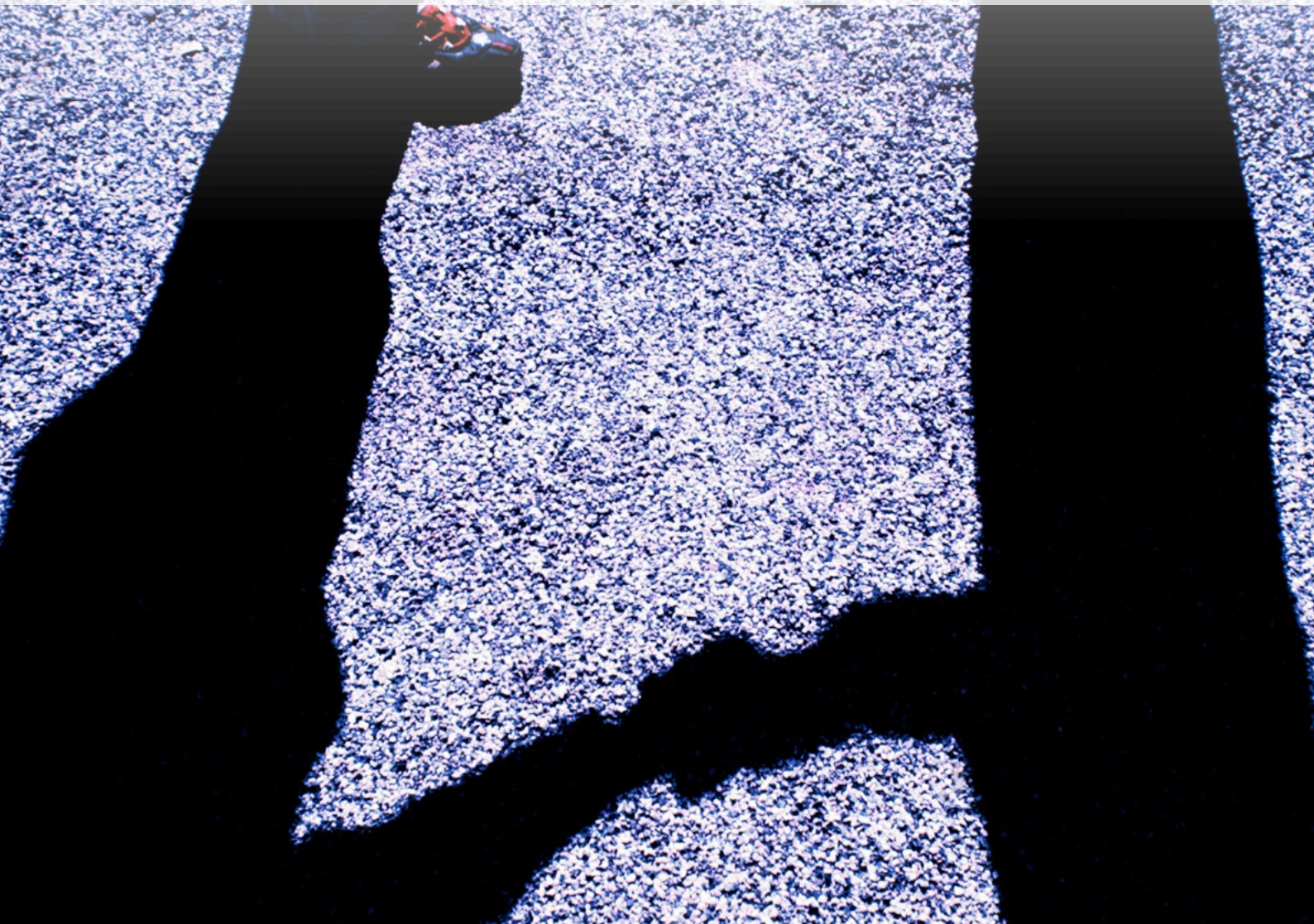
FATF Report – *Professional Money Laundering* – July 2018

FATF

FATF REPORT

Professional Money Laundering

July 2018



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

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

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

Citing reference:

FATF (2018), *Professional Money Laundering,* FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html

TABLE OF CONTENTS

Boxes

TABLE OF ACRONYMS

CFATF	Caribbean Financial Action Task Force
EAG	Eurasian Group
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MVTS	Money Value Transfer Service
PML	Professional Money Launderer
PMLO	Professional Money Laundering Organisation
PMLN	Professional Money Laundering Network
OCG	Organised Crime Group
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider

EXECUTIVE SUMMARY

This is the first time the FATF is undertaking a project which concentrates on professional money launderers (PMLs) that specialise in enabling criminals to evade anti-money laundering and counter terrorist financing safeguards and sanctions in order to enjoy the profits from illegal activities. The report aims to describe the functions and characteristics that define a "professional" money launderer, namely those individuals, organisations and networks that are involved in third-party laundering for a fee or commission. This report is therefore focused on money laundering *threats* as opposed to *vulnerabilities*, and it addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. While PMLs may act in a professional capacity (e.g. lawyer, accountant) and serve some legitimate clients, the report aims to identify those actors who serve criminal clients whether on a full-time or part-time basis.

PMLs provide services to criminals and organised crime groups by laundering the proceeds of their illegal activities. As the main purpose of PMLs is to facilitate money laundering, they are rarely involved in the proceeds-generating illegal activities. Instead, they provide expertise to disguise the nature, source, location, ownership, control, origin and/or destination of funds to avoid detection. PMLs generally do not differentiate between drug dealers, fraudsters, human traffickers or any other criminal with a need to move or conceal ill-gotten gains. These are all potential PML clients. PMLs operate under a number of business models and may be individuals; criminal organisations with a clear structure and hierarchy; or networks of loosely affiliated members. Providing services to criminals and organised crime groups, PMLs are criminal actors, profiting from these money laundering activities.

PMLs may provide the entire infrastructure for complex money laundering schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. These PMLs provide a menu of generally applicable services, with the result that the same laundering techniques (and potentially the same financial channels and routes) may be used for the benefit of multiple organised crime groups. As such, professional money laundering networks may act transnationally in order to exploit vulnerabilities in countries and particular businesses, financial institutions, or designated non-financial businesses or professions. PMLs, themselves, pose a threat to the financial system, as they facilitate money laundering and criminality more broadly, profiting from these illegal activities. The results of FATF's fourth round of mutual evaluations reveal that many countries are not sufficiently investigating and prosecuting a range of money laundering activity, including third-party or complex money laundering. Many countries continue to limit their investigations to *self-launderers*: criminals who

launder the proceeds of drug trafficking, fraud, tax evasion, human trafficking or other criminality. While this may address in-house or self-laundering, it does not impact on those specialised in providing criminals with money laundering services. PMLs, professional money laundering organisations and professional money laundering networks can survive law enforcement interdiction against any of its criminal or organised crime group clients, while still standing ready to support the next criminal clientele. Effective dismantling of PMLs requires focused intelligence collection and investigation of the laundering activities, rather than the associated predicate offences of the groups using the services of the PMLs. The dismantling of PMLs, can impact the operations of their criminal clients, and can be an effective intervention strategy against numerous criminal targets.

This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This can include locating investments or purchasing assets; establishing companies or legal arrangements; acting as nominees; recruiting and managing networks of cash couriers or money mules; providing account management services; and creating and registering financial accounts. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML. The analysis shows that PMLs use the whole spectrum of money laundering tools and techniques; however, the report specifically focuses on some of the common mechanisms used to launder funds, such as trade-based money laundering, account settlement mechanism and underground banking.

The project team also examined potential links between PMLs and terrorist financing, however, there was insufficient material provided to warrant a separate section on this topic. The *Khanani* provides the clearest example of a professional money laundering organisation, providing services to a UN designated terrorist organisation. One delegation also noted potential links between a loosely affiliated professional money laundering network and a domestically designated terrorist organisation. However, the vast majority of cases submitted relate to money laundering, rather than terrorist financing.

The non-public version report also explores unique investigative tools and techniques that have proved successful in detecting and disrupting PMLs to guide countries that are seeking to address this issue. The report includes a number of practical recommendations that are designed to enhance the identification and investigation of PML; identify strategies to disrupt and dismantle these entities; and identify steps to prevent PML. Combatting these adaptable PMLs requires concerted law enforcement and supervisory action at the national level, appropriate regulation and effective international co-operation and information exchange. This report emphasises the need for a more co-ordinated operational focus on this issue at a national level, and the importance of effective information sharing between authorities at an international level. The report also identifies the information and intelligence required to successfully identify, map, and investigate PMLs, with the objective of disrupting and dismantling those involved in PML and their criminal clientele.

This report intends to assist authorities at jurisdictional level target PMLs, as well as the structures that they utilise to launder funds, to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.

PROFESSIONAL MONEY LAUNDERING

SECTION I: INTRODUCTION

Purpose, Scope and Objectives

The FATF has conducted a number of studies on money laundering (ML) risks. The resulting reports have usually examined ML threats associated with particular proceeds generating offences or vulnerabilities associated with entities covered under the FATF Standards. This report assesses the threats associated with professional money launderers (PMLs), and does not assess ML vulnerabilities that are covered in other FATF reports. Specifically, the report aims to:

- raise awareness of the unique characteristics of professional money laundering (PML);
- understand the role and functions of those involved in PML;
- understand the business models and specific functions performed by PMLs;
- understand how organised crime groups (OCGs) and terrorists use the services of PMLs to move funds;
- identify relevant ML typologies and schemes;
- develop risk indicators for competent authorities and the private sector that are unique for PMLs; and
- develop practical recommendations for the detection, investigation, prosecution and prevention of PML.

Structure of the Report

Sections II and **III** provide the framework for the report, including key characteristics of PML; differences between individuals, organisations and networks involved in PML; and an explanation of the roles performed by those involved. The aim of these sections is to ensure a consistent dialogue on this topic as countries deepen their understanding of this issue.

Sections IV, **V** and **VI** highlight the main types of dedicated ML networks, including the types of complicit and criminal financial services providers and other professional intermediaries generally involved in PML, and common mechanisms used to launder funds. The types of information within these sections should not be considered finite, as PMLs utilise all ML tools and techniques available to them and continue to adapt their methods to take advantage of regulatory and enforcement gaps.

Methodology

This project was co-led by the Russian Federation and the United States and incorporates input from a variety of delegations across the FATF's Global Network. The project team received submissions from Argentina, Australia, Belgium, Canada, China, Germany, Israel, Italy, Malaysia, the Netherlands, the Russian Federation, Singapore, Spain, the United Kingdom, the United States, EAG Members (Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan), MONEYVAL (Ukraine), MENAFATF (Lebanon), CFATF (Belize) and EUROPOL.

Authorities provided detailed information, including from risk assessments and case examples of various schemes arranged by PMLs, strategic analysis outcomes, information on internal organisational and behavioural aspects of PMLNs and investigative techniques. The report includes select country examples to provide the necessary context.

Input was also gathered at the Middle East and Africa Joint Typologies and Capacity Building Workshop in Rabat, Morocco, from 22-25 January 2018, and input and feedback gathered at the FATF Joint Experts Meeting held in Busan, Republic of Korea, from 1-4 May 2018. The findings of this report also rely on feedback from financial intelligence units (FIUs) and law enforcement agencies (LEAs), based on their experiences in investigating PMLs.

There has been sparse research on this subject. However, the project team did take into consideration previous and ongoing work by the FATF on operational issues, including the 2012 *FATF Guidance on Financial Investigations*, 2013 *FATF Report on ML and TF Vulnerabilities of Legal Professionals* and the 2018 *Joint FATF/Egmont Report on the Vulnerabilities Linked to the Concealment of Beneficial Ownership*.

SECTION II: CHARACTERISTICS OF PROFESSIONAL MONEY LAUNDERING

This section of the report outlines the key characteristics, which make PML unique, and helps to frame the scope of this report. **Section III** then provides a list of specialised services, which include specific roles or functions performed by various individuals. The report has attempted to avoid the use of formal titles (e.g. controller, enabler and facilitator), as multiple and inconsistent terminology is used globally, which leads to confusion when describing these functions. **Section III** provides a business model demonstrating how PMLs generally conduct financial schemes.

Key Characteristics

PML is a subset of third-party ML. The FATF defines third-party ML as the laundering of proceeds by a person who was not involved in the commission of the predicate offence[1]. The main characteristic that makes PML unique is the provision of ML services in exchange for a commission, fee or other type of profit. While the specialisation in providing ML services is a key feature of PMLs, this does not mean that PMLs are not also involved in other activities (including legal businesses).

[1] FATF Methodology 2013, footnote to Immediate Outcome 7.

Similarly, this does not mean that they exclusively only launder illicit proceeds. PMLs also use specialised knowledge and expertise to exploit legal loopholes; find opportunities for criminals; and help criminals retain and legitimise the proceeds of crime.

Given that PMLs are third-party launderers, they are often not familiar with the predicate offence (e.g. narcotics or human trafficking) and are generally not concerned with the origins of the money that is moved. Nonetheless, PMLs are aware that the money that they move is not legitimate. The PML is concerned primarily with the destination of the money and the process by which it is moved. They are used by clients in order to create distance between those perpetrating the crimes and the illicit proceeds that they generate as profit, or because the criminal clients do not have the knowledge required to reliably launder the money without law enforcement detection.

Ultimately, PMLs are criminals, who often operate on a large scale and conduct schemes that are transnational in nature. The term "PMLs" is not intended to include unwitting or passive intermediaries who are exploited to facilitate an ML scheme. Other features of PMLs are that they sometimes operate on a large scale and often conduct schemes that are transnational in nature.

Commissions / Fees

A number of different and overlapping factors affect the fee paid to PMLs or the commission they receive for their services. The fee will often depend on the complexity of the scheme, methods used and knowledge of the predicate offence. The rate may change based on the level of risk that PMLs assume. For example, commission rates are often influenced by the countries or regions involved in the scheme, as well as other factors such as:

- the reputation of the individual PML;
- the total amount of funds laundered;
- the denomination (i.e. value) of the banknotes (in cases involving cash);
- the amount of time requested by a client to move or conceal funds (for example, if the laundering needs to be done in a shorter time period, the commission will be higher); and
- the imposition of new regulation(s) or law enforcement activities.

To obtain commission for their services, PMLs may (i) take commission in cash in advance, (ii) transfer a portion of money laundered to their own accounts or (iii) have the commission integrated into the business transaction.

Advertising / Marketing

Advertising and marketing of services can occur in numerous ways. Often, this involves the PMLs actively marketing their services by 'word-of-mouth' (through an informal criminal network). Criminal links and trust developed through previous criminal engagement also strengthens bonds and can encourage further co-operation. Authorities have also identified the use of posted advertisements for PML services on the Dark Web.

Record Keeping (Shadow Accountancy)

Law enforcement has reported that PMLs often keep a shadow accounting system that contains detailed records with code names. These unique accounting systems may use detailed spreadsheets that track clients (using code names); funds laundered; the origin and destination of funds moved; relevant dates; and commissions received. PMLs may either store their records electronically (e.g. a password-protected Excel spreadsheet) or use paper records. These records represent an invaluable resource for investigators.

Individuals, Organisations and Networks

PMLs can belong to one of three categories:

1. An **individual PML,** who possesses specialised skills or expertise in placing, moving and laundering funds. They specialise in the provision of ML services, which can also be performed while acting in a legitimate, professional occupation. These services can include, but are not limited to, the following: accounting services, financial or legal advice, and the formation of companies and legal arrangements (see *specialised services*, below). Individual PMLs often spread their risks across diverse products, and carry out business activities with several financial specialists and brokers (see examples below).

2. A **Professional money laundering organisation (PMLO)**, which consists of two or more individuals acting as an autonomous, structured group that specialises in providing services or advice to launder money for criminals or other OCGs. Laundering funds may be the core activity of the organisation, but not necessarily the only activity. Most PMLOs have a strict

hierarchical structure, with each member acting as a specialised professional that is responsible for particular elements of the ML cycle (see **Section III**).

3. A **Professional money laundering network (PMLN)**, which is a collection of associates or contacts working together to facilitate PML schemes and/or subcontract their services for specific tasks. These networks usually operate globally, and can include two or more PMLOs that work together. They may also operate as informal networks of individuals that provide the criminal client with a range of ML services. These interpersonal relationships are not always organised, and are often flexible in nature.

These extensive PML networks are able to satisfy the demands of the client by opening foreign bank accounts, establishing or buying foreign companies and using the existing infrastructure that is controlled by other PMLs. Collaboration between different PMLs also diversifies the channels through which illicit proceeds may pass, thereby reducing the risk of detection and seizure.

PMLOs work with OCGs of all nationalities, on a global basis or in a specific region, often acting as a global enterprise. The same PML can be used to facilitate ML operations on behalf of several OCGs or criminal affiliates. They are highly skilled and operate in diverse settings, adept at avoiding the attention of law enforcement. One relevant case has been identified demonstrating that the same money launderers provided services to both OCGs and terrorist organisations (see Box 1, below).

Box 1. Khanani Money Laundering Organisation

The Altaf Khanani Money Laundering Organisation (MLO) laundered illicit proceeds for other OCGs, drug trafficking organisations and designated terrorist groups throughout the world. The Khanani MLO was an OCG composed of individuals and entities operating under the supervision of Pakistani national, Altaf Khanani, whom the US Drug Enforcement Administration (DEA) arrested in 2015. The Khanani MLO facilitated illicit money movements between Pakistan, the United Arab Emirates (UAE), the United States, the United Kingdom, Canada, Australia and other countries. It was responsible for laundering billions of dollars in criminal proceeds annually.

The Khanani MLO offered ML services to a diverse clientele, including Chinese, Colombian and Mexican OCGs, as well as individuals associated with a US

domestically designated terrorist organisation. The Khanani MLO has also laundered funds for other designated terrorist organisations. Specifically, Altaf Khanani, the head of the Khanani MLO and Al Zarooni Exchange, has been involved in the movement of funds for the Taliban, and Altaf Khanani is known to have had relationships with Lashkar-e-Tayyiba, Dawood Ibrahim, al-Qa'ida and Jaish-e-Mohammed. Furthermore, Khanani was responsible for depositing drug proceeds via bank wires from a foreign business account in an effort to conceal and disguise the nature, source, ownership and control of the funds. Khanani conducted transactions, which involved multiple wire transfers from a number of general trading companies. Khanani's commission to launder funds was 3% of the total value of funds laundered.

The Khanani MLO itself was designated by OFAC in 2015 as a "transnational criminal organisation[1]," pursuant to Executive Order 13581. On the same day, OFAC designated the exchange house utilised by the Khanani MLO, Al Zarooni Exchange. In 2016, the US Treasury's Office of Foreign Assets Control (OFAC) designated four individuals and nine entities associated with the Khanani MLO. On October 26, 2016 Altaf Khanani pleaded guilty to federal ML charges. Approximately USD 46 000 in criminal proceeds was also confiscated from Khanani. In 2017, Altaf Khanani was sentenced to 68 months in prison for conspiracy to commit ML.

Extensive law enforcement co-ordination took place between multiple law enforcement agencies from Australia, Canada and the US who all held a different piece of the puzzle. The designation of Al Zarooni Exchange complements an action taken by the Central Bank of the UAE, with assistance from the AML Unit at Dubai Police General Headquarters, which closely coordinated with the DEA prior to the action taken.

Note: 1. Transnational Criminal Organisation (TCO) is a specific technical term used in the US designation process and is synonymous with organised crime group (OCG), the latter of which is used throughout this report.

Source: United States, Australia, Canada, UAE

OCGs use both outsiders and OCG members to perform ML services on behalf of the group. In cases where there is an in-house component of an OCG that is responsible for ML, these members may receive a portion of the proceeds of the group, rather than a fee or commission. The extent to which PMLs get involved in ML schemes depends on the needs of the criminal group, the complexity of the laundering operation that they wish to execute, as well as the risks and costs associated with such involvement.

When OCGs employ the services of PMLs, they often choose PMLs who are acquainted with persons close to, or within, the OCG network. They can be family members or close contacts. They may also be professionals that previously acted in a legitimate capacity, and who now act as:

- accountants, lawyers, notaries and/or other service providers;
- Trust and Company Service Providers (TCSPs);
- bankers;
- MVTS providers;

- brokers;
- fiscal specialists or tax advisors;
- dealers in precious metals or stones;
- bank owners or insiders;
- payment processor owners or insiders; and
- electronic and cryptocurrency exchanger owners or insiders.

OCGs also make use of external experts on a permanent or ad hoc basis. These experts knowingly operate as entrepreneurs and often have no criminal record, which can aid in avoiding detection. These complicit professionals are increasingly present on the criminal landscape, coming together as service providers to support specific criminal schemes or OCGs (see **Section VI**). PMLs can also provide services to several OCGs or criminal affiliates simultaneously, and are both highly skilled at operating in diverse settings and adept at avoiding the attention of law enforcement.

Compartmentalised relationships also exist, particularly within PMLNs, whereby there may be no direct contact between OCGs and the lead actors responsible for laundering the funds In these instances, transactions are facilitated via several layers of individuals who collect the money (see **Section III**) before funds are handed over to PMLs for laundering.

SECTION III: SPECIALISED SERVICES AND BUSINESS MODELS

PMLs can be involved in one, or all, stages of the ML cycle (i.e. placement, layering and integration), and can provide specialised services to either manage, collect or move funds. PMLOs act in a more sophisticated manner and may provide the entire infrastructure for complex ML schemes or construct a unique scheme, tailored to the specific needs of a client.

There are a number of specialised services that PMLs may provide. These include, but are not limited to:

- consulting and advising;
- registering and maintaining companies or other legal entities;
- serving as nominees for companies and accounts;
- providing false documentation;
- comingling legal and illegal proceeds;
- placing and moving illicit cash;
- purchasing assets;
- obtaining financing;
- identifying investment opportunities;
- indirectly purchasing and holding assets;
- orchestrating lawsuits; and
- recruiting and managing money mules.

Roles and Functions

This section identifies numerous roles and functions that are necessary to the operation of PMLs. These specific functions, outlined below, should not be considered an exhaustive list. Depending on the type of PML, an individual may perform a unique function or perform several roles simultaneously. Understanding these roles is important in order to identify all of the relevant players and ensure that all relevant aspects of PMLs are detected, disrupted and ultimately dismantled.

- ***Leading and controlling***: There may be individuals who provide the overall leadership and direction of the group, and who are in charge of strategic planning and decision making. Control over ML activities of the group is normally exercised by a leader, but may also be exercised by other individuals who are responsible for dealing with the funds from the time they are collected from clients until delivery (e.g. arranging the collection of cash and organising the delivery of cash at a chosen international destination). These individuals are also responsible for determining the commission charged and paying salaries to other members of the PMLO/PMLN for their services.
- ***Introducing and promoting***: There are often specific individuals who are responsible for bringing clients to the PMLs and managing communications with the criminal clients. This includes managers who are responsible for establishing and maintaining contact with other PMLOs or individual PMLs that operate locally or abroad. Through the use of these contacts, the PMLO gains access to infrastructure already established by other PMLs.
- ***Maintaining infrastructure***: These individuals are responsible for the establishment of a range of PML infrastructure or tools. This could include setting up companies, opening bank accounts and acquiring credit cards. These actors may also manage a network of registrars who find and recruit nominees (e.g. front men) to register shell companies on behalf of the client, receive online banking logins and passwords, and buy SIM-cards for mobile communication.

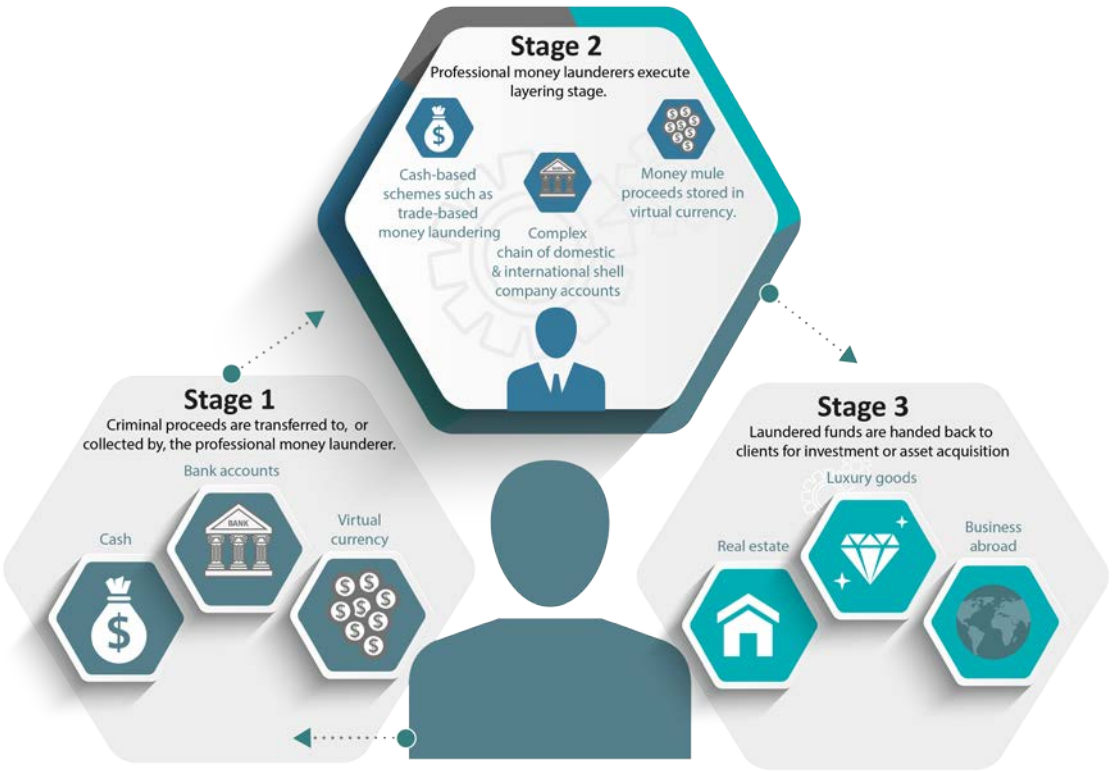
  One example of managing infrastructure is the role of a *money mule herder*, who is responsible for recruiting and managing money mules (e.g. via job ads and via a personal introduction), including the payment of salaries to mules. This salary can be paid either as a fee for their money transfer services or as a one-time payment for their services (see **Section IV** for a wider description of money mule networks and the roles within these specific networks).
- ***Managing documents***: These individuals are responsible for the creation of documentation needed to facilitate the laundering process. In some cases, these individuals are responsible for either producing or acquiring fraudulent documentation, including fake identification, bank statements and annual account statements, invoices for goods or services, consultancy arrangements, promissory notes and loans, false resumes and reference letters.
- ***Managing transportation***: These individuals are responsible for receiving and forwarding goods either internationally or domestically, providing

customs documentation and liaising with transport or customs agents. This role is particularly relevant to TBML schemes.

- ***Investing or purchasing assets***: Where needed, real estate or other assets, such as precious gems, art or luxury goods and vehicles, are used to store value for later sale. Criminals seek assistance in purchasing real estate overseas, and PMLs have been known to use elaborate schemes involving layers of shell companies to facilitate this.
- ***Collecting***: These individuals are responsible for collecting illicit funds, as well as the initial placement stage of the laundering process. Given that they are at the front end of the process, they are most likely to be identified by law enforcement. However, they often leave little paper trail and are able to successfully layer illicit proceeds by depositing co-mingling funds using cash-intensive businesses. These individuals are aware of their role in laundering criminal proceedings (compared to some money mules, who may be unwitting participants in a PML scheme).
- ***Transmitting***: These specific individuals are responsible for moving funds from one location to another in the PML scheme, irrespective of which mechanism is used to move funds. They receive and process money using either the traditional banking system or MVTS providers, and are also often responsible for performing cash withdrawals and subsequent currency exchange transactions.

General Business Model of Professional Money Laundering Networks

Figure 1. Three stages of professional money laundering



In general, financial schemes executed by PMLs consist of three stages:

Stage 1: Criminal proceeds are transferred to, or collected by, PMLs

In the first stage, funds are transferred, physically or electronically, to PMLs or to entities operating on their behalf. The precise manner of introduction of the funds into the ML scheme varies depending on the types of predicate offence(s) and the form in which criminal proceeds were generated (e.g. cash, bank funds, virtual currency, etc.):

Cash: When illicit proceeds are introduced as currency, they are usually passed over to a cash collector. This collector may ultimately deposit the cash into bank accounts. The collector introduces the cash into the financial system through cash-intensive businesses, MVTS providers or casinos, or physically transports the cash to another region or country.

Bank accounts: Some types of criminal activity generate illicit proceeds held in bank accounts, such as fraud, embezzlement and tax crimes. Unlike drug proceeds, proceeds of these crimes rarely start out as cash but may end up as cash after laundering. Clients usually establish legal entities under whose names bank accounts may be opened for the purposes of laundering funds. These accounts are used to transfer money to a first layer of companies that are controlled by the PMLs.

Virtual Currency: Criminals who obtain proceeds in a form of virtual currency (e.g. owners of online illicit stores, including Dark Web marketplaces) must have e-wallets or an address on a distributed ledger platform, which can be accessed by the PMLs.

Stage 2: Layering stage executed by individuals and/or networks

In the layering stage, the majority of PMLs use account settlement mechanisms to make it more difficult to trace the funds. A combination of different ML techniques may be used as part of one scheme. The layering stage is managed by individuals responsible for the co-ordination of financial transactions.

Cash: ML mechanisms for the layering of illicit proceeds earned in cash commonly include: TBML and fictitious trade, account settlements and underground banking.

Bank Accounts: Funds that were transferred to bank accounts managed by PMLs are, in most cases, moved through complex layering schemes or proxy structures. Proxy structures consist of a complex chain of shell company accounts, established both domestically and abroad. The funds from different clients are mixed within the same accounts, which makes the tracing of funds coming from a particular client more difficult.

Virtual Currency: Criminals engaged in cybercrime or computer-based fraud, as well as in the sale of illicit goods via online stores, often use the services of money mule networks (see Section IV). The illicit proceeds earned from these crimes are often held in the form of virtual currency, and are stored in e-wallets or virtual currency wallets that go through a complex chain of transfers.

Stage 3. Laundered funds are handed back over to clients for investment or asset acquisition

In the last stage, funds are transferred to accounts controlled by the clients of the PML, their close associates or third parties acting on their behalf or on behalf of affiliated legal entities. The PML may invest the illicit proceeds on behalf of these clients in real estate, luxury goods, and businesses abroad (or, in some cases, in countries where the funds originated from). The funds can also be spent on goods deliveries to a country where the funds originated or to a third country.

SECTION IV: TYPES OF DEDICATED ML ORGANISATIONS AND NETWORKS

As mentioned in the previous sections, PMLs may move funds through dedicated networks, utilising multiple mechanisms to move funds. These networks, often used during the placement and layering stages in the laundering cycle, are able to quickly adapt and adjust to shifting environmental factors (such as new regulation) and law enforcement activities. PMLs may also provide detailed guidance to assist with the entire ML scheme and often sell "packages" that contain the instruments and services required to facilitate an ML scheme. This section describes the key types of dedicated ML organisations and networks identified through an analysis of case studies: (i) money transport and cash controller networks; (ii) money mule networks; (iii) digital money and virtual currency networks; and (iv) proxy networks.

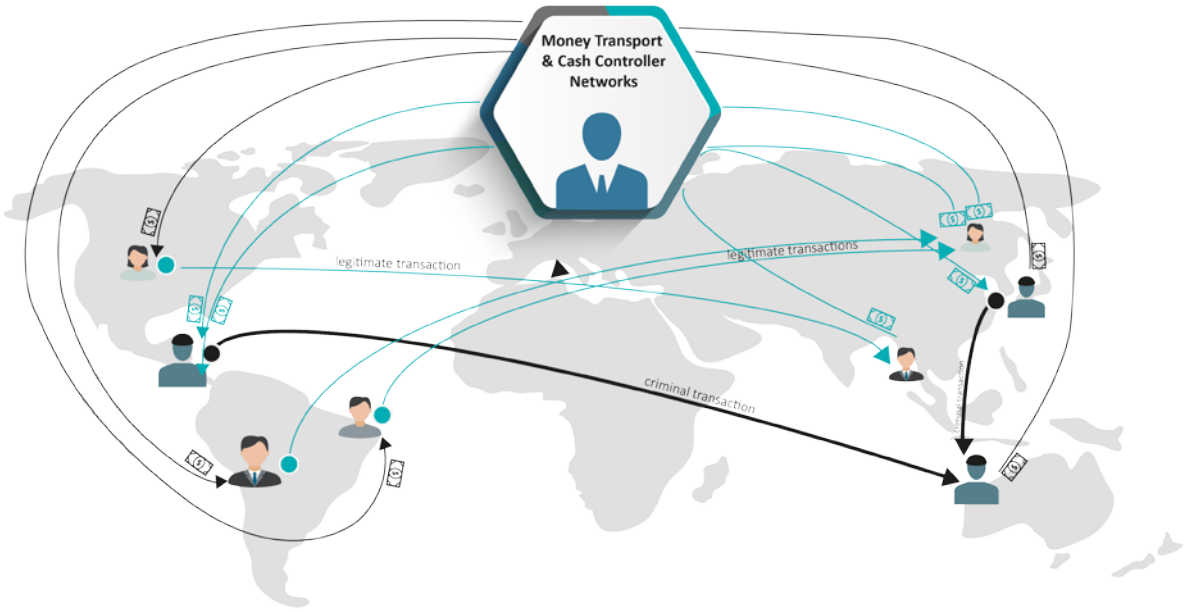
Money Transport and Cash Controller Networks

Criminals and OCGs that generate significant amounts of cash often use the services of cash controller networks that are capable of transferring vast sums of cash on their behalf. These international controller networks have the capacity to receive, hand over and transfer criminal proceeds, while charging a processing fee. Generally the structure of these networks consists of individuals who *control, co-ordinate, collect and transmit illicit funds,*[2] and who operate together to negotiate deals with the OCG.

Cash controller networks often orchestrate the laundering of the proceeds of crime for multiple OCGs located worldwide through an account settlement system, whereby illicit proceeds are substituted for legitimate funds. The ML technique employed sometimes involves the transfer of criminal funds through the accounts of unwitting customers who receive funds or payments from abroad. In this scheme, legal funds, which are to be transferred into the bank account of an unwitting third party, are substituted by the launderer with the illicit proceeds of the OCG. The launderer deposits the money in amounts under the reporting threshold to avoid detection.

[2] See roles and functions defined in Section III

Figure 2. Money Transport and Cash Controller Network



Amounts deposited do not immediately match the overall sums of illicit proceeds. However, in the long term, the value of illicit proceeds collected against the value of deposits tends to be equivalent. Where this is not the case, the PML may resort to other trade-based techniques, such as fake or over invoicing, in order to legitimise the movement of funds between two or more jurisdictions, to balance the system. This technique allows the PML to oversee payments made in another country, without the risk of being detected by holding bank accounts in their own name(s).

If an international cash controller network works with criminals and OCGs operating in different countries, it may easily avoid conducting cross-border transfers of funds, with the support of an account settlement mechanism (see Section V). The chart, below, illustrates the operations of an international cash controller network in four different situations.

Box 2. Cash Controller Network and Account Settlement Scheme

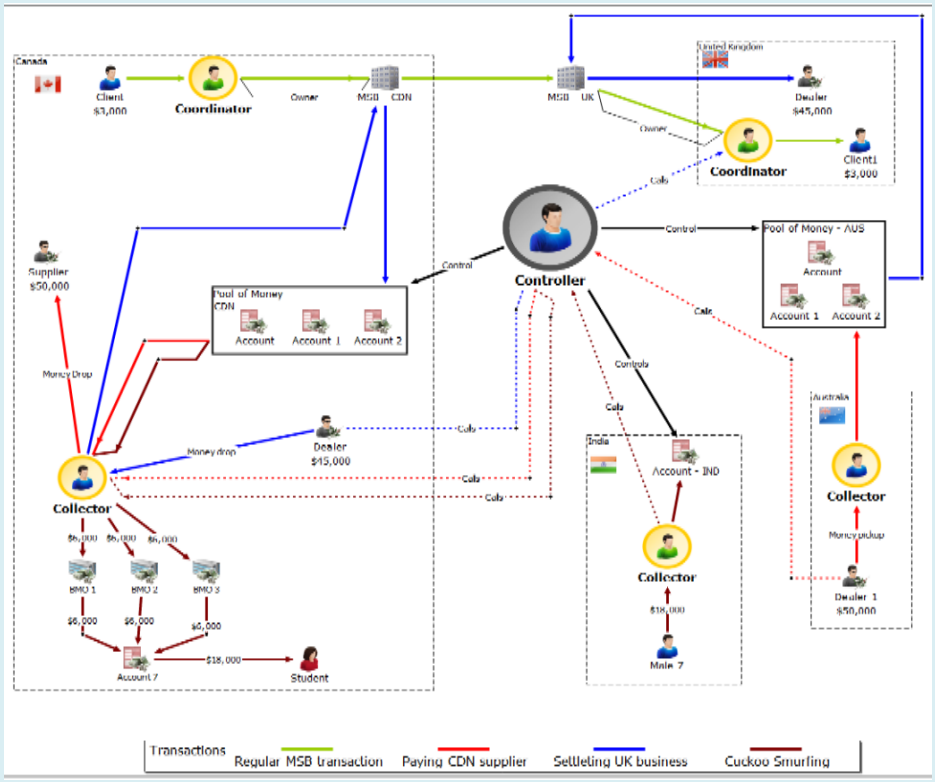
USD 3 000 GREEN: Basic transaction. The Canadian client wants to send money to another client in the UK. It is conducted through the MVTS provider's intermediary.

USD 50 000 RED: An Australian dealer wants to pay its Canadian supplier. The dealer contacts the controller to arrange the transfer. The controller instructs the collector to pick up money. The money is now part of a pool of money in that country under the control of the controller. The controller instructs his Canadian collector to take money from his Canadian pool of money to conduct a money-drop.

USD 45 000 BLUE: The Canadian dealer wants to settle an account in the UK.

The dealer contacts the controller and arranges a pick-up. The collector picks up the money and is instructed to deliver it to a complicit transmitter to place the money into bank accounts (structuring). This increases the Canadian pool of money. The controller then takes money from the UK pool and instructs the UK collector to deliver the money.

USD 18 000 MAROON: A father in India wants to send money to his daughter in Canada. The funds are sent through a hawala network[1]. The collector secures the contract for the controller. The controller then directs his Canadian collector to disperse deposits into the individual`s bank account. He visits three different branches to structure the deposits into the account.



Note: 1. For further information about hawala, see FATF, *Role of Hawala and Other Similar Service Providers in ML and TF*, October 2013

Source: Australia

The laundering of criminal proceeds generated in cash may include the physical transportation of bulk cash. Recent cases show that services to transport cash are also being outsourced to specialised cash transportation networks that are responsible for collecting cash, transporting it to pre-determined locations and facilitating its placement in the financial system. One of the recent examples of efforts taken to combat cash transportation networks that provide services to drug trafficking organisations operating in Europe is EUROPOL's Operation Kandil. The network was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and transporting this cash to Germany, where it was placed into the financial system through the purchase of second-hand cars, spare parts and equipment.

Box 3. Operation Kandil – Use of Cash Courier Network

In 2016, authorities from Germany, supported by EUROPOL experts, took action against an Iraqi OCG (based in Germany) that was suspected of performing ML services for international heroin traffickers. The operation was preceded by extensive and complex criminal investigations, supported by EUROPOL, which coordinated the law enforcement authorities in France, Spain, Germany and the Netherlands, mirrored by EUROJUST's co-ordination of judicial authorities.

This criminal syndicate, composed mainly of Iraqi nationals, was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and laundering these funds to the Middle East through Germany, with an estimated total amount of EUR 5 million already laundered.

The criminals' modus operandi involved the use of cash couriers traveling by car to pick up dirty cash all over Europe. This was followed by the use of TBML techniques to transmit the value to the Middle East, primarily through the shipment of second-hand cars; heavy machinery and construction equipment purchased in Germany and exported to Iraq, where the goods were ultimately resold in exchange for clean cash.

The OCG was then able to make use of MVTS services and unregulated financial channels (the hawala system) to integrate and further transfer funds into the regulated financial system. This left virtually no paper trail for law enforcement.

Professional service providers, such as solicitors, accountants and company formation agents, provided the skills and knowledge of financial procedures necessary to operate this scheme. Although, few groups are known to provide these services, they launder large amounts of money, and have a considerable impact on the ability of other OCGs to disguise and invest criminal proceeds. These syndicates are a significant obstacle to tracing criminal assets.

Source: EUROPOL (Germany)

Money Mule Networks

One of the significant elements of many PML schemes is the use of money mules. Money mules are people who are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. Money mules may be willing participants and are often recruited by criminals via job advertisements for 'transaction managers' or through online social media interactions. Money mule recruiters are also known as mule 'herders.' Money mules may be knowingly complicit in the laundering of funds or work unwittingly, or negligently, on behalf of a PMLN or OCG. Cyber criminals tailor their recruitment techniques based on the prospective mule's motivations. For example, these criminals will also offer off-the-record cash payments and free travel to incentivise and recruit "witting" mules motivated by easy money and free travel.

Box 4. Use Of Money Mules to Launder Criminal Proceeds

Person A was recruited by a Nigerian syndicate to receive money in her bank accounts. She was promised commissions of up to SGD 5 000 (EUR 3 160) for each transaction. Person A received criminal proceeds from fraud committed in the US and the Bahamas into her bank accounts. Most of the funds were transferred out or withdrawn within a few days of receipt, upon instructions of the Nigerian-based OCG.

Not only did Person A serve as a receptacle for illicit proceeds, she also recruited two other money mules. The control of the mules' bank accounts allowed her to obscure the locations of the illicit proceeds through layering, and enabled her to evade detection as the funds were spread out over multiple accounts. Through this network, Person A and her money mule network received a total of 12 fraudulent wire transfers, amounting to SGD 5 million (EUR 3 16 million) from overseas victims into their bank accounts in Singapore, within a period of six weeks.

Person A was convicted and sentenced to 72 months' imprisonment for receiving stolen property and ML offences.

Source: Singapore

PMLs frequently recruit money mules from diaspora networks and ethnic communities. A sizeable amount of money mule transactions are linked to online illicit stores and cybercrime, such as phishing, malware attacks, credit card fraud, business e-mail compromise and various types of other scams (including romance, lottery and employment scams).

Some money mules are unaware that they are being used to facilitate criminal activity. Unwitting mules are used by OCGs to cash counterfeit checks and money orders or purchase merchandise using stolen credit card numbers or other personal identification information. In some cases, the mules may suspect that the source of the money that they are moving is not legitimate. Such wilfully blind money mules often use income earned to supplement their regular income because they are facing financial difficulties or are motivated by greed.

In the past, money mules have been viewed as low-level offenders, transferring small amounts of cash. However, organised, sophisticated money mule schemes have evolved as a PML mechanism. These money mule networks are controlled by a hierarchical structure, and are well-resourced and highly effective in laundering funds. Money mule networks are usually associated with OCGs that operate cross-border, particularly those involved in cybercrime and the sale of illicit goods through online stores. Typically, these schemes involve criminals that create apparently legitimate businesses, hiring unsuspecting individuals whose jobs involve setting up bank accounts to receive and pass along supposedly legitimate payments. In reality, these unsuspecting individuals act as money mules, processing the criminals' illicit proceeds and wiring them to other criminals.

Money mule networks have been used to open numerous individual bank accounts locally as well as in global financial centres to facilitate the movement of criminal

proceeds. Bank accounts, opened by the mules, serve as the initial layering stage in the laundering process. This indicates that criminals still find the combination of money mule accounts, cash withdrawals and wire transfers to be an effective way to layer proceeds.

Box 5. Avalanche Network

Avalanche is an example of a criminal infrastructure dedicated to facilitating privacy invasions and financial crimes on a global scale. Avalanche was a hosting platform composed of a worldwide network of servers that was controlled via a highly organised central system. This cyber network hosted more than two dozen of the world's most pernicious types of malware and several large scale ML campaigns.

The Avalanche network, in operation since at least 2010, was estimated to serve clients operating as many as 500 000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of USD worldwide.

The Avalanche network offered cybercriminals a secure infrastructure, designed to thwart detection by law enforcement and cyber security experts. Online banking passwords and other sensitive information stolen from victims' malware-infected computers was redirected through the intricate network of Avalanche servers and ultimately to back-end servers controlled by the cybercriminals. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive, dark web criminal forums.

The types of malware and money mule schemes operating over the Avalanche network varied. Ransomware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of crypto-currency) to the cybercriminal. Other malware, such as GozNym, was designed to steal sensitive online banking credentials from victims in order to use those credentials to initiate fraudulent wire transfers from the victims' bank accounts.

The ML schemes operating over Avalanche involved highly organised individuals, who controlled server networks and money mules, which were a crucial part of the criminal network. In some cases, the leaders would use a network of individuals to open bank accounts in major global financial hubs to facilitate wire transfers. The mules were often sponsored by the leader of a particular, country-based network and brought to the US, or, they were unwitting individuals who were recruited. The mules purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

Source: United States

Digital Money and Virtual Currency Networks

PMLs also arrange schemes that allow criminals to cash out proceeds generated in virtual currency via online illicit markets (e.g. Dark Web drug-trafficking marketplaces). In many cases, payments for illicit drugs purchased online are transferred to e-wallets held in fiat currency or in virtual currency (e.g. Bitcoin). Afterwards, virtual currency is transferred through a complex chain of e-wallets, which may include the use of mixers and tumblers to further enhance the anonymity of the virtual currency transactions. Funds are then sent back to the e-wallet of the OCG, and subsequently transferred to bank cards and withdrawn in cash.

Financial instruments are issued under the names of money mules (usually students who obtain a bank card and then sell the bank card to criminals for a fee, knowing nothing about its subsequent usage and associated criminal activities). Money mules employed by the PML conduct ATM withdrawals in a coordinated manner, and then give the money to members of the client OCGs.

There are cases when the same financial scheme and the network of individuals worked for the benefit of multiple OCGs operating on the Dark Web. These persons then re-distributed funds to the respective OCGs.

Box 6. Laundering Proceeds from Dark Web Drug Stores

The Russian Ministry of Internal Affairs and FIU conducted an investigation into OCGs that sold drugs via the Dark Web. Customers could choose two ways to pay and transfer funds for their order either by an indicated e-wallet, held in fiat currency, or to a Bitcoin address. The majority of clients preferred using e-wallets held in fiat currency, instead of Bitcoins.

The financial scheme for the drug stores was arranged and managed by a financier and his network. The ML network was responsible solely for moving funds and had no links to drug trafficking. Numerous e-wallets and debit cards were registered in the names of front men. This usually involved students who issued e-wallets and credit cards, and then sold them to members of the ML network, unaware of the criminal purpose of their further usage. Some e-wallets were used at the placement stage of the laundering process and had a limit of USD 300 000, while other e-wallets had a higher limit.

To simplify the ML process, the network's IT specialists developed a 'transit-panel' that had a user-friendly interface and was accessible via the TOR browser. The transit panel automatically switched between e-wallets that were used for drug payments. Digital money was automatically moved through a complex chain of different e-wallets.

Money from e-wallets was then transferred to debit cards and withdrawn in cash via ATMs. Withdrawals via ATMs were conducted by "cash co-ordinators" who had multiple debit cards at hand (all cards were issued on the names of straw men[1]). Afterwards, cash was handed over to interested parties. In order to increase the complexity, proceeds were re-deposited on a new set of debit cards and transferred to the OCGs (usually located abroad).

In similar schemes, funds from e-wallets were exchanged into Bitcoins via virtual currency exchangers. The Bitcoins were used to pay salaries to members of the drug trafficking organisation. This included low-level members, such as small dealers and runners who facilitated the sale of drugs. The same financier worked with multiple owners of the Dark Web stores, distributing the laundered funds to the respective OCGs.

Note: 1. The term "straw men" refers to informal nominee shareholders and directors who are being controlled by the actual owner or controller of the company.

Source: The Russian Federation

Proxy Networks

Proxy networks are PMLs who supply a type of banking service to OCGs, generally through the use of multi-layered transfers via bank accounts. These specialised services offer all of the advantages that come with moving funds globally via the legitimate financial sector. The main task of these proxy networks is to move client funds to the final, pre-determined destination and to obfuscate the trail of the financial flows. In many cases, these schemes are supported by TBML mechanisms.

PML schemes that are arranged with the use of bank accounts consist of multiple layers of shell companies in different jurisdictions, which have been established purely to redistribute and mix funds from various sources. These shell companies could be located in the country where the predicate offence occurred, transit countries or countries where the final investment of funds is conducted. This scheme is designed to make the portion of funds that belong to a client untraceable. In most cases, laundered funds are transferred to a client's personal bank account(s), affiliated companies or foundations under their control, or handed over to them as physical cash.

In general, a cross-border ML scheme arranged by a proxy network has the following structure:

- **Step 1:** Clients' funds are transferred to accounts opened in the name of shell companies controlled by the PML, often through the use of legal entities controlled by them, or entities operating on their behalf. If the criminal proceeds were obtained in cash, controllers arrange to collect and deposit the cash into the accounts of PML-controlled shell companies.
- **Step 2:** Funds are moved through a complex chain of accounts established by domestic shell companies under fictitious contracts. The funds from different clients are mixed within the same accounts, which makes it difficult for investigators to trace the funds coming from a particular client.
- **Step 3:** Funds are transferred abroad under fictitious trade contracts, loan agreements, securities purchase agreements, etc. In most cases, accounts of the first-level layer of foreign companies are controlled by the same money launderers, who facilitated Step 1, or by foreign PMLs who act in collaboration with the domestic money launderers.
- **Step 4:** Funds are moved through a complex chain of international transfers. The ML infrastructure used (i.e. accounts set up by shell companies) is typically used to channel money that comes from all over the world. These

international money transfers often demonstrate similar geographical patterns.

- **Step 5:** Funds are returned to the accounts controlled by the initial clients, their close associates or affiliated legal entities and arrangements. Alternatively, the PML will purchase goods and services on behalf of the OCG. PMLs that arrange these schemes provide different reasons to justify or legitimise the wire transfers they conduct. These may include trade in various goods and services, import/export services, loans, consultancy services or investments. PMLs look for loopholes and other possible purposes for payments that give the veneer of legitimacy to these transactions. Bank accounts are chosen to make the activity appear legitimate, and to avoid suspicious transactions reporting and/or instances where the transaction are blocked by financial institutions. For example, PMLs use accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large), in accordance with the sums laundered.

Box 7. Facilitating the Laundering of Proceeds from Bank Fraud

In 2015, Russian law enforcement authorities, in co-operation with the FIU and the Central Bank, disrupted a large-scale scheme to embezzle funds and subsequently conduct illicit cross-border transfers.

During the course of the investigation, it was established that OCG members assisted in stealing assets from a number of Russian banks. Typically, the bank management team knowingly granted non-refundable loans and conducted fictitious real estate deals, which led to the bank's premediated bankruptcy. Illicit proceeds were then moved abroad via accounts of shell companies.

Law enforcement authorities and the FIU, in co-operation with foreign counterparts, detected a wider scheme of illicit cross-border money transfers that was used to move proceeds from several predicate offences abroad. Funds were moved via accounts of domestic shell companies and offshore companies (registered in the UK, New Zealand, Belize and other jurisdictions), with their accounts held by banks in Moldova and Latvia, under the pretext of fictitious contracts and falsified court decisions.

One of the major launderers of this scheme received profits for his services in his own personal bank accounts from two offshore companies that were used in the scheme.

The OCG consisted of more than 500 members. Law enforcement authorities seized more than 200 electronic keys of online bank accounts; more than 500 stamps of legal entities; shadow accountancy documents, copies of fictitious contacts; and cash. Bank managers and other complicit individuals were arrested.

Source: The Russian Federation

Social engineering frauds and other types of Internet-based fraud are often a source of illicit proceeds that may be laundered through a proxy network:

Box 8. Creating Infrastructure to Launder Funds

This investigation was conducted by a specially designated Israeli Task Force for PML investigations, which includes members from the Israeli Police, Tax Authority, IMPA (FIU) and Prosecution. The investigation also involved the co-operation of LEAs in another country.

The suspects of the investigation were criminals conducting massive fraud and extortion, as well as PMLs, who assisted the predicate offenders in laundering the proceeds of crimes. Funds were laundered using shell companies established in Europe and the Far East. "Straw men," couriers and hawala-type services. The companies were established in advance in countries that were less susceptible for illegal activity in the eyes of the fraud victims.

The PML built the infrastructure that enabled the ML activity, which in turn was part of a global ML network. The PML, through the use of other individuals, opened foreign bank accounts, established foreign companies, and also used a repatriation network of foreign immigrants to move funds as part of the ML network.

The suspects transferred fraudulent proceeds to bank accounts opened in the name of the shell companies and straw men. The funds were then transferred to other bank accounts in the Far East and immediately the suspects withdrew money in cash by using couriers, hawala networks and MVTS providers in Israel to transfer the funds to their final destinations.

During the investigation, an Israeli suspect (one of the PMLs) was arrested by an LEA of a third country. This assisted the investigation in understanding the modus operandi of the PMLN. It was established that the PML of the network was also able to provide bank accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large in accordance with the sums laundered). The bank accounts were thus chosen to make the activity look legitimate, avoiding unusual activity reports and/or instances where the transaction is blocked by the financial institution concerned.

Source: Israel

Proxy networks that facilitate cross-border movement of funds often tie into a wider network of other PMLs in several countries for the purpose of moving and laundering funds to and from the country where the predicate offence took place. PMLs who facilitate the outgoing flow of funds from the country where the predicate offence was conducted are typically part of a broader, global ML network that specialises in moving illicit proceeds around the globe. Some third-party money launderers, identified by responding countries, also acted through collaboration with other PMLs operating abroad which provided ML services at their request. The use of a global network of PMLs, located in different countries, as well as using different methods to transfer funds internationally, ensures the diversification of financial transactions and helps to limit the risk of detection. An analysis of proxy networks shows that PMLs may change their *modus operandi* and employ different contacts as needed.

Box 9. Large-Scale International Money Laundering Platform

A financial investigation was initiated into the embezzlement of public funds and suspected corruption, which led to the detection of a large-scale international ML platform that was used to move funds originating from different sources.

The proceeds of crime were moved to accounts of shell companies held with banks in Latvia, Cyprus and Estonia. The criminal proceeds were further transferred to accounts of companies controlled by the beneficiary's close associates and then moved back to Russia. Further investigation revealed that various companies used the same channel to move the funds.

A criminal proceeding on articles "Fraud", "Arrangement of organised criminal group" and "Money Laundering," according to the Criminal Code of the Russian Federation, was opened. The Central Bank of the Russian Federation withdrew the license of the Russian bank that facilitated frequent cross-border money transfers under fictitious contracts for violations of AML legislation. The European Central Bank also withdrew the license of a Latvian bank that facilitated the redistribution of criminal proceeds. A significant portion of funds was frozen on the accounts held by Latvian banks.

While the investigation of the case started with a particular predicate offence, it led to the identification of a wide international PML scheme that was used to move funds originating from various crimes. There are also indications that clients from other countries used this ML scheme. In a demonstration of the interconnectedness of PML, some companies involved in this scheme have financial links with a UAE company designated by the US in relation to the Altaf Khanani Money Laundering Organisation,[1] described in Box 1.

Note: 1. See Section III for the case study on this MLO.

Source: The Russian Federation

PML schemes and infrastructure can also be used to launder funds and to facilitate large-scale tax evasion schemes. In such schemes, multiple layers of shell companies may be used between the importer and producer of goods that are located abroad. Funds used for the purchase of foreign goods thus go through a complex chain of transactions, with only one portion of these funds used for the import deal. The rest is directed to accounts controlled by beneficiaries.

Proxy networks also use layering schemes to transform illicit proceeds generated within the financial system into cash. This is mostly arranged for those clients who need to move criminal proceeds from bank accounts to physical cash. The majority of such clients are involved in public funds embezzlement, tax fraud and cyber fraud schemes. At the final stage, funds are transferred to corporate bank cards, followed by subsequent cash withdrawals. The number of shell companies and personal bank accounts involved may exceed several thousands. This limits the risk of detection and diversifies possible losses.

In some cases, cash withdrawals may be conducted abroad. In one case, funds were channelled to accounts of companies registered in the Middle East, with subsequent

cash withdrawals via exchange houses. Cash was then transported back to the country of origin and declared on the border as profits from legitimate business activities in the Middle East, which were intended to be used for the purchase of real estate.

SECTION V: SUPPORTING MECHANISMS USED BY PROFESSIONAL MONEY LAUNDERERS

PMLNs use a wide variety of ML tools and techniques. Among the most significant mechanisms are TBML, account settlement mechanisms and underground banking.

Trade-Based Money Laundering (TBML)

TBML is defined as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin."[3] There are various TBML variations that can be employed by PMLs. These include:

- *The purchase of high-value goods using the proceeds of crime*, followed by the shipment and re-sale of goods overseas;
- *The transfer of funds which purport to be related to trade*, or to the purchase of goods that are ultimately never shipped or received (also known as "phantom shipments");
- *Falsifying the number and/or value of goods being shipped* to be higher or lower than the corresponding payment, allowing for the transfer or receipt of the value of proceeds of crime (also known as over or under-invoicing);
- *Using the proceeds of crime to purchase goods for legitimate re-sale*, with payment for goods made to drug traffickers/distributors by legitimate business owners (e.g. the Black Market Peso Exchange - BMPE); and
- *Using Money (Peso) Brokers*, who are third parties that seek to purchase drug proceeds in the location where illicit proceeds are earned by drug cartels (e.g. Colombia, Mexico) at a discounted rate. Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the drug trafficking organisation or the money brokers who serve as PMLOs.

Box 10. ML Network, Operating as a Trade-Based ML Scheme1

Project OROAD was a joint task force financial investigation, launched from a drug investigation into ML activities of a suspicious group[2]. Information received from FINTRAC helped identify a complex TBML where two of the group's central figures hired 10 nominees to establish 25 shell companies. The shell companies were opened using names across a diverse number of

[3] FATF, 2006.

industries: landscaping, interior design, electronics, metal recycling, plastics recycling, construction supplies, beauty supplies, etc.

The laundering network included legitimate businesses, operating in the financial and real estate sectors, as well as a small financial company, which was complicit in laundering the funds. The money launderer provided his accomplice at the financial company with large bags of cash, which were then deposited into business accounts in the name of shell companies. This continued until the accounts were closed by the financial institution that held the shell company's accounts, due to a high volume of suspicious transactions.

Investigators believe the ML group used a TBML scheme. The ML operation and the network of shell companies were largely centred on a logistics company. One of the money launderers was seen leaving the logistics company location with large bags of bulk cash, which were believed to be the proceeds of drug sales. The money launderer used nominees to make multiple cash deposits into their personal and business accounts.

The money launderer instructed nominees to either i) transfer funds back to the logistics company; or ii) transfer funds to other business accounts, held by nominees located in Canada, China, Panama and the US. Funds were sent by wire transfer, bank draft or cheque, some of which were then returned to the logistics company. In each case, the money launderer used fraudulent invoices to account for the proceeds of drug sales so that they could be more easily integrated into the financial system.

Investigators believe that some of the funds were transferred back to the Mexican drug trafficking organisation and to other companies controlled by the drug trafficking organisation in China, Mexico and the US. In some cases, funds were used for to purchase goods located in Panama or Mexico. The ringleaders in Canada established companies in these countries in attempts to make the transfers seem legitimate. The purchased goods were then shipped to other foreign countries for sale. Once the purchased goods arrive at the destination country, they were sold, and the proceeds of the sale (in the destination country's currency) were then transferred to the drug trafficking or ML organisation to provide the criminals with "clean" funds, laundered through TBML.

Notes:

1 See case study "Operation Snake" in Section III, which involves another professional ML network using a TBML and MVTS scheme

2 The investigation also revealed a number of bulk cash transactions between the ring and illegal money brokers; however, the focus here is on the ML ring.

Source: Canada

PMLs may also create and use false documentation, layer related financial transactions and establish shell and/or shelf companies to facilitate purported trade transactions. By using TBML mechanisms, PMLs can break the link between the predicate crime and related ML, making it difficult to associate the criminals with the ML activity.

Box 11. Venezuelan Currency Smuggling Network

During 2015, 10 limited liability companies established by a single person in Spain processed more than 110 000 transactions, totalling EUR 22.4 million, through mobile payment "point of sale (POS)" terminals. Nine of these companies were purportedly active as travel agencies, eight shared the same registered offices and six had the same associate and director.

The POS terminals held by these companies exclusively accepted payment cards issued by the Venezuelan government (Comisión de Administración de Divisas - CADIVI). Given strict currency controls in Venezuela, residents can only obtain foreign currencies when traveling abroad. Therefore, a maximum of USD 3 000 at a rate of 6.3 bolivars per dollar can be exchanged. This led to a large currency exchange fraud called "el raspao," where Venezuelan residents accessed euros or dollars, under the false pretence of a journey abroad. The payment cards issued by the CADIVI, at the official exchange rate, were debited abroad while drug traffickers received the counter value in cash, in euro or dollar notes, which was then smuggled back into Venezuela and sold on the black market at a rate of about ten times the official exchange rate. Authorities in Luxembourg suspect that the payment cards issued by CADIVI were smuggled in bundles to Spain and swiped through the POS terminals of complicit traders who operated through Spanish front companies.

Drug traffickers and Colombian cartels are believed to have taken advantage of this currency smuggling network in order to repatriate the proceeds generated in cash through drug sales in Europe back to South America. These criminals washed their illicit cash by handing it out to Venezuelan currency traffickers. Once processed, the debited amounts were credited to linked bank accounts. These bank accounts had International Bank Account Numbers (IBANs), issued by a former Luxembourg-licensed electronic money remitter.

AML investigations by the regulator and the financial intelligence unit (FIU) revealed that the Luxembourg electronic money remitter did not manage these accounts itself, as stipulated in regulation, but handed them over to a Bulgarian-licensed electronic money remitter, which used the accounts for its own customers. The POSs were sold to the Spanish front companies by the Bulgarian electronic money remitter. Additionally, the Spanish front companies applied for hundreds of withdrawal cards (most front companies had more than 10 withdrawal cards each), issued by the Bulgarian electronic money remitter, in order to allow them to withdraw cash from their accounts. About 106 000 withdrawals, totalling more than EUR 20 million were made at ATMs situated in Colombia. These withdrawals did not comply with the daily, weekly and monthly limits as laid out in the general terms and conditions of the Bulgarian electronic remitter. Authorities in Luxembourg were not aware of any related suspicious transaction reports that were reported to the Bulgarian FIU. The Luxembourg and Bulgarian electronic remitters were held by the same beneficial owner. Commissions received by the Bulgarian electronic remitter on the operations totalled as much as EUR 1.9 million, or 9 % of the amounts processed through the POSs.

Source: Luxembourg

Account Settlement Mechanisms

PMLNs can facilitate the settlement of accounts between multiple OCGs. They may do this for OCGs operating in different countries that generate proceeds from cash and hold funds within bank accounts. A PML may, for example, simultaneously provide ML services to criminals who have cash and want to send funds to bank accounts in other countries, and to criminals who have money in their bank accounts but need cash (e.g. to pay their networks and workers). This *modus operandi* is called an *account settlement mechanism*.

The case, below, illustrates how a PMLO accepted and moved cash by car to Belgium, as part of an account settlement mechanism.

Box 12. Money Laundering as Part of an "Account Settlement Scheme" Between Various Criminal Organisations

Several Belgian corporate customers transferred funds to the accounts of Belgian construction or industrial cleaning companies and their managers. These companies had a similar profile: they operated in the same industry, the managers were often from the same country, the articles of association were copied with slight modifications, and the companies' financial health was poor. Some companies had already gone bankrupt or no longer complied with their legal requirements.

Funds were channelled through different accounts: Part of the funds credited to the accounts was withdrawn in cash, presumably to pay workers. Another part of the funds were transferred to companies located abroad, in Europe and in Asia.

The funds transferred to Europe were credited to the accounts of other companies in the same industry. Often no explanation was provided for these transfers, even though the scale was significant. The references accompanying these transfers, if any, were vague. The majority of the funds were subsequently withdrawn in cash.

The funds transferred to Asia, mainly China and Hong Kong, were credited to the accounts of limited liability companies, which were not linked to the construction or industrial cleaning industry in any way.

Information received from a counterpart FIU revealed links with a criminal organisation involved in drug trafficking. This organisation, which held large amounts of cash, used an organisation that laundered the funds and transported the cash to Belgium by car. In Belgium, intermediaries then handed over the cash to various companies in Belgium that required cash to carry out their activities.

Based on this information, authorities have concluded that the Belgian construction and industrial cleaning companies involved in this case were part of an account settlement scheme. The cash proceeds of drug trafficking were used to pay illegal workers of Belgian companies.

Source: Belgium

Underground Banking and Alternative Banking Platforms

Underground banking is one tool often used by PMLs. This mechanism is used, with the goal of bypassing the regulated financial sector and creating a parallel system of moving and keeping records of transactions and accountancy.

Box 13. Investigation of Massive Underground Banking System

Subject X and his network of associates in British Columbia, Canada, are believed to have operated a PMLO that offered a number of crucial services to Transnational Criminal Organisations including Mexican Cartels, Asian OCGs, and Middle Eastern OCGs. It is estimated that they laundered over CAD 1 billion per year through an underground banking network, involving legal and illegal casinos, MVTSs and asset procurement. One portion of the ML networks illegal activities was the use of drug money, illegal gambling money and money derived from extortion to supply cash to Chinese gamblers in Canada.

Subject X allegedly helped ultra-wealthy gamblers move their money to Canada from China, which has restrictions on the outflow of fiat currency. The Chinese gamblers would transfer funds to accounts controlled by Subject X and his network in exchange for cash in Canada. However, funds were never actually transferred outside of China to Canada; rather, the value of funds was transferred through an Informal Value Transfer System. Subject X received a 3-5% commission on each transaction. Chinese gamblers were provided with a contact, either locally or prior to arriving, in Vancouver. The Chinese gamblers would phone the contact to schedule cash delivery, usually in the casino parking lot, which was then used to buy casino chips. Some gamblers would cash in their chips for a "B.C. casino cheque", which they could then deposit into a Canadian bank account. Some of these funds were used for real estate purchases. The cash given to the high-roller gamblers came from Company X, an unlicensed MVTS provider owned by Subject X. Investigators believe that gangsters or their couriers were delivering suitcases of cash to Company X, allegedly at an average rate of CAD 1.5 million a day. Surveillance identified links to 40 different organisations, including organised groups in Asia that dealt with cocaine, heroin and methamphetamine.

After cash was dropped off at Company X, funds were released offshore by Subject X or his network. Most transactions were held in cash and avoided the tracking that is typical for conventional banking. Subject X charged a 5% fee for the laundering and transfer service. As the ML operation grew, the money transfer abilities of Company X became increasingly sophisticated to the point where it could wire funds to Mexico and Peru, allowing drug dealers to buy narcotics without carrying cash outside Canada in order to cover up the international money transfers with fake trade invoices from China. Investigators have found evidence of over 600 bank accounts in China that were controlled or used by Company X. Chinese police have conducted their own investigation, labelling this as a massive underground banking system.

Source: Canada

An *alternative banking platform (ABP)* is an alternative bank that operates outside the regulated financial system. However, an ABP may use the facilities of the formal banking system, while creating a parallel accountancy and settlement system. ABPs are a form of shadow banking that make use of bespoke online software to provide banking services, without the regulated and audited customer due diligence checks. They are an effective way to transfer the ownership of money anonymously and provide banking services within a bank account across a number of individuals, without being reflected in traditional banking transactions. Usually, it is supported with special software that can encrypt traffic, manage transactions between accounts within the same platform, apply fees and assist with interaction with the outside financial system.

Box 14. Alternative Banking Platforms

An alternative banking platform (ABP) was used to assist organised crime groups (OCGs) in the UK to launder funds from VAT fraud. The ABP had a registered office in one jurisdiction with a holding company in a second jurisdiction and a bank account in a third jurisdiction. It was operated by a PMLN based in a fourth jurisdiction all outside of the UK. The ABP was used for a year with over EUR 400 million moved through it. The ABP was shut down and the creator of the financial software was arrested by international partners, with assistance from Her Majesty's Revenue and Customs (HMRC). The data gathered from the ABP servers was used to identify other ABPs and develop additional cases.

Source: United Kingdom

In some cases, PMLs use specialised software to create an ML scheme to move funds randomly through numerous accounts. This software is generally based on a random data generator principle.

SECTION VI: COMPLICIT/CRIMINAL FINANCIAL SERVICE PROVIDERS AND OTHER PROFESSIONALS

As mentioned in **Section II**, PMLs may occupy positions within the financial services industry (e.g. bankers and MVTS agents) and DNFBP sectors (e.g. lawyers, accountants and real estate professionals), and use their occupation, business infrastructure and knowledge to facilitate ML for criminal clients. The use of occupational professionals can provide a veneer of legitimacy to criminals and OCGs. As such, OCGs actively seek out insiders as potential accomplices to help launder illicit proceeds. In rare instances, complicit actors who facilitate PML schemes come from within a government institution (i.e. a corrupt official).

Box 15. Corrupt Official Joining Criminal Enterprise to Launder Funds

Ukraine's law enforcement and prosecution services conducted an investigation of a high-ranking official who abused his power and official position for approximately three years. The official agreed to participate in the

creation of a criminal organisation and implemented an illegal scheme for minimising tax liabilities, which led to the illegal use of a tax credit. The public official received a cash fee for his services, which were performed with the participation of other public officials and other members of the criminal organisation.

The public official conducted a number of functions to make illicit proceeds appear legitimate, including creating, registering and owning a number of shell companies on behalf of members of the criminal organisation and purchasing property on their behalf. The official also established offshore companies in Cyprus and the BVI using his relatives as nominees. The high-ranking official also acquired entities registered in Ukraine, which were controlled by his offshore companies, by transferring funds from a bank in Liechtenstein. Funds transferred into Ukraine were used to purchase property. Fictitious contacts or agreements (e.g. for consultation services) were also established using a network of fictitious entities for services that were never rendered.

Source: Ukraine

PMLs often ignore or circumvent AML/CFT requirements or actively conceal AML/CFT failures within a particular institution or business. They may also ignore professional obligations, such as restrictions associated with their licenses or professional ethics rules. While the exact definition of complicity is a matter of domestic law, it is widely understood as intentional acts carried out with knowledge or wilful blindness of the illicit nature of the funds with which the person is dealing. The ability of a criminal to purchase or gain ownership or control of a financial business is the ultimate measure of success.

Criminals will actively seek to recruit complicit insiders within existing institutions or businesses, since these individuals have insider access and may be able to falsify records or initiate transactions in a manner, which bypasses AML/CFT regulations or institutional practices. In rare circumstances, criminals may be able to compromise entire institutions or businesses, including by acquiring ownership or control of the institution and appointing their own criminal management. The complicit activity described above (insider compromise and institutional compromise) should not be confused with instances of lax compliance, weak internal controls or inadequate corporate governance structures, which can result in compliance deficiencies with AML/CFT requirements. A reputation for weak compliance, however, may make the institution more attractive for an OCG seeking out a corrupt insider.

Money Value Transfer Services (MVTS) Providers

Case studies and insight provided by delegations show that MVTS providers have knowingly facilitated PML activities, including currency conversions (i.e. foreign exchange), cash-based transactions, and/or electronic funds transfers. Complicit MVTS providers can play an important role in the placement stage of the ML process. The most common ML transactions facilitated by MVTS providers are:

- cash purchases of funds transfers at the physical location of MVTS providers;

- large cash deposits made in the accounts of individuals and businesses followed by a domestic transfer to the account of an MVTS provider, or the purchase of bank drafts (e.g. cashier's check) payable to an MVTS provider; and
- the purchase of bank drafts for the benefit of individuals and businesses, which are negotiated by MVTS providers to fund the purchase of funds transfers.

Box 16. Use of Foreign Exchange Broker and "Quick Drop" Facilities

A mechanic in the UK acted as a professional launderer for an unknown PMLN. The mechanic opened bank accounts in the UK, which were used to deposit GBP 5.3 million in cash between October 2013 and December 2014. Multiple deposits of GBP 25 000 were paid into the bank accounts per day using bank 'quick-drop' facilities. Once paid into the bank accounts, money was transferred to third-party bank accounts held in the UK and six other jurisdictions using bank and foreign exchange broker transfers. The mechanic was paid GBP 20 000 for moving the cash abroad. The launderer pleaded guilty to three charges of ML and, in April 2018, was sentenced to six years in jail and banned from being a company director for nine years.

Quick drop is a facility to deposit, cash either at the bank directly or at a third-party facility, where the money is counted and then transferred to the bank to be deposited[4]. Quick drop facilities allow cash to be deposited quicker, at more locations and often without coming into contact with staff.

Source: United Kingdom

Analysis conducted by some competent authorities indicates that complicit MVTS providers may continue to file suspicious transaction reports (STRs). For example, STRs may be filed so as not to arouse suspicion or give the perception that the MVTS provider is otherwise compliant. In jurisdictions that require other forms of transaction reporting, such as threshold cash transactions, complicit MVTS may operate two sets of account records (i.e. shadow accountancy), one of which is used exclusively for criminal clients and for which no reports are filed. Alternatively, these complicit MVTS providers may report the transactions using fictitious transaction details.

Box 17. Complicit MVTS Agents to Facilitate Third-Party ML

The Italian FIU identified a significant reduction in remittances sent to Country "A" within a three year period (from EUR 2.7 billion in 2012 to EUR 560 million in 2015). This data highlighted the specific exposure of this 'corridor' to the risk of channelling illegal funds.

Further analysis of STRs led to the detection of alternative channels, used by

[4] UK National Risk Assessment of Money Laundering and Terrorist Financing, October 2015

PMLNs, to transfer significant amounts to Country A. A significant portion of the reduction of remittances towards Country A was related to the migration of many Italian MVTS agents towards foreign ones that do not produce statistical reports under national legislations, and are not subject to Italian AML and fiscal requirements.

The FIU received many STRs concerning suspicious activity traced back to Italian money transfer agents. Financial flows were mainly characterised by significant cash deposits and wire transfers in favour of the Italian bank accounts of the foreign MVTS. Such financial flows allegedly referred to money remittances performed by MVTS agents. However, suspicion was triggered given that the agents sometimes deposited cash into their accounts through a branch of the bank located far away from their business. The FIU extended its studies to gain a better understanding of financial flows performed by the MVTS and agents, which revealed that in some cases:

- the MVTS legal representatives were involved;
- the MVTS had been recently incorporated;
- the MVTS had links to subjects originating from Country A;
- the MVTS had opened a branch in an Italian city that is well known for its growing economic and business links with Country A;
- many agents of the same foreign MVTS – all originating from Country A – had already been reported to the Italian FIU or had been prohibited from performing agent activities by the competent financial supervisory authority of Country A, for anomalous transactions and use of false ID documents for CDD purposes;
- the MVTS agents allowed their customers to structure transactions by splitting up remittances with several accomplices; and
- certain MVTS agents revealed tangible links to a common customer base.

In view of analysis carried out, the MVTS provider and agents were found to have disregarded AML obligations, exploiting asymmetries in the regulatory framework among different countries. A well-organised, skilled and complicit network of agents and foreign MVTS had been used to collect funds in Italy, and to transfer significant amounts abroad, splitting up remittances with several accomplices.

Source: Italy

Financial Institutions

The use of the international financial system has been instrumental in facilitating large-scale PML schemes. All of the complex layering schemes described in **Section IV** involve moving significant volumes of funds through various bank accounts in different jurisdictions opened on behalf of shell companies. These well-structured schemes often go undetected by banks, even in situations where there is an insider involved.

Investigative authorities have been able to detect patterns in how PMLs choose certain jurisdictions and banks that are used to move illicit proceeds. For example,

some criminals seek to use banks that operate in lax regulatory environments or have reputations for non-compliance with AML/CFT regulations.

It is challenging for competent authorities to establish factual evidence, which demonstrates that financial institutions are actively complicit in facilitating ML. Bank insiders generally do not communicate openly about their criminal conduct and may be able to leverage their insider status to conceal misdeeds. This can make it difficult to detect and prosecute wilful misconduct by complicit financial services professionals. A range of employees within financial institutions (from lower-level tellers to higher-level management) pose a significant vulnerability that can be exploited by money launderers, but also senior insiders who knowingly assist in ML may cause more damage.

Complicit bank employees may perform functions such as:

- Creating counterfeit checks;
- Monitoring (or not appropriately monitoring) money flows between accounts controlled by the co-conspirators;
- Co-ordinating financial transactions to avoid STR reporting;
- Accepting fictitious documents provided by clients as a basis for transactions, without asking any additional questions; and
- Performing 'virtual transactions' on the accounts of their clients – numerous transactions conducted, without an essential change of the net balance at the beginning and end of a working day.

Box 18. General Manager and Chairman of a Foreign Bank

An investigation by Italian authorities uncovered various ML operations that were carried out by senior foreign bank officials (general manager and chairman), together with a complicit accountant and a lawyer. The illicit proceeds were derived from an international cocaine trafficking organisation.

The criminals were put in contact with the general manager and the chairman of the foreign bank, which was experiencing a serious liquidity crisis at the time. The criminals and the bank executives agreed that one of the drug traffickers would deposit, in his own name, about EUR 15 million at the bank in crisis. This bank committed to provide the two professionals (the lawyer and accountant, noted above, who were also brothers) with a given amount of money in compensation for the intermediation work they performed, to be credited to accounts specifically opened in their names at the bank.

The accountant was also in charge of performing accounting tasks for several companies belonging to the drug trafficker. Following the intermediation activity, the bank's general manager received EUR 1.3 million, in two instalments, from a deposit made in the name of the drug trafficker. Subsequently, the bank's general manager, with the approval of the bank's chairman, started complex financial operations aimed at concealing the unlawful origin of the money deposited.

Authorities were able to ascertain the role played by the lawyer, leaving no

doubt as to his function as an intermediary between his client (custodian) and the bank, and the lawyer's knowledge of the actual illicit source of the money involved.

Source: Italy

The case below demonstrates a combination of different elements and tools, including the sale of shell companies, facilitation of transactions by complicit bank employees and the execution of deals on securities markets.

Box 19. Complicit Bank Employees, Securities Market Deals and the Sale of Shell Companies

An investigation by Russian authorities, conducted in co-operation with foreign FIUs, uncovered an ML and tax evasion scheme that was arranged by complicit bank employees and brokers.

Funds accumulated in bank accounts of shell companies were transferred abroad under the pretext of securities purchases by order of broker "R." At the same time, two broker companies operating on the London Stock Exchange sold shares for the same price, thus facilitating the transfer of money via mirror trading.

All limited liability companies used in this scheme were established by a legal service firm, specialising in the sale of "off-the-shelf" companies. Criminal proceedings were opened. The licenses of one of the banks that facilitated cross-border transfers, and of the securities company, were withdrawn for violations of the AML legislation.

Source: The Russian Federation

1. The cases analysed and information received also demonstrated that private banking advisors may act as PMLs and provide services to conceal the nature, source, ownership and control of the funds in order to avoid scrutiny, by employing various techniques, including:

- Opening and transferring money to and from bank accounts held in the names of individuals or offshore entities, other than the true beneficial owners of the accounts;
- Making false statements on bank documents required by the bank to identify customers and disclose the true beneficial owners of the accounts;
- Using "consulting services" agreements and other similar types of contracts to create an appearance of legitimacy for illicit wire transfers;
- Maintaining and using multiple accounts at the same bank so that funds transfers between those accounts can be managed internally, without reliance on international clearing mechanisms that are more visible to law enforcement authorities; and

- Opening multiple bank accounts in the names of similarly-named companies at the same, or different, institutions so wires do not appear to be coming from third parties.

Legal and Professional Services

In order to place greater distance between their criminal activity and the movement of funds, some OCGs use the services of third-party money launderers, including professional gatekeepers, such as attorneys, accountants and trust and company service providers (TCSPs). One delegation noted that OCGs tend to use professional service providers to set up corporate structures, and that accountants are favoured due to the range of skills and services that they may provide. There are case examples demonstrating that these types of professionals have been recruited to work as PMLs on behalf of larger criminal enterprises, such as DTOs. FATF's 2013 Report on *ML and TF Vulnerabilities of Legal Professionals* mentions that criminals often seek out the involvement of legal professionals in their ML/TF activities because they may be required to complete certain transactions or provide access to specialised legal and notarial skills and services, both of which can assist the laundering of the proceeds of crime

Box 20. A Complicit Lawyer and Bank Employee

A lawyer in Texas was convicted for laundering money for an OCG and engaging in a variety of fraud schemes. The OCG operated in the US, Canada, Africa, Asia and Europe. A complicit bank employee was also convicted for her role in creating counterfeit checks and monitoring money flows between the numerous accounts controlled by the OCG.

All of the victims of these various fraud schemes were instructed to wire money into funnel accounts held by other co-conspirators (money mules), who then quickly transferred the money to other US accounts as well as accounts around the world before victims could discover the fraud. Several millions of dollars were laundered in this manner. The numerous bank accounts opened by the mules served as the initial "layer" in the laundering process, which allowed co-conspirators to distance or conceal the source and nature of the illicit proceeds. For example, during a one-year period, a key money mule opened 38 fraudulent bank accounts.

The fraud schemes took several forms. Many victims were law firms that were solicited online provided counterfeit cashier's checks for deposit into the firms' trust accounts. The law firms were then directed to wire money to third-party shell businesses controlled by the co-conspirators. The fraud conspiracy also employed hackers who compromised both individual and corporate e-mail accounts, ordering wire transfers from brokerage and business accounts to shell accounts controlled by co-conspirators. The shell companies were incorporated in Florida with fictitious names and then used to open bank accounts at banks in Florida in those names.

The licensed attorney in Texas worked for the co-conspirators by laundering victim money through an interest on lawyers trust account (IOLTA). He also

met with individual money mules to retrieve cash from their funnel accounts. The lawyer recruited his paralegal and others to open accounts used in the laundering scheme.

Source: United States

One case involves a licensed attorney who was considered a full member of an OGC. As in the case above, the attorney facilitated ML services by using his interest on lawyers trust account, or ILOTA[5], to transfer the proceeds of drug trafficking and fraud.

Box 21. Operation CICERO

This case was initiated by a special currency police unit within the Guardia di Finanza as a follow-up investigation to a judicially authorised search conducted on the boss of a major organised crime group (La Cosa Nostra or LCN) in Palermo, Italy. This investigation was aimed at identifying those individuals acting as nominees, as well as individuals who facilitated the movement of criminal proceeds on behalf of LCN. The investigation identified that a well-known lawyer was the beneficial owner of the companies used to launder funds via a Palermo-based construction company, which was linked to family members of the organised crime boss.

The lawyer performed a "money box" function for the LCN, which consisted of managing the financial resources of the crime group with the purpose of concealing the origins of the illicit proceeds and avoiding detection by authorities of any assets purchased from these proceeds. Through his professional relationships, the lawyer developed and tapped into an elite social network, which he also made available to the organised crime group.

The lawyer, who was operating as a PML, conducted a number of services, such as: (a) obtaining a mortgage to purchase an apartment with EUR 450 000 in criminal proceeds on behalf of an organised crime family member; (b) using a fictitious contract to purchase an apartment with EUR 110 000 on behalf of the organised crime group; and (c) layering and integrating legal funds with criminal assets derived from construction work carried out on land purchased with criminal proceeds.

This investigation led to confiscation proceedings against nine individuals totalling EUR 550 000 as well as seven properties owned by the lawyer.

Source: Italy

[5] An IOLTA is an account opened by an attorney with the intention of holding client funds for future services. It is opened at a bank with a presumed higher level of confidentiality accorded to attorney-client relationships and related transactions.

PMLs also often use shell companies to facilitate complex ML schemes. Professional services may be used, such as the services of a TCSP or a lawyer, when setting up a shell company. Such professionals can supply a full range of services, including the incorporation of the company, the provision of resident or nominee directors, and the facilitation of new bank accounts.

Box 22. Use of Shell Companies and Accountant Providing Corporate Secretarial Services

Person G was a chartered accountant in the business of providing corporate secretarial services to small and medium-sized enterprises. As part of these services, he incorporated companies on behalf of his clients and acted as the resident director of companies whose directors were not ordinarily residents in Singapore.

Persons N and S, members of a foreign syndicate, approached Person G to set up three companies, Company K, Company W and Company M, and to apply for their corporate bank accounts in Singapore. Once the accounts were set up, Persons N and S left Singapore and never returned. Person G was appointed the co-director of the three companies; although, he was neither a shareholder, nor the authorised bank signatory of these companies.

These companies received criminal proceeds in their bank accounts derived from various frauds amounting to over SGD 650 000. The funds were quickly transferred by Person S to overseas bank accounts.

The companies had committed the offence of transferring benefits of criminal conduct, attributable to Person G's neglect. There was a lack of supervision by Person G over the companies' affairs, which allowed the foreign syndicate to have unfettered control over the companies and partake in their ML activities unimpeded. In January 2016, G was convicted of ML offences and for failing to exercise reasonable diligence in discharging his duties as a director. He was sentenced to a total jail term of 12 months, fined SGD 50 000 and disqualified from acting as a company director for the five years following his sentence.

Source: Singapore

After opening bank accounts in the name of shell companies, professional launderers may operate these accounts from overseas, receiving criminal proceeds from different individuals and companies to layer funds. The funds received in the shell companies' accounts are usually transferred out of the jurisdiction within a few days.

TCSPs are often blind to what their clients actually use the companies for, and therefore do not consider themselves complicit in ML schemes. However, a number of case studies have demonstrated that some TCSPs market themselves as 'no questions asked,' or being immune from official inquires. Moreover, if the TCSP also acts as the director of the company, the TCSP has to perform these duties as a director and could be held liable for the offences committed by the company, as illustrated in the above case study.

Law enforcement agencies worldwide have noted that corporate structures are often used in PML schemes and that professional service providers are used in setting up structures. Law enforcement agencies have identified the use of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal proceeds and that PMLNs exploit some TSCP services in the creation of structures. A handful of current investigations across the globe have indicated that TCSPs act as nominee directors of corporate structures with similar behaviours, observed whether large corporates or smaller TCSPs, including:

- using a 'tick the box' approach for compliance activity;
- distancing themselves from risk (i.e. downplay their responsibility);
- utilising chains of formation agents in multiple jurisdictions;
- engaging in deliberately negligent behaviour; and
- forging signatures and fraudulently notarising documents.

Box 23. Money Laundering through Real Estate Investments, Gastronomic Services and Show Production Services Linked With Drug Trafficking

An investigation was triggered by information received from OFAC, which revealed that an illicit network was conducting business activities in Argentina. This network was linked to an individual, J.B.P.C., who was suspected of being a member of a criminal organisation.

J.B.P.C., his family and business partners were also shareholders in a number of companies around the globe. More specifically, three Argentine companies (two operating companies and a management company) were suspected of developing ambitious real estate projects across the country. The president and main shareholder of those companies was Mr. B, a lawyer and friend of J.B.P.C. This person provided knowledge and experience on how to develop the businesses. Additional analysis revealed that J.B.P.C. was the shareholder of two other companies, which appeared as owners of the land where major real estate developments were to be undertaken.

Tax information that was collected by authorities revealed that these companies received accounting advice from Mr. C, who was a chartered accountant. He was also a shareholder and member of the Board of Directors of the concerned companies. Other transactions from J.B.P.C. were also detected during the same period. They were linked to two additional Argentine companies that provided bar services, coffee services and show production services. For one of the OFAC listed companies, it was discovered that the stock of the company was owned in its entirety by J.B.P.C.'s closest relatives. Likewise, management positions were occupied by his partners and close relatives. Another company, also with ties to J.B.P.C., opened an office in Argentina with the help of another lawyer, Mr. D.

The investigation into this case was conducted by FIU-Argentina in co-ordination with other domestic LEAs, as well as foreign counterparts in

Colombia (FIU-Colombia) and the United States (OFAC and DEA). Strong international co-operation was crucial to the success of this investigation, and joint efforts led to a significant number of simultaneous searches in Argentina, as well as in the other foreign jurisdiction where J.B.P.C. ran a majority of his illegal business. As a result, J.B.P.C., Mr. B and his spouse, Mr. C and Mr. D were arrested. Their property was also seized. Currently, they are facing prosecution in Argentina.

Source: Argentina

Payment Processing Companies

Payment processing companies provide payment services to merchants and other business entities, such as credit card processing or payroll processing services. Typically, bank accounts held by payment processors are used to facilitate payments on behalf of their clients. In certain circumstances, payment processing companies essentially act as "flow-through" accounts – there is no requirement for them to divulge the identities of their individual clients to financial institutions. Traditionally, payment processing companies were established to process credit card transactions for conventional retail outlets. However, over time, payment processing companies have evolved to serve a variety of domestic and international merchants, including Internet-based and conventional retail merchants, Internet gaming enterprises and telemarketing companies.

Payment processing companies can be used by criminal organisations to mask transactions and launder the proceeds of crime. For example, payment processing companies have been used to place illicit proceeds that originated from foreign sources directly into financial institutions[6].

A number of countries have observed the use of payment processing companies by suspected ML networks. In other instances, telemarketing companies have also been suspected of providing payment processing services, where illicit proceeds are co-mingled with payments suspected of being related to mass marketing fraud. Authorities suspect that these types of payment processors may be used by members and associates of multiple transnational OCGs.

Box 24. International Payment Processor Providing ML Services

PacNet, an international payment processor and MVTS provider based in Vancouver, Canada, helped dozens of fraudsters gain access to US banks. PacNet has a 20-year history of engaging in ML and mail fraud, by knowingly processing payments on behalf of a wide range of mail fraud schemes that target victims throughout the world. When it was shut down, PacNet consisted of 12 individuals and 24 entities across 18 countries. The network collectively has defrauded millions of vulnerable victims across the US out of hundreds of

[6] FINCEN, 2012 and FFIEC, nd.

millions of dollars.

With operations in Canada, Ireland and the UK, and subsidiaries or affiliates in 15 other countries, PacNet was the third-party payment processor of choice for perpetrators of a wide range of mail fraud schemes. US consumers receive tens of thousands of fraudulent lottery and other mail fraud solicitations nearly every day that contain misrepresentations designed to victimise the elderly or otherwise vulnerable individuals.

PacNet's processing operations helped to obscure the nature of the illicit funds and prevented the detection of fraudulent schemes. In a typical scenario, scammers mailed fraudulent solicitations to victims and then arranged to have victims' payments (both checks and cash) sent directly, or through a partner company, to PacNet's processing operations. Victims' money, minus PacNet's fees and commission, were made available to the scammers through wire transfers from the PacNet holding account, as well as by PacNet making payments on behalf of the scammers, thereby obscuring the link to the scammers. This process aimed to minimise the chance that financial institutions would detect the scammers and determine their activity to be suspicious.

The mail schemes involved a complicated web of actors located across the world and each scheme followed a similar pattern. These schemes involve a consortium of entities, including direct mailers, list brokers, printer/distributors, mailing houses, "caging" services[7], and payment processors. These six diverse groups worked together to (i) mail millions of solicitation packets each year, (ii) collect and distribute tens of millions of dollars in annual victim payments, and (iii) attempt to obscure their true identities from victims and law enforcement agencies worldwide.

Source: United States

Virtual Currency Payment Products and Services (VCPPS)

As noted in **Section IV**, PMLs offer a variety of services including the use of virtual currency in an attempt to anonymise those committing crimes and their illicit transactions. The use of complex, computer-based fraud schemes has led cyber criminals to create large-scale mechanisms to move the proceeds earned from these schemes. More specifically, virtual currency exchangers have been used as unlicensed or unregistered MVTS providers to exchange criminal proceeds in the form of virtual currency to fiat currency. In 2015, FATF issued guidance to demonstrate how specific FATF Recommendations should apply to convertible virtual currency exchangers in the context of VCPPS, and identify AML/CFT

[7] The processing of responses to direct mail is often conducted by a third party hired to perform various services, which may include processing payments, compiling product orders, correcting recipient addresses, processing returned mail, providing lockbox services, and depositing funds and the associated data processing for each of these services. Caging is a shorthand term for the service bundle.

measures that could be required[8]. Case studies have nonetheless shown that complicit virtual currency exchangers, which have been intentionally created, structured, and openly promoted as criminal business ventures, are being used.

Digital payment systems can also facilitate other crimes, including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption and drug trafficking. Complicit virtual currency providers also utilise shell companies and affiliate entities that cater to an online, worldwide customer base to electronically transfer fiat currency into, and out of, these exchangers (effectively serving as electronic money mules). Users of these complicit services have openly and explicitly discussed criminal activity on these providers' chat functions, and their customer service representatives have offered advice on how to process and access money obtained from illegal drug sales on Dark Web markets.

Box 25. Complicit Virtual Currency Exchanger

On July 26, 2017, a grand jury in the Northern District of California indicted a Russian national and an organisation that he allegedly operated, BTC-e, for operating an unlicensed money services business, ML and related crimes. The indictment alleges that BTC-e was an international ML scheme that allegedly catered to criminals, particularly cyber criminals, and evolved into one of the principal means by which criminals around the world laundered the proceeds of their illicit activity. The indictment alleges that one of the operators of BTC-e who directed and supervised BTC-e's operations and finances, along with others, intentionally created, structured, operated and openly promoted BTC-e as a criminal business venture, developing a customer base for BTC-e that was heavily reliant on criminals. BTC-e was also one of the world's largest and most widely used digital currency exchangers. The investigation has revealed that BTC-e received more than USD 4 billion worth of virtual currency over the course of its operations. In addition to the indictment charging BTC-e and one of its operators with the violations noted above, FinCEN – in close co-ordination with the Justice Department – assessed a USD 110 million civil money penalty against BTC-e for wilfully violating US. anti-money-laundering laws.

Source: United States

SECTION VII: CONCLUDING REMARKS

This threat report addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. A number of characteristics have been identified, based on an extensive case review (including, the role and functions of PMLs; the business models used; and relevant typologies and schemes). A non-public version of the report is available to Members of the FATF and the FATF Global Network upon request. This non-

[8] FATF, 2015.

public version includes further information, such as practical recommendations for the detection, investigation, prosecution and prevention of ML.

REFERENCES

FATF (2006), *Trade-Based Money Laundering*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html

FATF (2012a), *FATF Recommendations*, FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF (2012b), *FATF Guidance on Financial Investigations*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/operationalissues-financialinvestigationsguidance.html

FATF (2013a), *FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems – FATF Methodology*, FATF, Paris, France, www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

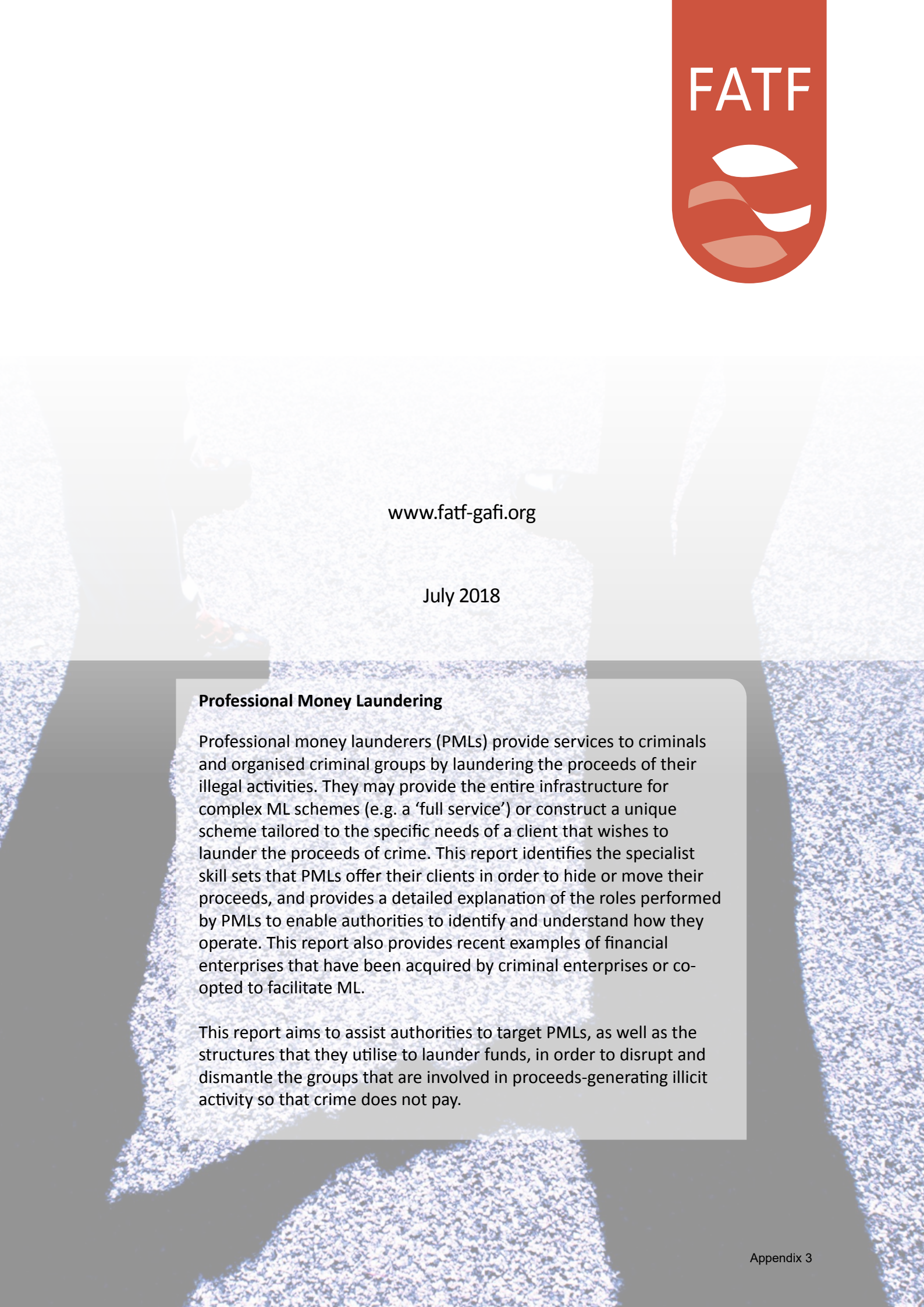
FATF (2013b), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals,* FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html

FATF (2015), *Guidance for a Risk Based Approach to Regulating Virtual Currency*, FATF, Paris, France www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF – Egmont Group (2018), Concealment of Beneficial Ownership, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html

FFIEC (nd), Bank *Secrecy Act, Anti-Money Laundering Examination Manual, Third-Party Payment Processors—Overview,* Bank Secrecy Act/Anti-Money Laundering InfoBase, Federal Financial Institutions Examination Council: www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

FINCEN (2012), *Risk Associated with Third-Party Payment Processors,* FIN-2012-A010. October 22, 2012, Department of the Treasury – Financial Crimes Enforcement Network, Washington, United States, October 22, 2012, https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf



www.fatf-gafi.org

July 2018

Professional Money Laundering

Professional money launderers (PMLs) provide services to criminals and organised criminal groups by laundering the proceeds of their illegal activities. They may provide the entire infrastructure for complex ML schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML.

This report aims to assist authorities to target PMLs, as well as the structures that they utilise to launder funds, in order to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.

Appendix 4

FATF – *International Standards on Combating Money Laundering and the Financing of Terrorism Proliferation* – June 2019

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

The FATF Recommendations

Updated June 2019

Appendix 4

FINANCIAL ACTION TASK FORCE

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

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

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

Citing reference:

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

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

THE FATF RECOMMENDATIONS

ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012

Updated June 2019

CONTENTS

THE FATF RECOMMENDATIONS

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

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

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

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

Version as adopted on 15 February 2012.

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

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

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

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

2. National cooperation and coordination

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

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

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

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

4. Confiscation and provisional measures *

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

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

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

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

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

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

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

7. Targeted financial sanctions related to proliferation *

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

8. Non-profit organisations *

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

(a) by terrorist organisations posing as legitimate entities;

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

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

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

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

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

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

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

(i) establishing business relations;

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

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

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

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

The CDD measures to be taken are as follows:

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

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

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

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

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

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

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

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

11. Record-keeping

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

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

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

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

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

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

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

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

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

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

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

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

13. Correspondent banking *

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

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

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

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

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

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

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

14. Money or value transfer services *

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

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

15. New technologies

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

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

16. Wire transfers *

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

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

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

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties *

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

The criteria that should be met are as follows:

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

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

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

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

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

18. Internal controls and foreign branches and subsidiaries *

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

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

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

19. Higher-risk countries *

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

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

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions *

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

21. Tipping-off and confidentiality

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

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

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

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence *

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

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

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

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

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

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

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

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

23. DNFBPs: Other measures *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d)

of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

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

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons *

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements *

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs *

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

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;

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

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary,

cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers *

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

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

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

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

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

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

(b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

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

(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

(e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

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

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation *

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

(a) ensure money laundering and terrorist financing are extraditable offences;

(b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

(c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

(d) ensure they have an adequate legal framework for extradition.

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

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing

cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

INTERPRETIVE NOTES TO THE FATF RECOMMENDATIONS

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH)

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

A. Obligations and decisions for countries

3. **Assessing risk** - Countries[1] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

4. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

5. **Lower risk** - Countries may decide to allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3.

   Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

6. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

   (a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

   (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

[1] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

7. **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

B. Obligations and decisions for financial institutions and DNFBPs

8. **Assessing risk** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

9. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

10. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.

11. **Lower risk** - Where lower risks are identified, countries may allow financial institutions and DNFBPs to take simplified measures to manage and mitigate those risks.

12. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

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

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

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

4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

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

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

7. Countries should ensure that:

   (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.

   (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.

   (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of

liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

(d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

INTERPRETIVE NOTE TO RECOMMENDATIONS 4 AND 38 (CONFISCATION AND PROVISIONAL MEASURES)

Countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries.

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. Objectives

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. Characteristics of the terrorist financing offence

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

3. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

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

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

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

7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.

8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.

9. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

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

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

    (a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

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

INTERPRETIVE NOTE TO RECOMMENDATION 6 (TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[2] or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions[3]; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)[4]. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

---

2 Natural or legal person.

3 Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

4 Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention)* and the *United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention),* which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions[5]. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

   (a) Countries should identify a competent authority or a court as having responsibility for:

      (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

      (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

[5] The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

(iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

(b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.

(c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.

(e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:

(i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and

(iv) specify whether their status as a designating state may be made known.

(f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:

(i) follow the procedures for listing, as adopted by the 1988 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

(g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries[6] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or

[6] In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBPs[7] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

(e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of

[7] Security Council resolutions apply to all natural and legal persons within the country.

such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**[8]:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof[9]; or

[8] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[9] OP2 of resolution 1617 (2005) further defines the criteria for being "associated with" Al-Qaida or Usama bin Laden.

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

(b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions**:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

(c) **Security Council resolution 1373 (2001)**:

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[10] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person[11] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[12]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.[13] The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

---

10 Recommendation 7 is focused on targeted financial sanctions. These include the specific restrictions set out in Security Council resolution 2231 (2015) (see Annex B paragraphs 6(c) and (d)). However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

11 Natural or legal person.

12 Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretive Note (June 2017), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). Resolution 2231 (2015), endorsing the Joint Comprehensive Plan of Action, terminated all provisions of resolutions relating to Iran and proliferation financing, including 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

13 Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and Security Council resolutions 1540 (2004) and 2235 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) provides that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions. Resolution 2231 (2015) provides that the Security Council shall make the necessary practical arrangements to undertake directly tasks related to the implementation of the resolution.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

   (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

      (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions[14], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

      (ii) proposing to the Security Council, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 2231 (2015) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

   (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 2231 (2015), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

[14] Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

(c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

(e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the Security Council, pursuant to resolution 2231 (2015) and any future successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(f) having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

(a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[15]; and

(b) in the case of resolution 2231 (2015) and any future successor resolutions by the Security Council,

when acting under the authority of Chapter VII of the Charter of the United Nations.

15 As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

   (a) Countries[16] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

   (b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

   (c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

   (d) Countries should require financial institutions and DNFBPs[17] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

   (e) Countries should adopt effective measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

   (f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or

16 In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

17 Security Council resolutions apply to all natural and legal persons within the country.

enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

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

9. Where countries have determined that the exemption conditions set out in resolution 1718(2006) and resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 2231 (2015) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) and continued by resolution 2231 (2015), or taken pursuant to resolution 2231 (2015), shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

    (a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in resolution 2231 (2015) and any future successor resolutions;

    (b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to resolution 2231 (2015); and

(c) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.[18]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016)**:

(i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

(ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programmes, including through illicit means;

(iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[19];

(iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[20];

(v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

(vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

---

18 In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013.*

19 The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

20 Ibid.

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

(b) **On Iran - Resolution 2231 (2015)**:

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities contrary to Iran's commitments in the Joint Comprehensive Plan of Action (JCPOA) or the development of nuclear weapon delivery systems, including through the involvement in procurement of prohibited items, goods, equipment, materials and technology specified in Annex B to resolution 2231 (2015);

(ii) any person or entity assisting designated persons or entities in evading or acting inconsistently with the JCPOA or resolution 2231 (2015); and

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of NPO. This definition is based on those activities and characteristics of an organisation which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Without prejudice to Recommendation 1, this Recommendation only applies to those NPOs which fall within the FATF definition of an NPO. It does not apply to the entire universe of NPOs.

2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important charitable services, as well as the difficulty of providing assistance to those in need, often in high risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. As well, there have been cases where terrorists create sham charities or engage in fraudulent fundraising for these purposes. This misuse not only facilitates terrorist activity, but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs and the donor community. Measures to protect NPOs from potential terrorist financing abuse should be targeted and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects countries' obligations under the Charter of the United Nations and international human rights law.

3. Some NPOs may be vulnerable to terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity.

B. OBJECTIVES AND GENERAL PRINCIPLES

4. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

   (a) A risk-based approach applying focused measures in dealing with identified threats of terrorist financing abuse to NPOs is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to terrorist financing abuse, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

   (b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

   (c) Past and ongoing terrorist financing abuse of NPOs requires countries to adopt effective and proportionate measures, which should be commensurate to the risks identified through a risk-based approach.

   (d) Focused measures adopted by countries to protect NPOs from terrorist financing abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community and with the general public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.

   (e) Countries are required to identify and take effective and proportionate action against NPOs that either are exploited by, or knowingly supporting, terrorists or terrorist organisations taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

   (f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist

financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. MEASURES

5. Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), countries should identify which subset of organisations fall within the FATF definition of NPO. In undertaking this exercise, countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.[21] It is also crucial to identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. Countries should review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified. These exercises could take a variety of forms and may or may not be a written product. Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.

6. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. An effective approach should involve all four of the following elements: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent examples of specific actions that countries should take with respect to each of these elements, in order to protect NPOs from potential terrorist financing abuse.

   (a) Sustained outreach concerning terrorist financing issues

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

      (ii) Countries should encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

      (iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect them from terrorist financing abuse.

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

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

(b) Targeted risk-based supervision or monitoring of NPOs

Countries should take steps to promote effective supervision or monitoring. A "one-size-fits-all" approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice, countries should be able to demonstrate that risk-based measures apply to NPOs at risk of terrorist financing abuse. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically reviewed. Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them.[22] Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[23] The following are some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified:

(i) NPOs could be required to license or register. This information should be available to competent authorities and encouraged to be available to the public.[24]

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

(iii) NPOs could be required to issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

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

(v) NPOs could be required to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries[25] and associate NPOs and that

22 In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

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

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

they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations[26]. However, NPOs should not be required to conduct customer due diligence. NPOs could be required to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality. The ultimate objective of this requirement is to prevent charitable funds from being used to finance and support terrorists and terrorist organisations.

(vi) NPOs could be required to maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation, and could be required to make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (ii) and (iii) above. Where appropriate, records of charitable activities and financial operations by NPOs could also be made available to the public.

(c) Effective information gathering and investigation

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

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

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

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

---

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

26 This does not mean that NPOs are expected to identify each specific individual, as such a requirement would not always be possible and would, in some instances, impede the ability of NPOs to provide much-needed services

(d) Effective capacity to respond to international requests for information about an NPO of concern. Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

D. RESOURCES FOR SUPERVISION, MONITORING, AND INVESTIGATION

7. Countries should provide their appropriate authorities, which are responsible for supervision, monitoring and investigation of their NPO sector, with adequate financial, human and technical resources.

Glossary of specific terms used in this Recommendation	
Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or NPO	refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

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

   (a) normally seek to identify and verify the identity[27] of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

   (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

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

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements[28], financial institutions should be required to identify and verify the identity of

---

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

28 In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue

the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

  (i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

  (ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

  (iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures[29] to verify the identity of such persons, through the following information:

  (i) For legal persons[30]:

    (i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest[31] in a legal person; and

---

to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

29 In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

30 Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

31 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries[32], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the

[32] For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers[33] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

H. RISK BASED APPROACH[34]

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:[35]

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

---

33 Existing customers as at the date that the national requirements are brought into force.

34 The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

35 Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

    - Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
    - Reducing the frequency of customer identification updates.
    - Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
    - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

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

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the payout of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

INTERPRETIVE NOTE TO RECOMMENDATION 13 (CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

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

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

INTERPRETIVE NOTE TO RECOMMENDATION 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created[36]. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk- based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

[36] References to creating a legal person include incorporation of companies or any other mechanism that is used.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

(a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.
(b) R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[37] on virtual asset transfers, submit[38] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

[37] As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

[38] The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers.

INTERPRETIVE NOTE TO RECOMMENDATION 16 (WIRE TRANSFERS)

A. OBJECTIVE

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

   (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

   (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and

   (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

B. SCOPE

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers , including serial payments, and cover payments.

4. Recommendation 16 is not intended to cover the following types of payments:

   (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

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

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

   (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

   (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

C. CROSS-BORDER QUALIFYING WIRE TRANSFERS

6. Information accompanying all qualifying wire transfers should always contain:

   (a) the name of the originator;

   (b) the originator account number where such an account is used to process the transaction;

   (c) the originator's address, or national identity number, or customer identification number[39], or date and place of birth;

   (d) the name of the beneficiary; and

   (e) the beneficiary account number where such an account is used to process the transaction.

7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE TRANSFERS

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter

[39] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

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

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.

12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.

13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it

16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

17. An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

    (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

    (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Glossary of specific terms used in this Recommendation	
Accurate	is used to describe information that has been verified for accuracy.
Batch transfer	is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Cover Payment	refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution

Glossary of specific terms used in this Recommendation

	through one or more intermediary financial institutions.
Cross-border wire transfer	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfers	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *wire transfer* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *wire transfer* that takes place entirely within the borders of the European Economic Area (EEA)[40].
Intermediary financial institution	refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
Ordering financial institution	refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Originator	refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Qualifying wire transfers	means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.
Required	is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the *required originator information.* Subparagraphs 6(d) and 6(e) set out the *required beneficiary information.*

40 An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

Glossary of specific terms used in this Recommendation	
Serial Payment	refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Wire transfer	refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[41]

[41] It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.

2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:

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

   (b) an ongoing employee training programme; and

   (c) an independent audit function to test the system.

2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

3. Compliance management arrangements should include the appointment of a compliance officer at the management level.

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial

group, including, as appropriate, requesting the financial group to close down its operations in the host country.

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

   (a) Requiring financial institutions to apply specific elements of enhanced due diligence.

   (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

   (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.

   (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

   (e) Limiting business relationships or financial transactions with the identified country or persons in that country.

   (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.

   (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.

   (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.

   (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

   There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.

2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.

3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable.

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:

   - Casinos (under Recommendation 22) - USD/EUR 3,000
   - For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

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

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.

2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

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

2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

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

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

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[42]) that are created[43] in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective.

2. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

   (a) identify and describe the different types, forms and basic features of legal persons in the country.

   (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

   (c) make the above information publicly available; and

   (d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.[44] Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company[45] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

---

42 Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

43 References to creating a legal person, include incorporation of companies or any other mechanism that is used.

44 "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

45 The information can be recorded by the company itself or by a third person under the company's responsibility.

(a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and

(b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[46] and categories of shares (including the nature of the associated voting rights).

5. The company registry should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

B. BENEFICIAL OWNERSHIP INFORMATION

7. Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.

8. In order to meet the requirements in paragraph 7, countries should use one or more of the following mechanisms:

(a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) Requiring companies to take reasonable measures[47] to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22[48]; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership.

---

46 This is applicable to the nominal owner of all registered shares.

47 Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

48 Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

9. Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include:

   (a) Requiring that one or more natural persons resident in the country is authorised by the company[49], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation.

10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

C. TIMELY ACCESS TO CURRENT AND ACCURATE INFORMATION

11. Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

13. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above.

D. OBSTACLES TO TRANSPARENCY

14. Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms: (a) prohibiting

[49] Members of the company's board or senior management may not require specific authorisation by the company.

them; (b) converting them into registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary; or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

15. Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request.

E. OTHER LEGAL PERSONS

16. In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.

17. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

18. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

19. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor

the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.

2. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[50]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

3. Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are:

   (a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.

   (b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts).

   (c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers.

4. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.

---

50 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

7. Countries should consider measures to facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

Other Legal Arrangements

9. As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.

International Cooperation

10. Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

Liability and Sanctions

11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.[51] Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to

[51] This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 5.

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.

2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.

3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.

4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and

autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

(c) Dissemination

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION

(a) Obtaining Additional Information from Reporting Entities

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation.

2. A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to:

   - identifying the extent of criminal networks and/or the scale of criminality;
   - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
   - developing evidence which can be used in criminal proceedings.

3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

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

5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.

8. Law enforcement authorities and prosecutorial authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the

staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical cross-border transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

(a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a “yes” or “no” box).

(b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

(c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

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

(a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

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

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

(d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

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

(f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of

money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

(g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is

Glossary of specific terms used in this Recommendation

	asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
Physical cross-border transportation	refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Related to terrorist financing or money laundering	when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should consider establishing an asset forfeiture fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. Countries should take such measures as may be necessary to enable them to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.

2. With regard to requests for cooperation made on the basis of non-conviction based confiscation proceedings, countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

   (a) the request is also considered to involve fiscal matters; and/or

   (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

   (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

Safeguards on information exchanged

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.

4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[52], consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of

[52] Information may be disclosed if such disclosure is required to carry out the request for cooperation.

information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

9. FIUs should have the power to exchange:

   (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and

   (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors[53]

10. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

---

53 This refers to financial supervisors which are competent authorities.

11. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

    (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.

    (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

    (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

12. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

13. Any dissemination of information exchanged or use of that information for supervisory and non- supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

14. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

15. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

16. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or

multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

Exchange of information between non-counterparts

17. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

18. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

      (i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[54] owns or controls a customer[55] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or

[54] Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

[55] This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities[56] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or

[56] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods;

Terms	Definitions
	■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[57] b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses,

[57] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	nor to professionals working for government agencies, who may already be subject to AML/CFT measures. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person or entity	The term designated person or entity refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council

Terms	Definitions
	resolution 1718 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 2231 (2015) and any future successor resolutions by the Security Council.
Designation	The term *designation* refers to the identification of a person[58], individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 2231 (2015) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. As far as Security Council resolution 2231 (2015) and any future successor resolutions are concerned, references to "designations" apply equally to "listing".
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts

[58] Natural or legal.

Terms	Definitions
	which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[59] 2. Lending.[60] 3. Financial leasing.[61] 4. Money or value transfer services.[62] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.

59 This also captures private banking.

60 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

61 This does not extend to financial leasing arrangements in relation to consumer products.

62 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[63]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.

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

Terms	Definitions
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Terms	Definitions
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.

Terms	Definitions
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent

Terms	Definitions
	authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN. to Recommendation 16.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [64]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

[64] Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.

Terms	Definitions
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[65]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

65 Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

Terms	Definitions
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer[66] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

66 In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

ANNEX I: FATF GUIDANCE DOCUMENTS

The FATF has published a large body of Guidance and Best Practices papers which can be found at: www.fatf-gafi.org/documents/guidance/.

ANNEX II: INFORMATION ON UPDATES MADE TO THE FATF RECOMMENDATIONS

The following amendments have been made to the FATF Recommendations since the text was adopted in February 2012.

Date	Type of amendments	Sections subject to amendments
Feb 2013	Alignment of the Standards between R.37 and R.40	■ R.37(d) – page 27 Insertion of the reference that DNFBP secrecy or confidentiality laws should not affect the provision of mutual legal assistance, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.
Oct 2015	Revision of the Interpretive Note to R. 5 to address the foreign terrorist fighters threat	■ INR.5 (B.3) – page 37 Insertion of B.3 to incorporate the relevant element of UNSCR 2178 which addresses the threat posed by foreign terrorist fighters. This clarifies that Recommendation 5 requires countries to criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Existing B.3-11 became B.4-12.
Jun 2016	Revision of R. 8 and the Interpretive Note to R. 8	■ R.8 and INR.8 – pages 13 and 54-59 Revision of the standard on non-profit organisation (NPO) to clarify the subset of NPOs which should be made subject to supervision and monitoring. This brings INR.8 into line with the FATF Typologies Report on Risk of Terrorist Abuse of NPOs (June 2014) and the FATF Best Practices on Combatting the Abuse of NPOs (June 2015) which clarify that not all NPOs are high risk and intended to be addressed by R.8, and better align the implementation of R.8/INR.8 with the risk-based approach.

Date	Type of amendments	Sections subject to amendments
Oct 2016	Revision of the Interpretive Note to R. 5 and the Glossary definition of 'Funds or other assets'	■ INR. 5 and Glossary – pages 37 and 121 Revision of the INR.5 to replace "*funds*" with "*funds or other assets*" throughout INR.5, in order to have the same scope as R.6. Revision of the Glossary definition of "*funds or other assets*" by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.
Jun 2017	Revision of the Interpretive Note to R.7 and the Glossary definitions of "Designated person or entity", "Designation" and "Without delay"	■ INR. 7 and Glossary – pages 45-51, 114-115 and 123 Revision of the INR.7 and consequential revisions of the Glossary definitions of *"Designated person or entity"*, *"Designation"* and *"Without delay"* to bring the text in line with the requirements of recent United Nations Security Council Resolutions and to clarify the implementation of targeted financial sanctions relating to proliferation financing.
Nov 2017	Revision of the Interpretive Note to Recommendation 18	■ INR.18 – page 77 Revision of INR.18 to clarify the requirements on sharing of information related to unusual or suspicious transactions within financial groups. It also includes providing this information to branches and subsidiaries when necessary for AML/CFT risk management.
Nov 2017	Revision of Recommendation 21	■ R. 21 – page 17 Revision of R. 21 to clarify the interaction of these requirements with tipping-off provisions.
Feb 2018	Revision of Recommendation 2	■ R. 2 – page 9 Revision of R. 2 to ensure compatibility of AML/CFT requirements and data protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

Date	Type of amendments	Sections subject to amendments
Oct 2018	Revision of Recommendation 15 and addition of two new definitions in the Glossary	■ R. 15 and Glossary – pages 15 and 126-127 Revision of R.15 and addition of new definitions "virtual asset" and "virtual asset service provider" in order to clarify how AML/CFT requirements apply in the context of virtual assets.
June 2019	Addition of Interpretive Note to R. 15	■ INR. 15 – page 70-71 Insertion of a new interpretive note that sets out the application of the FATF Standards to virtual asset activities and service providers.

www.fatf-gafi.org

Appendix 5

FATF – *Anti-Money Laundering and Counter-Terrorist Financing Measures Canada, Mutual Evaluation Report* – September 2016

Anti-money laundering and counter-terrorist financing measures

Canada

Mutual Evaluation Report

September 2016

Appendix 5

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

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

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation, whose members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the FATF Recommendations.

For more information about the APG, please visit the website: **www.apgml.org**

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

This assessment was conducted under the responsibility of the International Monetary Fund, adopted by the FATF at its June 2016 Plenary meeting.

Citing reference:

FATF (2016), *Anti-money laundering and counter-terrorist financing measures - Canada,* Fourth Round Mutual Evaluation Report, FATF, Paris
www.fatf-gafi.org/publications/mutualevaluations/documents/mer-canada-2016.html

CONTENTS

Executive Summary

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Canada as at the date of the on-site visit (3-20 November 2015). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

1. The Canadian authorities have a good understanding of most of Canada's money laundering and terrorist financing (ML/TF) risks. The 2015 Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (the NRA) is of good quality. AML/CFT cooperation and coordination are generally good at the policy and operational levels.

2. All high-risk areas are covered by AML/CFT measures, except legal counsels, legal firms and Quebec notaries. This constitutes a significant loophole in Canada's AML/CFT framework.

3. Financial intelligence and other relevant information are accessed by Canada's financial intelligence unit, FINTRAC, to some extent and by law enforcement agencies (LEAs) to a greater extent but through a much lengthier process. They are used to some extent to investigate predicate crimes and TF activities, and, to a much more limited extent, to pursue ML.

4. FINTRAC receives a wide range of information, which it uses adequately, but some factors, in particular the fact that it is not authorized to request additional information from any reporting entity (RE), limit the scope and depth of the analysis that it is authorized to conduct.

5. Law enforcement results are not commensurate with the ML risk and asset recovery is low.

6. Canada accords priority to pursing TF activities. TF-related targeted financial sanctions (TFS) are adequately implemented by financial institutions (FIs) but not by designated non-financial business and professions (DNFBPs). Charities (i.e. registered NPOs) are monitored on a risk basis.

7. Canada's Iran and Democratic People's Republic of Korea (DPRK) sanction regime is comprehensive, and some success has been achieved in freezing funds of designated individuals, there is no mechanism to monitor compliance with proliferation financing (PF)- related TFS.

8. FIs, including the six domestic systemically important banks, have a good understanding of their risks and obligations, and generally apply adequate mitigating measures. The same is not true for DNFBPs. REs have gradually increased their reporting of suspicious transactions, but reporting by DNFBPs other than casinos is very low.

9. FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and dealers in precious metals and stones (DPMS) sectors is not entirely commensurate to the risks in those sectors. A range of supervisory tools are used effectively especially in the financial sector. There is some duplication of effort between FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) in the supervisory coverage of federally regulated financial institutions (FRFIs) and a need to coordinate resources and expertise more effectively.

10. Legal persons and arrangements are at a high risk of misuse, and that risk is not mitigated.

11. Canada generally provides useful mutual legal assistance and extradition. The authorities solicit other countries' assistance to fight TF and, to a somewhat lesser extent, ML. Informal cooperation is generally effective and frequently used.

Risks and General Situation

12. Canada has a strong framework to fight ML and TF, which relies on a comprehensive set of laws and regulations, as well as a range of competent authorities.

13. It faces an important domestic and foreign ML threat, and lower TF threat. As acknowledged in the public version of the authorities' 2015 assessment of Canada's inherent ML and TF risks (the NRA), the main domestic sources of proceeds of crime (POC) are fraud, corruption and bribery, counterfeiting and piracy, illicit drug trafficking, tobacco smuggling and trafficking, as well as (to a slightly higher level than assess) tax evasion. Canada's open and stable economy and accessible financial system also make it vulnerable to significant foreign ML threats, especially originating from the neighbouring United States of America (US), but also from other jurisdictions. The main channels to launder the POC appear to be the financial institutions (FIs), in particular the six domestic systemically important banks (D-SIBs) due to their size and exposure, as well as money service businesses (MSBs). While not insignificant, the TF threat to Canada appears lower than the ML threat. A number of TF methods have been used in Canada and have involved both financial and material support to terrorism, including the payment of travel expenses of individuals and the procurement of goods.

Overall Level of Effectiveness and Technical Compliance

14. Since its 2007 evaluation, Canada has made significant progress in bringing its AML/CFT legal and institutional framework in line with the standard, but the fact that AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries is a significant concern. In terms of effectiveness, Canada achieves substantial results with respect to five of the Immediate Outcomes (IO), moderate results with respect to five IOs, and low results with respect to one IO.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

15. The authorities have a generally good level of understanding of Canada's main ML/TF risks. The public version of the 2015 NRA is of good quality. It is based on dependable evidence and sound judgment, and supported by a convincing rationale. In many respects, the NRA confirmed the authorities' overall understanding of the sectors, activities, services and products exposed to ML/TF risk. While the NRA's findings did not contain major unexpected revelations, the process was useful in clarifying the magnitude of the threat, in particular the threat affecting the real estate sector and emanating from third-party money launderers. The authorities nevertheless may be underestimating the magnitude of some key risks, such as the risk emanating from tax crimes and foreign corruption.

16. All high-risk areas are covered by the AML/CFT regime, with the notable exception of the legal professions other than British Columbia (BC) notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

17. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in some higher risk areas such as the real estate and DPMS.

18. AML/CFT cooperation and coordination appear effective at the policy level, but in some provinces, greater dialogue between LEAs and the Public Prosecution Service of Canada (PPSC) would prove useful.

19. While FIs generally appear adequately aware of their ML/TF risks, the same does not apply in some DNFBP sectors, in particular the real estate sector.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

20. Financial intelligence and other relevant information is collected and used to some extent only by competent authorities to carry out investigations into the predicate crimes and TF activities, and, to a more limited extent, to pursue ML. FINTRAC receives a range of information from REs and LEAs, which it adequately analyses. Some factors nevertheless hamper its ability to produce more comprehensive intelligence products, in particular, the fact that FINTRAC is not authorized to obtain from any RE additional information related to suspicions of ML/TF. FINTRAC's analysis and disclosures are mainly prepared in response to the requests made by LEAs in Voluntary Information Records (VIRs). LEAs use these disclosures mainly to investigate the predicate offense, rather than to carry out ML investigations. FINTRAC also produces strategic reports that address the LEAs' operational priorities and advise them on new ML/TF trends and typologies. Information resulting from cross-border transportation of cash and other bearer negotiable instruments is not exploited to its full extent. The FIU and the LEAs cooperate effectively and exchange information and financial intelligence on a regular basis and in a secure way.

21. LEAs have adequate powers and cooperation mechanisms to undertake large and complex financial investigations. This has notably resulted in some high-profile successes in neutralizing ML

networks and syndicates. However, current efforts are mainly aimed at the predicate offenses, with inadequate focus on the main ML risks other than those emanating from drug offenses, i.e. standalone ML, third-party ML and laundering of proceeds generated abroad. Some provinces, such as Quebec, appear more effective in this respect. LEAs' prioritization processes are not fully in line with the findings of the NRA, and LEAs generally suffer from insufficient resources and expertise to pursue complex ML cases. In addition, legal persons are not effectively pursued and sanctioned for ML, despite their misuse having been identified in the NRA as a common ML typology. Criminal sanctions applied are not sufficiently dissuasive. The majority of natural persons convicted for ML are sentenced in the lower range of one month to two years of imprisonment, even in cases involving professional money launderers.

22. Overall, asset recovery appears low. Some provinces, such as Quebec, appear more effective in recovering assets linked to crime. Falsely and undeclared cross-border movements of currency and other bearer negotiable instruments are rarely analysed by the FIU or investigated by the RCMP. As a result, the majority of the cash seized by the Canada Border Services Agency (CBSA) is returned to the traveller at the border.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9- 11; R.5-8)

23. The authorities display a good understanding of Canada's TF risk and cooperate effectively in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations. Canada accords priority to investigations and prosecutions of terrorism and TF. There are a number of TF investigations, which resulted in two TF convictions. Canada also makes regular use of other disruption measures.

24. Implementation of TF-related targeted financial sanctions (TFS) is generally good but uneven. Large FIs implement sanctions without delay, but DNFBPs do not seem to have a good understanding of their obligations and are not required to conduct a full search of their customer databases on a regular basis. In practice, few assets have been frozen in connection with TF-related TFS, which does not seem unreasonable in the Canadian context.

25. Charities (i.e. registered NPOs) are monitored by the Canada Revenue Agency (CRA) on a risk basis, but the number of inspections conducted over the last few years does not reflect those TF risks. The NRA found the risk of misuse of charities as high, but only a small percentage of charities have been inspected. Nevertheless, to limit this risk, the CRA's charities division has developed an enhanced outreach plan which reflects the best practices put forward by the FATF.

26. Canada's framework to implement the relevant UN counter-proliferation financing sanctions is strong and, in some respect, goes beyond the standard, but does not apply to all types of assets listed in the standard. The current lists of designated persons are available on the OSFI websites, and changes to those lists are promptly brought to the attention of the FRFIs (i.e. banks, insurance companies, trust and loan companies, private pension plans, cooperative credit associations, and fraternal benefit societies). There is a good level of policy and operational cooperation between the relevant authorities including those involved in export control, border control, law enforcement and AML/CFT supervision. Some success has been achieved in freezing

funds of designated persons. None of the Canadian authorities has an explicit mandate to monitor FIs' and DNFBPs' implementation of their counter-PF obligations but, in practice, OSFI has examined implementation by FRFIs of TFS for both TF and PF, and has also identified shortcomings and requested improvements.

Preventive Measures (Chapter 5 - IO4; R.9-23)

27. AML/CFT requirements are inoperative towards legal counsels, legal firms and Quebec notaries. These requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada on 13 February 2015. In light of these professionals' key gatekeeper role, in particular in high-risk sectors and activities such as real-estate transactions and the formation of corporations and trusts, this constitutes a serious impediment to Canada's efforts to fight ML.

28. FRFIs, including the six domestic banks that dominate the financial sector, have a good understanding of their risks and AML/CFT obligations. Supervisory findings on the implementation of the risk-based approach (RBA) are also generally positive. The large FRFIs conducted comprehensive group-wide risk assessments and took corresponding mitigating measures. In an effort to mitigate some of the higher risks, a number of FRFIs have gone beyond the Canadian requirements (e.g. by collecting information on the quality of AML/CFT supervision in the respondent bank's country).

29. Nevertheless, some deficiencies in the AML/CFT obligations undermine the effective detection of very high-risk threats identified in the NRA, such as corruption. This is notably the case of the current requirements related to politically exposed persons (PEPs). The identification of beneficial ownership also raises important concerns. Although the legal requirements have recently been strengthened, little is done by FIs to verify the accuracy of beneficial ownership information. DNFBPs are not required to identify the beneficial ownership nor to take specific measures with respect to foreign PEPs.

30. Most DNFBPs are not sufficiently aware of their AML/CFT obligations. This is in particular the case of real estate agents. Extensive work has been conducted by FINTRAC with relevant DPMS trade associations, to increase the DNFBPs' awareness, which is leading to some improvement in compliance. REs have gradually increased the number of STRs and other threshold-based reports filed with FINTRAC but reporting remains very low. The fact that no STRs have been filed by accountants and BC notaries, and the low number of STRs received from the real estate sector raise concern.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-.35)

31. FINTRAC and OSFI supervise FIs and DNFBPs on a risk-sensitive basis. FINTRAC should, however, apply more intensive supervisory measures to DNFBPs. There is good supervisory coverage of FRFIs, but FINTRAC and OSFI need to improve their coordination to share expertise, maximize the use of the supervisory resources available and avoid duplication of efforts. FINTRAC has increased its supervisory capacity in recent years. It adopted an effective RBA in its compliance

and enforcement program, but needs to further develop its sector-specific expertise and increase the intensity of supervision of DNFBPs, particularly in the real estate sector and with respect to DPMS, commensurate with the risks identified in the NRA.

32. There are good market entry controls in place to prevent criminals and their associates from owning or controlling FIs and most DNFBPs. There are, however, no controls for DPMS, and fitness and probity controls at the provincial level are not conducted on an ongoing basis (i.e. including after-market entry).

33. Supervisors appear generally effective. Remedial actions are effectively used and have been extensively applied by supervisors but the sanctioning regime for breaches of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the PCMLTFA) has not been applied in a proportionate and/or sufficiently dissuasive manner. Supervisors have demonstrated that their actions have largely had a positive effect on compliance by FIs and some categories of DNFBPs. They have increased guidance and feedback to REs in recent years but further efforts are necessary, particularly with regard to the DNFBP sector. The exclusion of most of the legal professions (legal counsels, legal firms and Quebec notaries) from AML/CFT supervision has a negative impact on the effectiveness of the supervisory regime as a whole.

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

34. Canadian legal entities and legal arrangements are at a high risk of misuse for ML/TF purposes and that risk is not mitigated. This is notably the case with respect to nominee shareholding arrangements, which are commonly used across Canada and pose real obstacles for LEAs.

35. Basic information on legal persons is publicly available, but beneficial ownership information is more difficult to obtain. Some information is collected by FIs and to a limited extent DNFBPs, the tax authorities and legal entities themselves, but is neither verified nor comprehensive in all cases. LEAs have the necessary powers to obtain that information, but the process is lengthy. Information exchange between LEAs and the CRA is also limited by stringent legal requirements.

36. The authorities have insufficient access to information related to trusts. Some information is collected by the CRA as well as by FIs providing financial services, but that information is not verified, does not always pertain to the beneficial owner, and is even more difficult to obtain than in the case of legal entities.

37. LEAs have successfully identified the beneficial owners in limited instances only. Despite corporate vehicles and trusts posing a major ML and TF risk in Canada, LEAs do not investigate many cases in which legal entities or trusts played a prominent role or that involved complex corporate elements or foreign ownership or control aspects.

International Cooperation (Chapter 8 - IO2; R. 36-40)

38. range of mutual legal assistance (MLA) provided by Canada is generally broad, and countries provided—through the FATF—largely positive feedback regarding the responsiveness and

quality of the assistance provided. Canada solicits other countries' assistance in relatively few instances in pursuit of domestic ML, associated predicate offenses and TF cases with transnational elements. Some concerns were nevertheless raised by some Canadian LEAs about delays in the processing of incoming and outgoing requests. The extradition framework is adequately implemented. Informal cooperation is effective. Cooperation between LEAs, FINTRAC, the CBSA and OSFI and their respective foreign counterparts is more fluid, and more frequently used than MLA. Nevertheless, some weaknesses in Canada's framework (e.g. the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs from DNFBPs) negatively affects the authorities' ability to assist their foreign counterparts.

Priority Actions

- Ensure that legal counsels, legal firms, and Quebec notaries engaged in the activities listed in the standard are subject to AML/CFT obligations and supervision. Bring all remaining FIs and DNFBPs in the AML/CFT regime.
- Increase timeliness of access by competent authorities to accurate and up-to-date beneficial ownership information - Consider additional measures to supplement the current framework.
- Increase timely access to financial intelligence – authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF.
- Use financial intelligence to a greater extent to investigate ML and traces assets.
- Increase efforts to detect, pursue and bring before the courts cases of ML related to all high-risk predicate offenses, third party ML, self-laundering, laundering of POC of foreign predicate and the misuse of legal persons and trusts in ML activities.
- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Ensure compliance by all FIs with the requirement to confirm the accuracy of beneficial ownership in relation to all customers.
- Require DNFBPs to identify and verify the identity of beneficial owners and PEPs.
- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resource and expertise, and review implementation of the current approach.
- Ensure that FINTRAC develops sector-specific expertise, and applies more intensive supervisory measures to the real estate and the DPMS sectors.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

IO.1 - Risk, policy and coordination	IO.2 - International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	**Substantial**	**Substantial**	**Moderate**	**Low**	**Moderate**

IO.7 - ML investigation & prosecution	IO.8 - Confiscation	IO.9 - TF investigation & prosecution	IO.10 - TF preventive measures & financial sanctions	IO.11 - PF financial sanctions
Moderate	**Moderate**	**Substantial**	**Substantial**	**Moderate**

Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	R.2 - national cooperation and coordination	R.3 - money laundering offence	R.4 - confiscation & provisional measures	R.5 - terrorist financing offence	R.6 - targeted financial sanctions – terrorism & terrorist financing
LC	**C**	**C**	**LC**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
LC	**C**	**C**	**LC**	**LC**	**NC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	**C**	**NC**	**PC**	**PC**	**LC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
C	**PC**	**LC**	**NC**	**NC**	**PC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
NC	**LC**	**C**	**PC**	**PC**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
LC	**LC**	**C**	**LC**	**LC**	**C**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	**LC**	**C**	**LC**		

C = Compliant
LC = Largely compliant
PC = Partially compliant
NC = Non-compliant

MUTUAL EVALUATION REPORT

Preface

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in Canada as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology as updated at the time of the on-site. The evaluation was based on information provided by Canada, and information obtained by the evaluation team during its on-site visit to Canada from 3-20 November 2015.

The evaluation was conducted by an assessment team consisting of:

- Nadim Kyriakos-Saad (team leader),
- Nadine Schwarz (deputy team leader),
- Antonio Hyman-Bouchereau (legal expert, IMF),
- Katia Bucaioni (financial sector expert, *Unità di Informazione Finanziaria*, Italy),
- Anthony Cahalan (financial sector expert, Central Bank of Ireland),
- Carla De Carli (legal expert, Regional Circuit Prosecution, Brazil),
- Gabriele Dunker (IMF consultant),
- John Ellis (IMF consultant),
- Sylvie Jaubert (law enforcement expert, Directorate of Intelligence and Customs Investigations, France),
- Amy Lam (law enforcement expert, Hong Kong Police).
- The report was reviewed by Emery Kobor (US), Erin Lubowicz (New Zealand), Peter Smit (South Africa), Richard Berkhout (FATF Secretariat) and Lindsay Chan (Asia Pacific Group on Money Laundering—APG secretariat).

Canada previously underwent a FATF mutual evaluation in 2007, conducted according to the 2004 FATF Methodology. That evaluation concluded that Canada was compliant with 7 Recommendations; largely compliant with 23; partially compliant with 8; and non-compliant with 11. Canada was rated compliant or largely compliant with 13 of the 16 Core and Key Recommendations. Canada was placed in the regular follow-up process, and reported back to the FATF in February 2009, February 2011, October 2011, October 2012, and February 2013. The FATF February 2014 follow-up report found that overall, while some minor deficiencies remained, Canada had made sufficient progress with respect to the Core and Key Recommendations. Canada was therefore removed from the follow-up process in February 2014.

The 2008 mutual evaluation report (MER) and February 2014 follow-up report have been published and are available at www.fatf-gafi.org/countries/#Canada.

CHAPTER 1. ML/TF RISKS AND CONTEXT

39. Canada extends from the Atlantic to the Pacific and northward into the Arctic Ocean, covering 9.98 million square kilometres (3.85 million square miles) in total, making it the world's second-largest country by total area (i.e. the sum of land and water areas) and the fourth-largest country by land area. Canada is a developed country and the world's eleventh-largest economy as of 2015 (approximately USD1.573 trillion). As of 2015, the population of Canada is estimated to be 35 851 774. The foreign-born population of Canada represented 20.6% of the total population in 2011, the highest proportion among the G7 countries.[1]

40. Canada is a federation of ten provinces and three territories[2] in the northern part of North America. Ottawa, in the province of Ontario, is the national capital. Canada is a federal parliamentary democracy and a constitutional monarchy, with her Majesty Queen Elizabeth II being the Head of State. The Governor General of Canada carries out most of the federal royal duties in Canada as representative of the Canadian crown.

41. Canada's Constitution consists of unwritten and written acts, customs, judicial decisions, and traditions dating from 1763. The composition of the Constitution of Canada is defined in subsection 52(2) of the Constitution Act, 1982 as consisting of the Canada Act 1982 (including the Constitution Act, 1982), all acts and orders referred to in the schedule (including the Constitution Act, 1867 and the Charter of Rights and Freedoms), and any amendments to these documents.

42. All provinces and territories within Canada follow the common law legal tradition, except Quebec, which follows the civil law tradition. In addition, all federal laws also follow the common law legal tradition and are applicable in every province and territory (Quebec's civil tradition only applies to provincial laws).

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

43. Canada faces important ML risks generated both domestically and abroad. Estimates of the total amount of POC generated and/or laundered in Canada vary: the Criminal Intelligence Service Canada (CISC) estimated in 2007 that POC generated annually by predicate crimes committed in Canada represent approximately 3-5% of Canada's nominal gross domestic product (GDP), or approximately USD47 billion. The RCMP estimated in 2011 that the amount of money laundered annually in Canada to be somewhere between USD 5 billion and USD 15 billion. The NRA indicates that profit-generating criminal activity generates billions of dollars in POC that might be laundered.

[1] Statistics Canada (2011), Immigration and Ethnocultural Diversity in Canada – National Household Survey, 2011, www12.statcan.gc.ca/nhs-enm/2011/as-sa/99-010-x/99-010-x2011001-eng.cfm.

[2] The 10 provinces are Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec, and Saskatchewan. The three territories are Northwest Territories, Nunavut, and Yukon.

1

44. Organized Criminal Groups (OCGs) pose the greatest domestic ML risk, as they are involved in multiple criminal activities generating large amounts of POC. There are over 650 OCGs operating in Canada. The public version of the NRA does not include a detailed analysis of the risks associated with the methods and financial channels used to raise, collect or transfer funds for TF, due to reasons of national security. The classified version of the NRA includes specific ratings for the TF risks represented by each of the terrorist groups. However, this could not be shared and therefore not assessed by the assessors due to national security concerns.

45. Canada appears to be moderately exposed to PF risks, due primarily to the size of the Canadian financial sector. Canada produces a range of controlled military and dual-use goods, and while no estimates were provided regarding the value and volume of goods exported, they are understood to be relatively large. In addition, Canada appears vulnerable to being used as a transshipment or transit point for military controlled and dual-use goods produced in the US. There are no estimates of the financial flows between Canada and either Iran or the DPRK, but, due to the number of restrictions in place (see R.7 and IO.11), are understood to be low.

ML/TF Threats

46. POCs in Canada are mainly generated from: human smuggling, payment card fraud, tobacco smuggling and trafficking, mass marketing fraud, mortgage fraud, capital markets fraud, illicit drug trafficking, counterfeiting and piracy, corruption and bribery, and commercial trade fraud. Canada is exposed to very high ML threats of both local and foreign origin: (i) Fraud, including capital markets fraud, trade fraud, mass marketing fraud, and mortgage fraud, is a major source of POC in Canada.(ii) The proceeds of drug trafficking laundered in Canada are also significant, and derive predominantly from domestic activity controlled by OCGs. (iii) Third-party ML has started to pose a significant threat in recent years. The NRA found, and discussions on-site confirmed that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers[3] (i.e. individuals specialized in the ML of POC who offer their services for a fee), nominees or money mules. It also found that, of the three, professional money launderers pose the greatest threat both in terms of laundering domestically generated POC as well as laundering, through Canada, of POC generated abroad.[4]

47. The threat emanating from other countries is significant but less easily definable. While some countries have been identified as being the main source of POC laundered in Canada, the authorities' assessment of the foreign ML threat is less detailed and comprehensive than their analysis of the domestic threat.

48. The TF threat was assessed in relation to the terrorist organizations and associated individuals that have financing or support networks in Canada. In particular, the TF threat posed by the actors associated with the following ten terrorist groups and foreign fighters was

[3] It is suspected that criminally-inclined real estate professionals, notably real estate lawyers, are used to facilitate ML. OCGs involved in mortgage fraud appear to launder funds through banks, MSBs, legitimate businesses and trust accounts.

[4] Public version of the NRA, Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, p.22, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

assessed: Al Qaeda in the Arabian Peninsula; Al Qaeda Core; Al Qaeda in the Islamic Maghreb; Al Shabaab; Hamas; Foreign Fighters/Extremist Travellers; Hizballah; Islamic State of Iraq and Syria; Jabhat Al-Nusra; Khalistani Extremist Groups; and Remnants of the Liberation Tigers of Tamil Eelam. Using rating criteria and currently available intelligence, the terrorist groups were assessed as posing a low, medium or high TF threat in Canada. The sectors and products exposed to very high TF risks are corporations, domestic banks, national full-service MSBs, small family-owned MSBs and express trusts. The NRA indicates the possible existence of TF networks in Canada suspected of raising, collecting and transmitting funds abroad to various terrorist groups.[5] The only domestically listed terrorist organizations that pose a TF threat to Canada are those that have financing or support networks in Canada.[6] Terrorism and TF have been increasing in the last two years and more resources were therefore shifted by the authorities to address these threats. As resources remain limited, these issues are putting additional pressures on the AML/CFT regime, and in particular LEAs. Additional funding for AML/CFT activities was authorized in Budget 2015, but these new resources have yet to be fully deployed.

Vulnerabilities

49. Canadian banks offer a number of inherently vulnerable products and services to a very large client base, which includes a significant amount of high-risk clients and businesses. In addition, banks are exposed to high-risk jurisdictions that have weak AML/CFT regimes and significant ML/TF threats. The main channels to launder the POC appear to be the FIs, in particular the D-SIBs due to their size and exposure, as well as MSBs. Terrorist financiers mostly use international and domestic wire transfers to move funds within Canada and/or abroad.

50. The legal profession in Canada is especially vulnerable to misuse for ML/TF risks, notably due to its involvement in activities exposed to a high ML/TF risk (e.g. real estate transactions, creating legal persons and arrangements, or operation of trust accounts on behalf of clients).[7] Following a 13 February 2015 Supreme Court of Canada ruling legal counsels, legal firms and Quebec notaries are not required to implement AML/CFT measures,[8] which, in light of the risks, raises serious concerns.

51. Businesses that handle high volumes of cash are highly vulnerable to ML/TF as they are attractive to launderers of drug proceeds. These include brick and mortar casinos, convenience

[5] The TF methods that have been used in Canada include both financial and material support for terrorism, such as the payment of travel expenses and the procurement of goods. The transfer of suspected terrorist funds to foreign locations has been conducted through a number of methods including the use of MSBs, banks and NPOs as well as smuggling bulk cash across borders.

[6] Organizations posing a terrorist threat to Canada do not necessarily pose a TF threat to Canada. In such cases, the level of threat may not be the same.

[7] The use of trust accounts by lawyers has been recognized by the Department of Finance as a high vulnerability. See: Standing Senate Committee on Banking, Trade and Commerce (2013), Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not really, p. A-26- Lawyers and legal firms, www.parl.gc.ca/Content/SEN/Committee/411/BANC/rep/rep10mar13-e.pdf.

[8] See Judgements of the Supreme Court of Canada (2015), Canada (Attorney General) v. Federation of law societies of Canada, 2015 SCC 7, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14639/index.do.

1

stores, gas stations, bars, restaurants, food-related wholesalers and retailers, and DPMS (notably in the diamonds sector).[9]

52. The real estate sector is highly vulnerable to ML, including international ML activities, and the risk is not fully mitigated, notably because legal counsels, legal firms and Quebec notaries (who provide services in related financial transactions) are not required to implement AML. The sector provides products and services that are vulnerable to ML and TF, including the development of land, the construction of new buildings and their subsequent sale. Also, the real estate business is exposed to high risk clients, including PEPs, notably from Asia[10] and foreign investors (including from locations of concern).

53. Other activities, such as the mining of diamonds, dealing in high value goods, virtual currencies and open loop prepaid cards, are subject to higher ML/TF vulnerability.[11][12] The NRA classifies the virtual currency sector as having high vulnerability, in particular convertible virtual currencies due to the increased anonymity that they can provide as well as their ease of access and high degree of transferability. White-label automated teller machine (ATM) operators are vulnerable to ML/TF. According to the RCMP, OCGs use white-label ATMs to launder POC in Canada. The money withdrawn has previously been deposed into a bank accounts controlled by OCGs through third parties.

54. Legal persons and legal arrangements are inherently vulnerable to misuse for ML/TF purposes to a high degree. There is no legal requirement for legal persons and entities to record and maintain beneficial ownership information. Accordingly, companies and trusts can be structured to conceal the beneficial owner and can be used to disguise and convert illicit proceeds. Privately-held corporate entities can also be established relatively anonymously in Canada. Express trusts have global reach; Canadians and non-residents can establish Canadian trusts in Canada or abroad.

55. Full-service MSBs are vulnerable to ML/TF as they are widely accessible and exposed to clients in vulnerable businesses or occupations, and clients conducting activities in locations of concern. Drug traffickers are particularly frequent users of MSBs.[13]

---

[9] Ibid. p. 63.

[10] For example, there are cases of Chinese officials laundering the PoC through the real estate sector, particularly in Vancouver, and the Chinese government has listed Canada as a country that it wishes to target for recovering the proceeds of Chinese corruption. Canada may be particularly vulnerable to such laundering, as there is no extradition treaty with China.

[11] See FATF (2013), ML and TF through Trade in Diamonds, pp. 30 and 41, www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf.

[12] See "Developing a ML/TF Risk Assessment Framework for Canada," updated by the Public-Private Sector Advisory Committee (PPSAC) in May 2014. In this regard, AML/CFT requirements have not been extended to the other sectors (i.e. luxury goods, automobile, antiquities) when they engage in any cash transaction with a customer equal to or above a designated threshold.

[13] APG (2013), Yearly Typologies Report, www.apgml.org/includes/handlers/get-document.ashx?d=e92a27b8-42d8-4f8e-bea0-6289dcb30b9b .

International Dimension of ML/TF Vulnerabilities

56. Some of Canada's key attributes (e.g. political and economic stability, well-developed international trade networks, cultural environment, and highly developed financial system and regulatory environment)[14] also make it attractive to those seeking to launder money or finance terrorism. Canada's appeal as an investment setting also makes it an attractive destination for foreign POC.

57. Canada and the US share the longest international border in the world, at over 8 800 kilometers. Some passages are unguarded and provide opportunity for criminals to move easily between both countries. OCGs in Canada and the US actively exploit the border for criminal gain. Both countries endeavour to tackle this vulnerability through close cooperation and careful monitoring of threats.

58. Outflows of POC generated within Canada appear to be moderate in comparison with the inflows of POC. Illicit proceeds from cocaine sales in Canada are often smuggled into the US. Canadian individuals and corporations use tax havens and offshore financial centres to evade taxes, in particular those located in the Caribbean, Europe and Asia.

59. Canada's multiethnic and multicultural character also leaves the country vulnerable to exploitation by OCGs seeking to launder POC or terrorist organizations looking to conceal themselves within law-abiding diaspora communities to finance and promote terrorist activities. Some terrorist groups have also been known to use extortion to gain power over individuals to further their objectives, including by extorting funds from diaspora communities in Canada.[15] Moreover, informal diaspora remittances are open to criminal interference because they circumvent exchange controls and can therefore facilitate ML.

Country's risk assessment & Scoping of Higher Risk Issues

60. The Canadian authorities recently undertook a comprehensive ML/TF NRA. They prepared a classified, restricted NRA report that was shared within the government, as well as a shorter, public version that was published in July 2015.

61. The NRA weighs ML/TF threats against the inherent vulnerabilities of sectors (i.e. to assess the likelihood of ML/TF) and then maps those inherent potential risk scenarios using ratings (i.e. very high, high, medium, low) of individual threat and vulnerability profiles. The threats analysed included some related to sectors that are not currently subject to the PCMLTFA (e.g. check cashing businesses, closed-loop pre-paid access, financing and leasing companies). Ratings serve to illustrate the relative importance of various factors/elements/components relevant to ML/TF.

[14] In response to such threats, Canada created the Illicit Financing Advisory Committee (IFAC) in September 2010. IFAC is responsible for advising the Department of Finance and its Minister about high-risk jurisdictions, and provides a formal mechanism to share information among Canadian government departments and AML/CFT agencies in order to identify and assess the ML/TF threats posed by foreign jurisdictions and entities to Canada.

[15] Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (NRA), p. 26, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp.

1

Metrics were based on judgments and were heavily reliant on subject-matter experts' input and readily available information. Based on this approach, all assessed sectors and products were found to be potentially exposed to inherent ML risks while a more limited number of them were found to be exposed to inherent TF risks.

62. While the NRA findings did not contain major unexpected revelations regarding inherent ML or TF threats, the authorities reported that the exercise revealed the magnitude of the threat affecting the real estate sectors and arising from third-party money launderers.

a) Scoping of Higher Risk Issues

63. The assessment team gave increased attention to the following issues which it considered posed the highest ML/TF risk in Canada or warranted more thorough discussions:

- Third-party money launderers (e.g. professional money launderers): The NRA found that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers;
- Exposure of the Canadian economy to international ML/TF activities (i.e. deposit taking sector, real estate sector, and illicit outflows from Canada to so-called tax haven jurisdictions): A number of sectors are highly vulnerable to ML/TF linked to foreign countries, notably due to the openness of the Canadian economy, the volume of international migrants and visitors, a large and accessible financial system, and a well-developed international trading system;
- Inflows and outflows of POC (including with respect to fraud, corruption, OCG and tax evasion): A better understanding of the nature and magnitude of the inflows and outflows of POC was sought to analyse how Canadian regulators and banks are mitigating the risks of the banking system and to evaluate the effectiveness of international cooperation efforts;
- Sanctioning of ML activities (i.e. all ML offenses) and confiscation of POC: The team gathered information on the number and nature of investigations, prosecutions, sanctions imposed and confiscations related to ML and the main predicate offenses in order to analyse trends since the 2008 mutual evaluation report (MER).; and
- Transparency of legal persons and trusts: The high level of vulnerability of Canadian legal persons and arrangements is reflected by the high level of threat of third-party ML, the inoperativeness of AML/CFT requirements to legal counsels, legal firms and Quebec notaries, and the frequent use of front companies by OCGs.

Materiality

64. Canada has a large and diversified economy, with assets totalling about 500% of GDP.[16] In 2014, 70% of the economy was devoted to services, while manufacturing and primary sectors accounted for the remaining 30%.[17] International trade represents more than 60% of Canada's GDP. Most of Canada's trade is with the US (74% of export and 64% of import) followed by China and Mexico.[18]

65. Canada's financial system plays a key role in the Canadian economy and the global financial system. Canadian FIs provide substantial services to non-residents. The financial system is dominated by banks that total 42% of the financial sector assets, and by a handful of players in most sectors. The D-SIBs hold 93% of bank assets. The IMF's 2014 Financial Sector Assessment Program (FSAP) found that Canada's regulatory and supervisory framework demonstrates strong compliance with prudential international standards. Responsibility for supervision of FIs and markets is divided among federal and provincial authorities. The majority of the prudential supervision of the financial sector is regulated at the federal level by OSFI, though a significant segment is subject to provincial regulation.[19] In regard to prudential and business conduct, financial supervision is generally well coordinated across the federal oversight bodies.

Financial Sector and DNFBPs

66. There are approximately 30 000 REs subject to the PCMLTFA.

Table 1. **Entities by Sector (as of November 2015)**

Sector	Number of Entities	Subject to PCMLTFA (Y/N)
Domestic Systemically Important Banks (D-SIBs)	6	Y
Domestic Banks (other than D-SIBs)	22	Y
Foreign Bank Subsidiaries	24	Y
Foreign Bank Branches	29	Y
White-Label ATM Operators (Non-bank or financial institution)	43 100 (est.)	N
Mortgage Lenders	Not available	N
Leasing Companies	Over 200 (est.)	N
Life Insurance Companies	73 federal and 18 provincially-regulated	Y
Independent Life Insurance Agents And Brokers[1]	154 000 agents and 45 000 brokers (est.)	N

[16] Canada is one of the 29 jurisdictions whose financial sectors are considered by the IMF to be systematically important: *Press Release NO 14/08* of 13 January 2014.

[17] See Canada's National Risk Assessment, p.27.

[18] CIA World Factbook, 2015.

[19] For more information on the financial sector, see IMF 2014 Financial Sector Stability Assessment of Canada (www.imf.org/external/pubs/ft/scr/2014/cr1429.pdf). Canada's NRA states that the banking sector is highly concentrated and holds over 60% of the financial system's assets.

Sector	Number of Entities	Subject to PCMLTFA (Y/N)
Trust and Loan Companies	63 federally-regulated trust companies and loan companies and 14 provincially-regulated	Y
Securities Dealers	3 487 (The D-SIBs own six of the securities dealers, accounting for 75% of the sector's transaction volume)	Y
Credit Unions and *Caisses Populaires* (CU/CPs)	696 CU/CPs9 that are provincially-regulated; 6 Cooperative Credit Associations and 1 Cooperative Retail Association that are federally-regulated	Y
Money Services Businesses (MSBs)	850 registered MSBs	Y
Check cashing businesses	Not available	N
Provincially-Regulated Casinos	39	Y
Ship-based casinos	0	N
Real Estate Agents & Developers	20 784	Y
Dealers in Precious Metals and Stones	642	Y
British Columbia Notaries	336	Y
Accountants	3 829	Y
Legal Professionals	104 938 lawyers, 36 685 paralegals and 3 576 civil law notaries	N (to legal counsels, legal firms and Quebec notaries)
Trust & Company Services Providers	8	N
Registered Charities	86 000 federally registered charities	N

1. While independent insurance agents and brokers are not directly covered under the PCMLTFA, life insurance companies may use agents or brokers to ascertain the identity of clients on the basis of a written agreement or arrangement, which must conform to the requirements of PCMLTFR, s.64.1.

67. The broader deposit taking sector includes trust and loan companies. Canada's largest trust and loan companies are subsidiaries of major banks. Some trusts have provincial charters and are regulated at that level of government. Credit unions and *caisses populaires* are provincially incorporated and may not operate outside provincial borders. Relative to banks, these entities are minor participants in the deposit-taking sector. However, *caisses populaires* represent a large portion of the deposit-taking sector in the province of Quebec.

68. The insurance industry is an important player in the financial services sector, providing almost one-fifth of all financing to Canadian companies. Canadian-owned insurers take in more than 70% of total Canadian premium income. Canadian companies are also active abroad, especially in south-east Asia, generating more than half of their premium income from foreign operations.

Structural Elements

69. The key structural elements for effective AML/CFT controls are present in Canada. Canada is generally considered to be a very stable democracy. Political and institutional stability,

accountability, the rule of law and an independent judiciary are all well established. There also appears to be a high-level political commitment to improve the effectiveness of Canada's AML/CFT regime, as evidenced by the Economic Action Plans 2014 and 2015.[20-21] However, LEAs' resources are generally insufficient to pursue complex ML cases.

70. Canada has an independent, efficient, and transparent Justice System. The judicial process is widely trusted and effective, as well as relatively quick.

71. Canada has a comprehensive legal framework that governs the protection of personal information of individuals in both the public and private sectors. The primary source of constitutionally enforced privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms. The Office of the Privacy Commissioner (OPC) oversees compliance with both federal privacy laws (see Box 1 below). Every province has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation. The Canadian regime is implemented while seeking an appropriate balanced between privacy and security considerations. In that regard, in 2012 the OPC issued guidance for REs regarding reporting suspicions to FINTRAC, in light of their customers' privacy rights.[22]

[20] Budget 2014 announced the Government's intention to take action to address the need to enhance the AML/CFT framework. As a result, the Government introduced in 2015 legislative amendments and regulations aiming to strengthen Canada's AML/CFT regime and improve Canada's compliance with international standards. This reform was based on the five-year review of the PCMLTFA undertaken by the Standing Senate Committee on Banking, Trade and Commerce in 2013. Economic Action Plan 2015 (Budget 2015) provides updates on these measures. The Government proposed to provide FINTRAC up to CAD 10.5 million over five years and up to CAD 2.2 million per year subsequently. The Government also proposed to provide up to CAD 12 million on a cash basis over five years to improve FINTRAC's analytics system. This allocation intends to better meet the needs of Canadian law enforcement and other regime partners. See Budget 2014, www.budget.gc.ca/2014/docs/plan/pdf/budget2014-eng.pdf

[21] Includes additional allocation of CAD 292.6 million over five years in intelligence and law enforcement agencies for additional investigative resources to counter terrorism. See www.budget.gc.ca/2015/docs/plan/budget2015-eng.pdf.

[22] Office of the Privacy Commissioner of Canada (2012), Privacy and PCMLTFA: How to balance your customers' privacy rights and your organization's anti-money laundering and anti-terrorist financing reporting requirements, www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp.

Box 1. **Legal Framework for Information and Data Protection in Canada**

The primary source of privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms, which provides protection against unreasonable search and seizure by authorities. This means, generally, that in situations where the person concerned has a reasonable expectation of privacy in relation to an object or document, in order for the state (i.e. government authorities such as LEAs) to have access to these items, prior judicial authorization will need to be obtained. Where such access is sought for the purposes of a criminal investigation, LEAs will generally seek to obtain a search warrant or a production order from a Canadian court. The latter is typically used for access to financial information held by a third party, such as a FI. "Reasonable grounds to believe" that an offense has been committed is the legal standard of proof in Canadian Law for the court to issue the appropriate order. In addition, it is necessary to demonstrate that evidence of the offense is to be found in the place to be searched. In certain cases, such as in relation to certain types of financial information, a lower legal standard of "reasonable grounds to suspect" applies.

At the federal level, Canada has two different privacy acts which are enforced by the Office of the Privacy Commissioner of Canada. The Privacy Act regulates the handling of personal information by federal government departments and agencies. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to the commercial transactions of organizations that operate in Canada's private sector. PIPEDA applies to all private sector entities in Canada, except in provinces that have enacted substantially similar legislation. Every Canadian province and territory has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation.

The Privacy Act lists13 uses and disclosures that might be permissible without the consent of the individual (e.g. national security, law enforcement, public interest). Canadian law provides for lawful access to law enforcement and national security agencies to legally intercept private communications and the lawful search and seizure of information, including computer data, without the consent of either the sender or receiver to investigate serious crimes, including ML and threats to national security, such as terrorism. Lawful access is provided for in the CC, the CSIS Act, the Competition Act and other acts.

The Anti-Terrorism Act (ATA) provides law enforcement and national security agencies powers to obtain electronic search warrants. The ATA also allows Canadian intelligence agencies to intercept communications of Canadians in Canada, and allows the Attorney General to prevent the disclosure of information on the grounds of national security.

Under the PCMLTFA, FINTRAC receives detailed personal information through reports from REs, which can then be provided to the CRA (in cases which include tax matters), CSIS, CBSA, Citizenship and Immigration Canada (in cases which include immigration matters) or to LEAs (e.g. when the information is relevant to the investigation and prosecution of ML or TF offenses).

Background and other Contextual Factors

72. Canada ranks among the highest in international measurements of government transparency, civil liberties, quality of life, economic freedom, and education. It enjoys a high rate of financial inclusion, with 96% of the population having an account with a formal FI. Canadian banks and other FIs operate an extensive network of more than 6 000 branches, and around 60 000 ATMs of which about 16 900 are bank-owned (the rest are white-label ATMs).[23]

73. The authorities have identified corruption as a high-risk issue for ML. Recent assessments of Canada's implementation of international anti-corruption conventions indicate a rather moderate range of positive outcomes in identifying and sanctioning cases of corruption and implementing structures and systems to prevent corruption.[24] Nevertheless, corruption does not appear to hinder the implementation of the AML/CFT regime. Canada is ranked as 9 out of 168 countries in Transparency International's 2015 Corruption Perception Index (with a score of 83/100).[25]

Overview of AML/CFT strategy

74. As formulated in Budget 2014, the Government's priority in regards to AML/CFT is to improve the ability to trace and detect criminal funds in Canada. Besides law enforcement goals, this priority also aims to protect the tax base by supporting the Government's efforts to ensure tax compliance. Addressing this priority requires improving corporate transparency.

75. Canada does not have formal 'stand-alone' AML, CFT or PF strategies. There is, however, a set of relevant policies and strategies: the National Identity Crime Strategy (RCMP 2011); National Border Risk Assessment 2013–2015 (CBSA); 2014–16 Border Risk Management Plan (CBSA); Enhanced Risk Assessment Model and Sector profiles (FINTRAC); AMLC Division AML and CFT Methodology and Assessment Processes (OSFI); Risk Ranking Criteria (OSFI); RBA to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals (CRA) and CRA- RAD Audit Selection process. The RCMP recently developed its National Strategy to Combat ML.[26] These AML strategies and policies are linked to the *Canadian Law Enforcement Strategy on Organized Crime* adopted by senior police officials across Canada in 2011.

---

[23] In Canada, "white label" or "no name" ATMs are those run by independent operators and not by major financial institutions. They are usually located in local small establishment retailers such as gas stations, bars/pubs, and restaurants and do not display labels from financial institutions on the machine.
[24] See 2014 review of the implementation by Canada of the Inter-American Convention against Corruption; 2013 Phase 3 report on implementation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transaction and the 2009 Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions.
[25]Transparency International (2015), 2015 Corruption Perception Index, www.transparency.org/cpi2015.
[26] Royal Canadian Mounted Police (nd), Royal Canadian Mounted Police 2015–16 Report on Plans and Priorities, www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2015-16-report-plans-and-priorities, this strategy was finalized in 2016.

76. The Government's other main AML/CFT concerns are reflected in Finance Canada's Annual Report on Plans and Priorities,[27] which describes the AML/CFT regime's spending plans, priorities and expected results. Canada's CFT strategy policy guidance is derived from its 2012 Counter-terrorism Strategy.[28] This comprehensive Strategy guides more than 20 federal departments and agencies to better align them to address terrorist threats, including in regard to CFT activity and initiatives. The Minister of Public Safety and Emergency Preparedness, in consultation with the Minister of Foreign Affairs, is responsible for the Strategy's implementation. Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological and nuclear weapons.

Overview of the legal & institutional framework

77. Canada's AML/CFT regime is organized as a horizontal federal program comprised of a large number of federal departments and agencies. Finance Canada is the domestic and international policy lead for the regime, and is responsible for its overall coordination, including guiding and informing strategic implementation of the RBA. It chairs the four main governing bodies of Canada's AML/CFT regime, namely:

- The interdepartmental Assistant Deputy Minister (ADM) Level Steering Committee, which was established to direct and coordinate the government's efforts to combat ML and TF activities. The ADM Committee and its working group consists of representatives of all partners;[29]
- The Interdepartmental Coordinating Committee (ICC), which provides a forum for government working-level stakeholders[30] to assess the operational efficiency and effectiveness of the regime;
- The National ML/TF Risk Assessment Committee (NRAC) provides a forum for regime and *ad hoc* partners to exchange information on risks and discuss about ML/TF risks in Canada and their mitigation; and
- The Public Private Sector Advisory Committee (PPSAC) which is a discussion and advisory committee, with membership from (federal public sector) regime partners and private sector REs, as well as provincial law enforcement.[31]

[27] Department of Finance Canada (2014), Report on Plans and Priorities 2014–15, www.fin.gc.ca/pub/rpp/2014-2015/index-eng.asp.
[28] Public Safety (2012), Building Resilience Against Terrorism – Canada's Counter-Terrorism Strategy, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx.
[29] The ADM Committee is composed of the following agencies: Finance Canada; Justice Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; OSFI; and CSIS.
[30] The ICC is composed of the following agencies: Finance Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; CSIS; OSFI; Privy Council Office (PCO); and Global Affairs Canada.
[31] This Committee consist of approximately 30 members, with more than half of the members coming from the private sector. The public sector participants generally consist of members who already participate in the Interdepartmental Steering Committee on this topic. The private sector participants will consist of participants from sectors covered by the PCMLTFA. This includes financial entities, life insurance companies, securities

78. The AML/CFT regime operates on the basis of three interdependent pillars: (i) policy and coordination; (ii) prevention and detection; and (iii) investigation and disruption. On this basis, the following are the primary ministries, agencies, and authorities responsible for formulating and implementing Canada's AML/CFT policies (i.e. the regime partners):

Policy and Coordination:

- **Finance Canada** is the lead agency of the regime, responsible for developing AML/CFT policy related to domestic and international commitments.
- **Department of Justice Canada (DOJ)** is responsible for the drafting and amending of statutory provisions dealing with criminal law and procedure, and to negotiate and administer mutual legal assistance (MLA) and extradition treaties.
- **Global Affairs Canada (GAC)**[32] is responsible for the designation of entities and individuals in Canada associated with terrorist activities listed by the United Nations 1267 Sanctions Committee or under Resolution 1373 of the United Nations Security Council. GAC also chairs the Counter-Proliferation Operations Committee, coordinating responses to threats within Canada.
- **Public Safety Canada (PSC, previously known as Public Safety and Emergency Preparedness)** chairs the Threat Resourcing Working Group and ensures coordination across all federal departments and agencies responsible for national security and the safety of Canadians, including on terrorist financing matters. It is responsible for the listing of terrorist entities under the Criminal Code and co-chairs the Interdepartmental Coordinating Committee on Terrorist Listings.

Prevention and Detection:

- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** is Canada's financial intelligence unit. It is also responsible for supervising and monitoring all REs' compliance with the PCMLTFA.
- **Office of the Superintendent of Financial Institutions Canada (OSFI)** prudentially supervises FRFIs.
- **Innovation, Science and Economic Development Canada (ISED, former Industry Canada)** collects information about business corporations, including the business name and address, and information about the directors.

---

dealers, money service businesses, accountants, the notarial profession, the real estate sector, casinos, dealers in precious metals and stones, and home builders.

[32] Global Affairs Canada's Anti-Crime and Counter-Terrorism Capacity Building programs (ACCBP and CTCBP) funding has been used to support the Regime's AML and CFT projects in a number of regions.

- **Office of the Privacy Commissioner of Canada (OPC)** ensures that the necessary safeguards protecting privacy are upheld. The Privacy Commissioner has the ability to audit the public (e.g. FINTRAC) and private sector to ensure privacy laws are respected. The OPC is required to conduct a privacy audit of FINTRAC every two years.

Investigation and Disruption:

- **Royal Canadian Mounted Police (RCMP)** is Canada's main law enforcement agency (LEA) responsible for investigating predicate offenses, ML and TF.
- **Public Prosecution Service of Canada (PPSC)** is responsible for prosecuting criminal offenses under federal jurisdiction. It also provides legal advice to the RCMP and other LEAs over the course of their investigations, and for undertaking any subsequent prosecutions.
- **Canada Revenue Agency (CRA)**—the CRA's Criminal Investigations Directorate (CID) investigates cases of suspected tax evasion/tax fraud and seeks prosecution through the PPSC where warranted. The CRA also has responsibility for administering the registration system for charities under the Income Tax Act through its Charities Directorate.
- **Canada Border Services Agency (CBSA**) enforces the physical cross-border reporting obligation.
- **Canadian Security Intelligence Service (CSIS)** collects, analyses and reports to the Government of Canada information and intelligence concerning threats to Canada's national security.
- **Public Services and Procurement Canada (PSPC, previously Public Works and Government Services Canada)**, under the Seized Property Management Directorate (SPMD), is responsible for managing assets seized or restrained by law enforcement in connection with criminal offenses and for disposing and sharing the proceeds upon court declared forfeitures.

79. The AML/CFT regime is also supported by a number of other partners including: provincial, territorial and municipal LEAs, provincial and territorial financial sector regulators, and self-regulatory organizations.

80. Canada's AML/CFT framework is established in the PCMLTFA, supported by other key statutes, including the Criminal Code (CC). The Parliament of Canada undertakes a comprehensive review of the PCMLTFA every five years. The Government announced a series of measures to enhance the AML/CFT regime in Budget 2014, which received Royal Assent in June 2014. Accordingly, amended Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) were released in draft form for consultation by the Government on 4 July 2015.

Proliferation Financing

81. The principal legislation governing Canada's export control system is the Export and Import Control Permits Act (EIPA), which provides for the requirements for exporters to report goods to the Government of Canada and for the enforcement of national control lists. The Customs Act and Canada Border Services Agency Act provide the CBSA with the authority to enforce Canada's export legislation. The country's efforts to combat the proliferation of weapons of mass destruction and, to some extent, its financing, are carried out by the following agencies: PSC (coordination of counter-proliferation policy and main operational partner); Global Affairs Canada (lead on international engagement on non-proliferation and disarmament and chairs the Counter-Proliferation Operations Committee); CBSA (law enforcement regarding the illicit export and proliferation of strategic goods and technology); Canadian Nuclear Safety Commission (licensing of nuclear-related activities); PWGSC (administers the Controlled Goods Program); FINTRAC (discloses financial intelligence that can assist in investigations and prosecutions); RCMP (enforces the counter-proliferation regime, investigates related criminal offenses, collects and analyses evidence to support prosecutions in court); the Public Health Agency of Canada (national authority on biosafety and biosecurity for human pathogens and toxins); and Finance (responsible for safeguarding Canada's financial system from illegitimate use, through the PCMLTFA and associated regulations, and the overall coordination of Canada's AML/CFT regime domestically and internationally).

Overview of preventive measures

82. The legal framework relevant to the preventive measures includes the PCMLTFA, the OSFI Act and the FRFIs' governing legislation (i.e. the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act). The PCMLTFA is applicable to most of the financial activities and DNFBPs.

Overview of legal persons and arrangements

83. Canada's company law consists of federal, provincial and territorial frameworks. Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). A federally incorporated entity is entitled to operate throughout Canada. However, provincial and territorial law requires federal entities to register with the province or territory in which the entity is carrying out business. Incorporation on the federal level is carried out by Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) is responsible for the incorporation of federal corporate entities, while each province has its own system for incorporating and administering legal entities.

84. There are over 2.6 million corporations incorporated in Canada, including almost 4 000 publicly-traded companies. About 91% of corporations are incorporated at the provincial or territorial levels and the remaining 9% at the federal level. Bearer shares are permitted in most provinces and at the federal level, but seem to be rarely used. There is also a relatively small market for stock warrants. All companies are obliged to file tax returns with the CRA on an annual basis.

1

Provincial legal entities incorporated in Alberta and Quebec must also file tax returns with the provincial tax authorities.

85. Partnerships are created under provincial law only and, other than limited partnerships, are created under the rules of the common law although subject to laws that codify and regulate certain aspects of the partnership. In contrast, limited partnerships are created under statute and subject to ongoing registration requirements.

86. The only form of legal arrangement that exists in Canada is the trust in form of testamentary or *inter vivos* trust. There is no general requirement for trusts to be registered, but Canadian resident trusts and certain foreign-resident trusts are subject to obligations to file information under the income tax laws. Specific-purpose trusts such as unit or mutual fund trusts are also subject to the securities laws of the relevant province. Trusts created under the laws of Quebec are required to register in some instances. According to the NRA, the total number of Canadian trusts is estimated in the millions. As of 2007, only 210 000 trusts filed tax returns with the CRA.

International Context for Legal Persons and Arrangements

87. According to the UNCTAD 2014 World Investment Report, Canada ranks amongst the top ten countries both with respect to inflowing and outflowing foreign direct investment, with much of the activity taking place in the manufacturing and oil and gas sectors. Canada received over USD 53 billion of foreign direct investment in 2014 coming mostly from the EU, the US, and China. On the outflow, Canada invested approximately USD 52 billion abroad in 2014, mostly in the EU and the US. While detailed figures are not available with respect to foreign ownership of Canadian companies, the statistics provided by the UNCTAD leads to the conclusion that foreign ownership of Canadian legal entities is significant. Canada is not perceived as an international centre for the creation or administration of legal persons or arrangements.

Overview of supervisory arrangements

88. Financial regulation is shared by a number of government bodies in Canada. The Bank of Canada has overall responsibility for financial stability, as well as for the conduct of monetary policy and the issuance of currency. As mentioned above, OSFI supervises and regulates FRFIs (banks and insurance companies, trust and loan companies, cooperative credit associations, fraternal benefit societies, and private pension plans). All banks, including branch operations of foreign banks, are regulated solely at the federal level. The securities sector including in respect of mutual funds, is currently regulated on a province by province basis with connections between the provinces through the Canadian Securities Administrators Association. Markets for securities and collective investments are overseen by provincial securities commissions, which co-ordinate their activities through the Canadian Securities Administrators.[33]

[33] Canada is currently developing a Cooperative Capital Markets Regulatory System (CCMRS), a new joint federal and provincial initiative. Under this system, the provinces and the federal government would delegate

89. In March 2013, FINTRAC and OSFI entered into an agreement to conduct concurrent examinations to improve the effectiveness and cohesion of supervision and allocation of resources, and to reduce the regulatory burden on FRFIs. FINTRAC and OSFI thus concurrently assess FRFIs' AML/CFT compliance and risk management regimes using a RBA. FINTRAC and OSFI mutually share information under a Memorandum of Understanding (MOU) was signed in 2004 with respect to FRFIs. At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other national and provincial supervisors under various MOUs.

their regulatory functions to the CCMR, which may be useful in regard to the identification of systemic risk and criminal enforcement.

1

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

The Canadian authorities have a good understanding of the country's main ML/TF risks and have an array of mitigating measures at their disposal. Canada's NRA is comprehensive, and also takes into account some activities not currently subject to the AML/CFT measures.

All high-risk areas are covered by AML/CFT measures, except activities listed in the standard performed by legal counsels, legal firms and Quebec notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

FIs and casinos have a good understanding of the risks. Other DNFBPs, and in particular those active in the real estate sector, do not have a similarly good understanding.

Law enforcement action focus is not entirely commensurate with the ML risk emanating from high-risk offenses identified in the NRA.

Cooperation and coordination are good at both the policy and operational levels, except, in some provinces, in the context of the dialogue between LEAs and the PPSC.

Communication of the NRA findings to the private sector was delayed, but is in progress.

Recommended Actions

Canada should:

- Mitigate the risk emanating from legal counsels, legal firms, and Quebec notaries in their performance of the activities listed in the standard.
- Strengthen policies and strategies to address emerging ML risks (in particular white label ATMs and online casinos).
- Review LEAs' priorities in light of the findings of the NRA.
- In the context of the update of the NRA, examine more closely ML linked to tax evasion, corruption, legal persons and arrangements, third-party ML and foreign sources of POC and use results to implement mitigating actions.

The relevant Immediate Outcome considered and assessed in this chapter is IO1. The recommendations relevant for the assessment of effectiveness under this section are R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

90. As indicated in Chapter 1 above, Canada completed in 2015 a national assessment of the inherent ML/TF risks that it faces. The process and main findings of the NRA are described above.

Country's understanding of its ML/TF risks

91. The authorities' understanding of ML/TF risks has been forged through the development of several national threat and risks assessments undertaken by different governmental agencies over the past decade on related matters (see Criterion 2.1). The Parliament's Standing Senate Committee on Banking, Trade and Commerce undertakes a comprehensive review of the PCMLTFA every five years. As a result of the most recent review (completed in 2013),[34] the Government introduced legislative amendments in 2014 to address the Committee's recommendations (e.g. including measures to strengthen customer due diligence (CDD) requirements, improve compliance, monitoring and enforcement and enhance information sharing). The authorities demonstrated a sound understanding of the issues highlighted in Chapter 1, including a good understanding of the linkages between the threats and inherent vulnerabilities of the different sectors and the domestic and foreign offenses that are a source of most of the ML/TF[35] in the country. The NRA process has also contributed to a deeper understanding of the powers, resources and operational needs of all regime partners. NRAC ensures that all regime partners generally have a similar level of understanding of the ML/TF risks.

92. Following the publication of the NRA in July 2015, the NRAC concluded a gap analysis in September 2015 to categorize the residual risks (i.e. the risk remaining after the mitigation of the identified threats and inherent vulnerabilities) and identify and prioritize the actions required to mitigate the risk. The review and updating of the NRA is expected to be finalized by the fall of 2016. The authorities indicated that as new, improved controls are put in place, the residual risk will be an indicator of the areas that remain pending to be addressed. As of the date of the on-site visit, it was not possible to establish if the publication of the NRA has led to improvements of the RE's level of compliance with AML/CFT requirements.

National policies to address identified ML/TF risks

93. The adjustment of the national policies and strategies related to the identified ML/TF risks is in its early stages and no updates have been completed. The authorities have been addressing the inherent risks identified in different ways including through ongoing policy coordination through NRAC, the discussion of draft amendments to the PCMLTF Regulations, adjusted supervisory priorities, more focused police investigations, and amendments to the law regarding the seizure of illicit assets, among others.

---

[34] Standing Senate Committee on Banking Trade and Commerce (2013), Follow The Money: Is Canada Making Progress In Combatting Money Laundering And Terrorist Financing? Not Really, www.parl.gc.ca/Content/SEN/Committee/411/banc/rep/rep10mar13-e.pdf.

[35] As elaborated in Chapter 1, the classified version of the NRA, which was not shared with the assessment team, ranks in greater detail the TF risks associated with terrorist groups.

94. On the basis of the NRA, a package of regulatory amendments was issued in July 2015 for public comment. The government is now moving forward with final publication and the Regulations will come into force one year after registration of the regulations. Canada is preparing a second package of regulatory amendments based on the NRA, including measures to cover pre-paid payment products (e.g. prepaid cards), virtual currency as well as money service businesses without a physical presence in Canada in the AML/CFT Regime. The authorities are also revisiting the PCMLTFA provisions relating to legal counsels, legal firms and Quebec notaries, in order to bring forward new provisions for the legal professional that would be constitutionally compliant. Furthermore, also informed by the NRA results, FINTRAC and OSFI are reviewing their RBA to supervision, the RCMP developed its Money Laundering Strategy, and the CBSA is reviewing its Cross-Border Currency Reporting program.

95. As discussed in Chapter 1, Canada's CFT strategy policy guidance is derived from its 2012 Counter-Terrorism Strategy. The PS coordinates Canada's counter-proliferation policy approach across the government, which includes PF.

Exemptions, enhanced and simplified measures

96. Canada's AML/CFT framework does not provide for simplified CDD measures, but the PCMLTFR provide a small number of exceptions to REs based on the risk circumstances and products (see Criterion 10.18). These exemptions correspond to lower-risk scenarios that are consistent with the NRA findings in regard to FIs (i.e. in regard to life insurance companies, brokers, or agents).

Objectives and activities of competent authorities

97. FINTRAC and OSFI objectives and activities are largely consistent with the ML and TF risks in Canada, as detailed in the NRA. With the exception of the legal professions (other than BC notaries), the supervisory coverage is adequate.

98. Law enforcement action is focused on LEAs current priorities, which include drug-related offenses and OCGs, but is not commensurate with the ML risk emanating from these and other types of offenses.

99. In terms of the resources required, the Government's Economic Action Plans for 2014 and 2015 included a commitment to ensuring that law enforcement and security agencies have the investigative resources and tools to address the threats presented by OGCs, ML and terrorism and to further their understanding of Canada's ML/TF risks. Nevertheless, the authorities advised the assessors that all regime partners are under significant pressures at the working level given the increased terrorist threats and combined with the increased threat of professional ML with transnational organized crimes and the number competing priorities.

National coordination and cooperation

100. AML/CFT policy cooperation and coordination to address Canada's ML/TF risks is adequate—with the exception of the dialogue between LEAs and the PPS in some provinces, which is currently insufficient- and constitutes an essential strength of the Canadian AML/CFT framework, as evidenced by the organization and process of the NRA. Canada has wide-ranging arrangements in place for AML/CFT coordination and cooperation at both the policy and operational levels, including with respect to strategic and tactical information sharing (See R.2). Coordination and cooperation at the policy design platform is exceptional.

101. The NRA has allowed the identification and inclusion of new partners for AML/CFT (e.g. Defence Research and Development Canada and Environment Canada), and to reconsider the roles and responsibilities of traditional partners that gained a more prominent role in the fight of ML/TF over the years given enhanced understanding of ML/TF risks (e.g. Industry Canada). Overall, the public version of the NRA is of good quality and is drafted in an accessible language. Moreover, the assessment process has yielded reasonable findings that broadly reflect the country's ML/TF context and risk environment.

Private sector's awareness of risks

102. The public version of the NRA had not been circulated widely at the time of the on-site visit, due to a broader prohibition on the federal public service undertaking consultations with private sector stakeholders during the August to October 2015 federal election campaign. However, the public NRA has been made available on Finance Canada's, OSFI's and FINTRAC's website since July 2015.[36] The report was also shared with the PPSAC. As of the dates of the on-site visit, the authorities had not formally presented the results of the communication strategy for the broader private sector, but were in the process of reaching out to selected FIs. FINTRAC also provides access to guidelines, Interpretation Notices reports on current and emerging trends and typologies in ML and TF on its website to assist FIs and DNFBPs.

Overall Conclusions on Immediate Outcome 1

103. **Canada has achieved a substantial level of effectiveness for IO.1.**

[36] The NRA has since been made available on several websites (e.g. OSFI, Investment Industry Organization of Canada, among others).

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

IO.6

Financial intelligence and other relevant information are accessed by FINTRAC to some extent, and by LEAs to a greater extent but through a much lengthier process.

They are then used by LEAs to some extent to investigate predicate crimes and TF, and, to a more limited extent, to investigate ML and trace assets.

FINTRAC receives a wide range of information, which it uses adequately to produce intelligence. This intelligence is mainly prepared in response to Voluntary Information Records (VIRs; i.e. LEAs' requests) and used to enrich ongoing investigations into the predicate offenses. FINTRAC also makes proactive disclosures to LEAs, some of which have prompted new investigations.

Several factors significantly curtail the scope of the FIU's analysis—and consequently the intelligence disclosed to LEAs—in particular: the impossibility for FINTRAC to request from any RE additional information related to suspicions of ML/TF or predicate offense, the absence of reports from some key gatekeepers (i.e. legal counsels, legal firms, and Quebec notaries), and the inability for FINTRAC to access to information detained by the tax administration. This is compensated by LEAs in their investigations to some extent only due to challenges in the identification of the person or entity who may hold relevant information.

FINTRAC also produces a significant quantity of strategic reports that usefully advise LEAs, intelligence agencies, policy makers, REs, international partners, and the public, on new ML/TF trends and typologies.

FINTRAC and the LEAs cooperate effectively and exchange information and financial intelligence in a secure way.

IO.7

Canada identifies and investigates ML to some extent only. While a number of PPOC cases are pursued, overall, the results obtained so far are not commensurate with Canada's ML risks.

LEAs have the necessary tools to obtain information, including beneficial ownership information, but the process is lengthy.

In some provinces, such as Quebec, federal, provincial, and municipal authorities are relatively more effective in pursuing ML.

Nevertheless, overall, as a result of inadequate alignment of current law enforcement priorities with the findings of the NRA and of resource constraints, LEAs' efforts are aimed mainly at drug offenses and fraud, with insufficient focus on the other main ML risks (corruption, tobacco smuggling, standalone ML, third-party ML, ML of foreign predicate offenses). In addition, investigations generally do not focus on legal entities and trusts (despite the high risk of misuse), especially when

more complex corporate structures are involved.

There is a high percentage of withdrawals and stays of proceedings in prosecution.

Sanctions imposed in ML cases are not sufficiently dissuasive.

IO.8

Canada has made some progress since its last evaluation in terms of asset recovery, but the fact that assets of equivalent value cannot be recovered hampers Canada's recovery of POC.

Confiscation results do not adequately reflect Canada's main ML risks, neither by nature nor by scale.

Results are unequal, with some provinces, such as Quebec, being significantly more effective, and achieving good results with adequately coordinated action (both at the provincial level and with the RCMP) and units specialized in asset recovery.

Administrative efforts to recover evaded taxes appear more effective.

Sanctions are not dissuasive in instances of failure to properly declare cross-border movements of currency and bearer negotiable instruments.

Recommended Actions

Canada should:

IO.6

- Increase timely access to financial intelligence. Authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF in order to enhance its analysis capacity.
- Use financial intelligence to a greater extent to investigate ML and trace assets.
- Analyse and, where necessary, investigate further information resulting from undeclared or falsely declared cross-border transportation of cash and bearer negotiable instruments.
- Ensure that LEAs and FINTRAC can identify accounts and access records held by FIs/DNFBPs in a timely fashion.
- Consider granting FINTRAC access to information collected by the CRA for the purposes of its analysis of STRs.

IO.7

- Increase efforts to detect, pursue, and bring before the courts cases of ML related to high-risk predicate offenses other than drugs and fraud (i.e. corruption and tobacco smuggling), as well as third-party ML, self-laundering, laundering of POC of foreign predicate offenses, and the misuse of legal persons and trusts in ML activities.
- Ensure that LEAs have adequate resources (in terms of number and expertise) for ML

investigations.

- Engage prosecutors at an earlier stage for securing relevant evidence for ML/PPOC prosecutions in order to limit instances where charges are dropped at the judicial process and minimize waste of resources in ML investigations.
- Ensure that effective, proportionate, and dissuasive sanctions for ML are applied.

IO.8

- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Make a greater use of the available tools to seize and restraint POC other than drug-related instrumentalities and cash (i.e. including other assets, e.g. accounts, businesses, and companies, property or money located abroad), especially proceeds of corruption, including foreign corruption, and other major asset generating crimes.
- Amend the legal framework to allow for the confiscation of property of equivalent value.
- Consider increasing the sanctions and seizures related to falsely declared or undeclared cross-border movements of currency and bearer negotiable instruments.

The relevant Immediate Outcomes considered and assessed in this chapter are IO6-8. The recommendations relevant for the assessment of effectiveness under this section are R.3, R4 & R29-32.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

104. Financial intelligence derives from a wide range of information collected by LEAs and received by FINTRAC. Both processes are closely linked. FINTRAC's main financial intelligence product takes the form of disclosures made in response to LEAs' requests (i.e. voluntary information records, VIRs). FINTRAC also disseminates information to LEAs spontaneously (i.e. through "proactive disclosures").

105. LEAs request and obtain financial information held by the private sector either through a court warrant or a production order, when they can establish (as per the CC) that assets are POC. To obtain this judicial authorization, LEAs must identify the FI/DNFBP or entity that holds the information (i.e. account or assets owned or controlled, financial transactions or operation). Various methods are available (see TCA criterion 24.10) and used in practice, such as "grid searches," VIRs to FINTRAC, and consultation of other sources of information as well as use of a range of investigative activities. In Ontario (where the major D-SIBs have their headquarters), "grid searches" are frequently conducted: LEAs send a request to the six D-SIBs (as they dominate about 80% of the deposit-taking market) inquiring whether a particular person is amongst their customers. If there is indication that this person is in business relationships with another FI or with a DNFBP, a request will be sent to that RE as well. Once a D-SIB (or other RE) confirms that a specific person is its

customer, the LEAs apply for a court order requiring the D-SIB to produce the relevant account and beneficial ownership information, as well as transaction records. If necessary, the production is staged to expedite the procedure (i.e. the specific information stated in the order is produced first, and the remainder of the information is provided at a later stage). Nevertheless, the D-SIBs typically take up to several weeks to provide basic and beneficial ownership information to the LEA. As result of the time required at the initial stage (i.e. identification of the relevant RE that may hold the information), as well as the time imparted to implement the production order, it frequently takes 45-90 days before LEAs can obtain the initial transaction records of potential POCs. If the culprit uses numerous layering techniques before integration, it takes LEAs several months or even years to trace POCs. The outlined process is useful only if the persons under investigation bank with the D-SIBs or one of the other large FIs. In cases where a targeted person or entity is in a business relationship with a smaller FI or a DNFBP, the tracing of assets is far more burdensome; given the size of Canada and its financial and non-financial sectors, it is not possible for LEAs to check with each FI and DNFBP individually whether it holds relevant information. In these instances, the identification of the relevant FI or DNFBPs relies on other potentially lengthier methods (e.g. surveillance).

106. LEAs frequently obtain financial information and intelligence from FINTRAC, with or without prior judicial authorization. Most often, they request the information by sending VIRs (which do not require prior judicial authorization). This provides LEAs with a quicker access to the information they need to obtain the judicial authorization (but timeliness of production of requested information remains a challenge). The number of VIRs has increased steadily over the years.[37] This indicates a greater appetite for and appreciation of FINTRAC's reports.[38] Most LEAs expressed their satisfaction with the richness of FINTRAC's responses to VIRs and mentioned that these responses adequately supplement their ongoing investigations.[39] In 2011, the Canadian Association of Chiefs of Police also recognized the contribution of financial intelligence, and called on all Canadian LEAs to include financial intelligence in their investigations and share their targets with FINTRAC.[40]

107. FINTRAC also provides information to LEAs on a spontaneous basis, through proactive disclosures, both in instances linked to ongoing investigation and in cases that identify new potential targets. Between 1 January 2010 and 31 November 2015, the RCMP received 2 497 FINTRAC

[37] Number of VIRs received: 2010–2011: 1 186; 2011–2012: 1 034; 2012–2013: 1 082; 2013–2014: 1 320; 2014–2015: 1 380.

[38] The Canadian authorities were not able to provide additional information regarding the proportion of predicate offense investigations that lead to a VIR.

[39] The Canadian authorities provided examples of written testimonies of some agencies' satisfaction with FINTRAC's response to their VIRs. E.g. "*The disclosure was very impressive in its detail and scope. Shortly after receiving it, our General Investigation Service Unit generated a file resulting in a large seizure of drugs. The individuals mentioned in the disclosure were identified as involved*" (RCMP 'G' Division Federal Investigations Unit); "*The information obtained led us to start a new investigation focused on the money trail—namely the illegal means used by the accused to launder the money they obtained in this case*"(*Sûreté du Québec*); "*Quick turnaround time was appreciated. The disclosures provided new information of potential interest along with account numbers not previously known. The Service was further able to identify additional relationships, which assisted our national security investigation. The information in the electronic funds transfers was found to provide valuable intelligence*" (Canadian Security Intelligence Service).

[40] Canadian Association of Chiefs Police (Resolution #06-2011).

disclosures, 867 of which were proactive.[41] Of these proactive disclosures, the authorities indicated that 599 generated a new investigation.[42] Very few resulted in ML charges (see IO.6.3 and IO.7). The cases communicated to and discussed with the assessors highlighted that FINTRAC information (in response to VIRs and/or shared proactively) is used by LEAs mainly as a basis for securing search warrants, aiding in the selection of investigational avenues (including the identification of targets, associates, and victims) and providing clarification of relevant domestic and international bank accounts and cash flows.

108. Additional relevant information is used to varying degrees: (i) The RCMP and other LEAs receive relevant information from provincial Securities Commissions and recognize the value of such information in combating ML/TF in the context where corporations are identified as very highly vulnerable to be abused for ML/TF. In Toronto and Montreal, the RCMP now includes personnel from the Securities Commission (Joint Securities Intelligence Unit—SIU) to facilitate intelligence gathering, analysis, and dissemination functions. The Canadian authorities provided examples of the use of information communicated to LEAs by the "*Autorité des marches financiers*" (AMF) (including Project Carrefour detailed below, as well as projects Convexe, Jongleur, Incitateur, and Ilot). In these cases, the financial intelligence was used to develop the financial part of the investigation into the predicate offense, not to investigate potential ML activities. (ii) The CRA-CID also uses financial intelligence to identify potential tax evasion. (iii) The CBSA forwards to FINTRAC and to the RCMP all Cross-Border Currency reports (CBCRs) submitted by importers or exporters. It also forwards seizure reports to FINTRAC. It seems that both FINTRAC and the RCMP use the CBSA information to supplement ongoing analysis and investigations[43] and that they analyse or, in the case of LEAs, investigate the CBSA information to a very limited extent, namely only when it has no link to existing cases (see IO.7). Two cases originating from this intelligence have been communicated to the assessors, including project Chun (see Box 4 in IO.7).

[41] FINTRAC also makes disclosures to other LEAs.

[42] According to the authorities, 297 completed feedback forms indicated that FINTRAC proactive disclosures prompted a new investigation in 53 cases between 1 January 2008 and 31 November 2015. In 92 cases a proactive disclosure provided the names of, or leads on, previously unknown persons or businesses/entities, 90 provided new information regarding persons or businesses of interest, 53 triggered a new investigation and 17 provided intelligence that may generate a future investigation. Only one of the 53 new investigations prompted following a proactive disclosure was shared with the assessors.

[43] RCMP indicated that of all ML, PPOC and TF investigations, cross-border currency reporting have been used in 331 cases.

Box 2. **Project Carrefour**

In December 2008, the Montreal Integrated Market Teams (IMET) Program[44] initiated an investigation based on an AMF referral. The AMF is mandated by the government of Quebec to regulate the province's financial markets and provide assistance to consumers of financial products and services. The referral indicated that individuals' Registered Retirement Savings Plans (RRSPs) and other types of retirement savings accounts were being emptied using methods that avoided attention from regulatory and fiscal authorities. The scheme consisted of attracting the attention of investors, through classified ads, with RRSPs and/or other types of retirement savings accounts looking for financial aid. In order for the investors to receive that aid, they had to give up full control of their accounts. The operators of the schemes would then empty those accounts to use the funds to transact on a variety of publicly traded companies under their control, hence engaging in market manipulation. On 15 February 2011, eleven Montréal and Toronto residents were charged with various fraud related offenses committed against 120 investors. They were also charged with fraudulent manipulation of stock exchange transactions estimated at USD 3 million.

109. In sum, financial intelligence is used to some extent to develop evidence and trace criminal proceeds. While a great deal of information provided by REs and others (i.e. in STRs and CBCRs) is used by FINTRAC for tactical analysis, strategic analysis, and to take supervisory action, a large part of this information is not further used by its partners for tactical cases, until it appears relevant for an ongoing investigation. Moreover, a relatively small portion of the intelligence is used for the specific purpose of pursuing ML activities.

110. Financial intelligence and other relevant information are, however, more frequently used to pursue TF. FINTRAC, in consultation with some of the other competent authorities, published advisories that assisted the FIs in their efforts to identify potential ISIL and TF-related activities and funding. Financial intelligence is accessed and used in TF investigation (see below and IO.9), and the on-site discussions as well as the authorities' submissions indicate that FINTRAC's proactive disclosures and responses to VIRs are appreciated by LEAs in their TF efforts.[45]

STRs received and requested by competent authorities

111. FINTRAC receives a significant quantity of information in various reports (see table below), which it uses to develop its financial intelligence.

[44] The objective of the IMET program is to effectively enforce the law against serious criminal capital market fraud offenses in Canada. The authorities involved in the program are the RCMP, ODPP, DOJ, and Finance Canada.

[45] "*FINTRAC is considered a key partner and has provided valuable financial intelligence on an ongoing basis that contributed to "terrorist financing investigations." FINTRAC through their disclosures identified new linkages/nexus between entities and/or individuals through financial transactions which surfaced new avenues of investigation. FINTRAC has always responded in a timely fashion to our priority VIRs*" (RCMP Anti-Terrorist Financing Team, National Security Criminal Operations, Headquarters, Ottawa. FINTRAC 2012 Annual Report, pg. 11, Document 102).

Table 2. **Types of Reports Received by FINTRAC (excluding terrorist property reports)**

	2010–2011	2011–2012	2012–2013	2013–2014	2014–2015
Large Cash Transaction Reports	7 184 831	8 062 689	8 523 416	8 313 098	8 445 431
Electronic Funds Transfer Reports	11 878 508	10 251 643	10 993 457	11 182 829	12 348 360
STRs	58 722	70 392	79 294	81 735	92 531
Cross-Border Currency Reports / Cross-Border Seizure Reports	40 856	35 026	31 826	42 650	47 228
Casino Disbursement Reports	102 438	109 172	116 930	130 141	155 185
Total	**19 265 355**	**18 528 922**	**19 744 923**	**19 750 453**	**21 088 735**

112. With respect to STRs, the authorities indicated that the quality of reporting has improved over the years—notably as a result of FINTRAC's efforts to reach out to REs—and that the information filed is particularly useful for the analysis of individual behaviours and transactional activity. Half of the STRs are sent by MSBs. Banks and credit unions and *caisses populaires* have submitted more STRs to the FIU in the last two years, but the number of STRs filed by DNFBPs other than casinos, while it has increased as a result of FINTRAC's outreach efforts, remains very low (278 in 2014–2015), including those filed by the real estate sector despite the very high ML risk that it faces.[46]

113. The wide range of systematic reports of transactions above CAD 10 000 that FINTRAC receives constitutes an important source of information which has allowed FINTRAC to detect unusual transactions, make links between suspected persons and/or detect bank accounts and other assets held by these persons.

114. Despite the important amount of information received, several factors limit the scope and depth of the analysis that the FIU can do, namely: (i) the fact that some REs listed in the standard are not required to file STRs (in particular legal counsels, legal firms and Quebec notaries) – as a result, FINTRAC does not receive information from key gatekeepers which would otherwise prove useful to its analysis and/or highlight additional cases of potential ML; (ii) the fact that some REs, such as those active in the real estate sector, file few STRs – as a result, information on some areas of high risks is limited; (iii) delays in reporting (FINTRAC supervisory findings seem to confirm that STRs are not filed promptly but within 30 days); and (iv) the fact that FINTRAC is not authorized to

[46] Regarding the real estate sector, the authorities indicated that an important part of STRs received from banks and credit unions and *caisses populaires* over the last three years related to suspicions of ML activities in real estate transactions. This compensates partially but not fully the lack of reporting from legal professionals—other than BC notaries (who, although subject to AML/CFT reporting requirements had not filed STRs at the time of the assessment)- who are directly involved in these transactions. Real estate brokers, sales representatives, and developers (when carrying out certain activities) have filed STRs but in very small numbers.

request additional information related to suspicions of ML, predicate offenses or TF from any REs – as a result, FINTRAC is largely dependent on what is reported. These factors entail that it is challenging for FINTRAC to follow the flows of potential POC in certain cases. For example, when an STR indicates that suspicious funds have been transferred to another FI, FINTRAC can only follow the trail of particular activities or transactions if other intermediaries and/or the final FI have also filed an STR or another report above the required threshold. This is particularly acute when the funds transferred are divided into multiple transfers below CAD 10 000. Enabling FINTRAC to request additional information from REs would considerably facilitate and strengthen the analysis and development of financial intelligence.

Operational needs supported by FIU analysis and dissemination

115. FINTRAC nevertheless provides a significant amount of financial intelligence to LEAs. Over the years, it has increased the number of disclosures sent to regime partners, both in response to VIRs and proactively. In 2014–15, the FIU sent 2 001 disclosures to partners including the RCMP, CBSA, CRA, CSIS, municipal and provincial police, as well as foreign FIUs. Of these, 923 were associated to ML, while 228 dealt with cases of TF and other threats to the security of Canada. 109 disclosures had associations with all three. Additional statistics provided showed that FINTRAC's disseminations of financial information are appropriately spread between the different provinces.

Table 3. **FINTRAC Disclosures to Regime Partners** [1]

Year	Municipal Police	Provincial Police	CRA	CSIS	CBSA	CSEC	RCMP	Total
2012–13	182	144	149	164	96	32	580	**1 347**
2013–14	207	135	153	243	139	33	703	**1 613**
2014–15	331	214	173	312	169	23	779	**2 001**

1. A number of disclosures may have been sent to more than one regime partner.

116. The main predicate offenses highlighted in the disclosures are drugs-related offenses (27% of the cases disseminated), frauds (30%), and tax evasion (11%). Between FY 2010–2011 and 2013–2014, the type of predicates was stable.[47] In FY 2014–2015, FINTRAC also provided information pertaining to potential other predicate offenses to ML (namely crimes against persons, child exploitation, prostitution, weapons and arms trafficking, cybercrimes, and illegal gambling).[48] These predicate offenses are in line with the main domestic sources of POC identified in the NRA, except corruption and bribery, counterfeiting and piracy and tobacco smuggling and trafficking. FINTRAC's disclosures have assisted LEAs in their ongoing investigations in a number of instances, such as in the case of project Kromite described below.

[47] The range of predicate offenses related to the cases disclosed were: drugs, fraud, "unknown," i.e. unspecified, tax evasion, corruption, customs/excise violations, theft, human smuggling/trafficking.
[48] The percentages were the following: crimes against persons, 4%; child exploitation, 1%; prostitution/bawdy houses, 1%; weapons/arms trafficking, 1%; cybercrimes, 0.3%; illegal gambling, 0.3%.

Box 3. **Project Kromite**

In May 2013, the RCMP participated in an international investigation which focused on significant amounts of heroin being imported from source countries (Afghanistan, Pakistan and Iran) to Tanzania and South Africa. The investigation determined that the heroin was transported through various methods to destinations in Europe, South America, the Far East, Australia, the United States, and Canada. Profits from the distribution and sale of illicit drugs were being collected in Canada and disbursed back to the criminal organization in South Africa and Tanzania.

The RCMP sent VIRs to, and received financial disclosures from FINTRAC. The disclosures were able to identify accounts, businesses owned by the subjects and transactions which led to the identification of relevant banking information and, ultimately, to the identification of targets. The financial intelligence was used by the RCMP to collaborate with the DOJ and the PPSC to draft and issue judicial authorizations. Authorizations took various forms including four MLATs, which were issued to three foreign jurisdictions to provide a formal release of information, and Production Orders and Search Warrants that were used to trace and seize POC, both assets and funds. Formal drug-related charges under the Canada's Controlled Drugs Substances Act were laid. The ML-related component of the investigation has been concluded and potential ML/PPOC-related charges were being prepared at the time of the assessment, but no charges had been laid.

117. FINTRAC tailors its analysis to the LEAs' operational priorities. It focuses mainly on answering the VIRs and also discloses intelligence related to LEAs' priorities. Regular operational meetings[49] and discussions are conducted with disclosure recipients to discuss investigative priorities, analytical processes, the development of indicators, and to provide assistance regarding the use of FINTRAC intelligence. The CSIS Financial Intelligence Center (FIC), which is in charge of all financial Intelligence related to national security investigations and linked notably to terrorism and proliferation, also interacts with FINTRAC on a regular basis.

118. FINTRAC's financial intelligence products include its analysis of all relevant information collected: the information contained in STRs, EFTRs, LCTRs, other reports and other information received or accessed by the FIU are all an integral part for developing case disseminations. As mentioned above, LEAs generally consider that FINTRAC's disclosures provide useful supplements to their investigations and generally meet their operational needs. FINTRAC also uses the information gathered in the exercise of its AML/CFT supervisory function, as well as information from a fair range of law enforcement and administrative databases maintained by—or on behalf of—other authorities, and information from open and public sources. While this broad range of information is undeniably useful, it does not necessarily provide FINTRAC with sufficient information about the suspected person's financial environment. In this context, it would prove particularly useful to ensure that FINTRAC has adequate access, for the purposes of the analysis of STRs, to information collected by the CRA, as this would assist FINTRAC with information that could

[49] Seventy-six meetings have been laid in 2014–2015 between FINTRAC and different LEAs agencies, including municipal, provincial and federal agencies, as intelligence services.

strengthen its analysis further, such as information about a person's or entity's income and assets, as well as information on trust assets and trustees (see IO.5).

119. In addition to disclosures in response to VIRs and proactive disclosures, FINTRAC produced from FY 2010/11 to 2014/15, 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors. These reports support the operational needs of competent authorities and many of them are developed in collaboration with the Canadian and international security, intelligence and law enforcement communities. FINTRAC's classified strategic financial intelligence assessments address the nature and extent of ML/TF activities inside and outside of Canada. Canadian authorities provided testimonies of some partners' satisfaction with FINTRAC's strategic intelligence reports.[50]

120. FINTRAC provides a significant amount of disclosures on TF to a variety of LEAs. FINTRAC sent 234 disclosures related to TF and other threats to the security of Canada in 2013-14, and 228 disclosures in 2014-15. These disclosures were communicated to a variety of partner agencies, including CBSA, CRA, CSIS, CSE and RCMP, as well as to municipal and provincial police, and other FIUs, and generated 40 new RCMP TF investigations in 2014 and 126 in 2015.. FINTRAC has increased its disclosures regarding TF to 161 for the first six months of FY 2015-2016, of which 82 were proactive disclosures. This increase in the number of disclosure shows the involvement of the FIU in analysing and disseminating information regarding TF.

Cooperation and exchange of information/financial intelligence

121. Most agencies adequately cooperate and exchange information including financial intelligence. FINTRAC meets with partners on a regular basis, as seen above, and the FIU focuses on priority investigations to support the LEAs' operational needs. In particular, VIRs constitute an important channel for cooperation and information sharing between FINTRAC and LEAs, as well as between LEAs. FINTRAC may send a single disclosure to multiples agencies simultaneously, which informs LEAs that another agency is working on a case. A LEA can further disseminate a disclosure that was based on another agency's VIR, provided that it obtains the permission from the source agency to further disseminate to the requester. In 2014-2015, FINTRAC was authorized by the source agency to disseminate further its disclosures to another LEA in some 41% of cases.

---

[50] FINTRAC's report, Mass Marketing Fraud: "*Money Laundering Methods and Techniques, is helpful to Canadian law enforcement and government agencies in understanding the complexity and international scope of mass marketing fraud impacting Canada. The CAFC has been able to leverage this report to provide insight into the prominent money laundering techniques used by criminal organizations engaged in mass marketing fraud*" (Canadian Anti-Fraud Centre); "*FINTRAC's report (on terrorism financing risks related to a particular group) … have contributed to AUSTRAC's understanding of the topic … FINTRAC and AUSTRAC have been able to collaborate on analytical products, supporting a multilateral approach to information sharing*" (Australian Transaction Reports and Analysis Centre) ; "*Public Safety Canada benefits from strategic financial intelligence reports on ML and TF provided by FINTRAC to inform the overall analysis of national security and organized crime issues. Strategic financial intelligence helps Public Safety to identify the nature and extent of money laundering and terrorism* financing and its potential links to *Canada, international conflicts, crimes, sectors and/or organizations, and the growing links between transnational organized crime and terrorism*" (Public Safety Canada).

122. In addition, FINTRAC has direct and indirect access to LEAs and Security (i.e. intelligence services) databases. The authorities indicated that FINTRAC regularly queries LEA databases in the course of its normal work. FINTRAC and LEAs have established privacy and security frameworks to protect and ensure the confidentiality of all information under FINTRAC's control (including information collected, used, stored and disseminated). In October 2013, FINTRAC strengthened its compliance policies and procedures to increase further the protection of the confidentiality of the information it maintains.

123. Where necessary, LEAs also share information indirectly via FINTRAC by highlighting the disclosures that should be disclosed to other agencies: In this respect, the RCMP has, in specific cases, flagged some files with cross border features to the FINTRAC for disclosure to the CBSA where cross border elements. Similarly, the CBSA has advised FINTRAC to disclose the results of certain VIRs to another regime partner where it determined that further investigations should be carried out.

124. Additionally, the CRA—Charities shares information with other government departments, including RCMP, CSIS and FINTRAC, when there are reasonable grounds to suspect the information would be relevant to an investigation of a terrorism offense or a threat to the security of Canada. Similarly, CSIS shares information on security issues with a range of domestic partners, including FINTRAC, on a regular basis. The sharing of intelligence includes financial intelligence.

Overall Conclusions on Immediate Outcome 6

125. **Canada has achieved a moderate level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

126. ML cases are primarily identified from investigations of predicate offenses, human sources (e.g. informants, victims, suspects, informers, etc.), intelligence (including FINTRAC responses to VIRs), coercive powers, and, in fewer instances, FINTRAC's proactive disclosures, as well as referrals from other government departments without ML investigative powers. LEAs mentioned that they examine all cases with a financial component and assess whether a concurrent financial investigation is warranted. The decisions on whether to investigate a case and how much resources should be devoted to a specific investigation are guided by the LEAs' prioritization processes.[51] As a result, LEAs principally investigate the financial aspects of ML[52] or PPOC[53] occurrences in serious

[51] In the case of the RCMP: The Prioritization Process is designed to aid the judgment of RCMP management in the application of its investigative resources against the most important (priority) criminal threats and activities facing the country. It takes into consideration a series of variables designed to gauge the overall profile of the investigation (or project), its targets, the expected impact against those targets, as well as the expected cost in terms of investigative resources and the length of time they will be dedicated to the project. Prioritization criteria include: economic, political and social integrity of Canada, strategic relevance to RCMP, links to other GoC and partner priorities, etc. Investigations are scored in three tiers (Tier 1 being the highest priority). Highest priority files afforded resources as required to successfully conduct the investigations.
[52] ML encompasses the CC: ss. 462.31(1) and (2) for laundering property and proceeds of property.

and organized crime cases, and in less serious investigations pursue PPOC charges if proceeds are seized through the predicate investigation.

Table 4. **ML and PPOC-Related "Occurrences**[1]
(numbers extracted from all police services' records management systems across Canada)

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	684	716	596	593	608	3 197
PPOC-related Occurrences	42 261	38 796	38 638	37 521	36 012	193 228
Total	**42 945**	**39 512**	**39 234**	**38 114**	**36 620**	**196 425**

1. The basic unit of this data capture system is an "incident", which is defined as the suspected occurrence of one or more criminal offense(s) during one single, distinct event. During the on-site visit, authorities explained that the ML/PPOC related occurrences are classified when the offenses or incidents fall into the definitions of PPOC/ML under the CC. E.g. a simple theft case can be regarded as a PPOC incident; and if the thief further transfers the stolen good, it will be a ML occurrence.

Source: Statistics Canada's Uniform Crime Reporting Survey (2015)

Table 5. **ML/PPOC Occurrences Handled by the RCMP**

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	945	844	692	619	664	3 764
PPOC-Related Occurrences	12 753	11 408	11 573	12 299	14 177	62 210
Total	**13 698**	**12 252**	**12 265**	**12 918**	**14 841**	**65 974**

Source: RCMP

127. The ML/PPOC occurrences handled by RCMP (unlike the numbers provided in the table for all police forces) include 1 599 ML- and 13 179 PPOC-related "assistance files," i.e. cases where the RCMP rendered assistance to foreign agencies. In practice, requests from foreign counterparts are used to a limited extent to identify potential ML cases in Canada. In particular, requests from foreign countries seeking information regarding Canadian bank accounts suspected of receiving or transferring POC are generally only acceded to and a ML investigation initiated when the account holder(s) is/are subject to ongoing investigation(s) in Canada, or there is clear indication of a predicate offense having been committed in Canada. Although Canada has identified third-party ML as one of the very high ML threat, it does not focus sufficiently on foreign requests that may reveal the presence, in Canada, of third-party launderers.

128. As mentioned in IO.6, FINTRAC provides a significant amount of information to LEAs. FINTRAC responses to VIRs (which constitute the majority of FINTRAC's disclosures) and proactive disclosures that have a link with an existing file and/or target are adequately used by LEAs. LEAs mentioned that due to time and resources considerations, in line with their prioritization process, fewer investigations are initiated on the basis of a proactive disclosure which has no link to an ongoing investigation. Between 2010 and 2014, FINTRAC made 867 proactive disclosures to the RCMP, of which 599 led to new ML/PPOC related occurrences for further investigations.

[53] PPOC includes CC s. 354 possession of property of proceeds obtained by crime.

129. While the CBSA may investigate fiscal crimes, it does not have the powers to investigate related ML/PPOC cases, and in instances where it considers that there are reasonable grounds to suspect that a person is or has been engaging in ML activities, it reports the case to the RCMP. The latter recorded that between 2010 and 2014 there were 444 ML/PPOC occurrences related to cross border currency reporting. The authorities provided one case ("Project Chun," described in the Box below) of a successful ML investigation started in 2002 on the basis of a CBSA referral. Whilst the assessment team was also shown several ML cases involving parallel investigations arising from CBSA's enquiries into smuggling or customs related offenses, no other cases arising from CBSA's cross-border declaration/seizure reports were provided. It therefore appears that, in practice, information collected at the border is analysed or investigated with a view to pursuing ML activities to a very limited extent only. The cross-border declaration system is not adequately used to identify potential ML activities.

Box 4. **Case study: Project Chun**

In October 2002, a male was intercepted at the Montreal International Airport with USD 600,000 cash in his hand luggage. In the absence of a valid explanation, the money was seized and the case was referred to RCMP which initiated an investigation to determine the source and destination of the money. Extensive enquiries unveiled that the male and his wife owned two currency exchange companies in Canada and in 2000 they made an agreement with a drug trafficker to assist the latter in laundering proceeds deriving from drug trafficking activities. The laundering included use of various financial services and an elaborate scheme for the transfer of money to a bank in Cambodia that was owned and controlled by the couple. The precise amounts involved in these activities are estimated at more than CAD 100 million. Information received from FINTRAC indicated that the couple dealt in large sums of cash and that their bank account activities did not fit their economic profiles. Travel records of one of the accomplice money launderers were received from Cuba through MLAT requests. The accomplice, who was detained in custody in the US, was later transferred from the US to Canada to provide testimony for the prosecution. Canadian investigators had travelled to Israel and Cambodia for tracing after and restraining the crime proceeds. The couple applied delaying tactics during the prosecution and the Canadian authorities eventually convicted the couple with six counts of Money Laundering and seven counts of tax offenses. In March 2015, the couple was each sentenced to eight years of imprisonment and ordered to pay fines of CAD 9 million. Two real properties, USD 600 000 and the shares of a bank in Cambodia were forfeited.

130. Canada's main law enforcement policy objective is to prevent, detect and disrupt crimes, including ML, but in practice, most of the attention is focused on securing evidence in relation to the predicate offense and little attention is given to ML, as evidenced by the discussions held as well as by the case studies provided. LEAs focus on criminal actions undertaken by OCGs (i.e. mainly drug-related offenses and fraud). Cases studies and figures provided by LEAs demonstrated that they also investigate other high-risk offenses (e.g. corruption and tobacco smuggling), but to a limited extent only. Insufficient efforts are deployed in pursuing the ML element of predicate offenses and pursuing

ML without a direct link to the predicate offense (e.g. third-party/professional money launderers). Since 2010, when tax evasion became a predicate offense to ML, none of the tax evasion cases finalized by the CRA have included sanctions for ML. There are, however, ongoing investigations that contemplate the ML activities.

131. The various LEAs adequately coordinate their efforts, both at the strategic level and at the operational and intelligence levels, through working groups and meetings. Within the RCMP, a centralized database is used to minimize the risk of duplicative investigative efforts against the same groups or persons. Direct exchanges regularly occur during relevant LEAs meetings, as well as through specific joint projects: in particular, the CRA-CID and the RCMP have entered into special projects (i.e. Joint Forces Operations, JFOs) for a specific duration, to identify targets of potential criminal charges including ITA/ETA offenses. Between 2010 and 2015, 10 JFOs were conducted. In these cases, the JFO agreements do not supersede or override the confidentiality provisions of the ITA/ETA, but they, nevertheless, enable the CRA to provide tax information to the RCMP if this is reasonably regarded as necessary for the purposes of the administration and enforcement of the Acts.

132. LEAs regularly seek the production of a court order to obtain banking (or other relevant) information for the purposes of their investigations. However, as detailed in R 31.3 and IO6, the length of the process leading to the identification of relevant accounts considerably delays the tracing of POC in ML/PPOC investigations.

133. The LEAs also access tax information (outside JFOs) with prior judicial authorization. During the period 1 April 2013 to 31 December 2015, the CRA CID received in excess of 2 500 LEA requests for taxpayer information. One RCMP unit indicated that this information is obtained in all significant cases by way of letter under S241 of ITA when charges are laid or by CC authorization of Tax order. The RCMP sent 91 tax letters from 2010 to 2016.

134. LEAs also regularly consult public registries of land and companies, but the paucity of accurate basic and beneficial ownership information in these registries limit the usefulness of the information obtained. Investigations in Canada typically do not focus on complex ML cases involving corporate structures (and/or involving transnational activities). LEAs stated that, in the few cases where legal entities were under investigation, the beneficial ownership information was typically obtained from FIs, in particularly the D-SIBs. Investigators are aware of the risk of misuse of corporate entities in ML schemes, but, in some provinces, do not investigate such cases to the extent that they should mainly because of a shortage of adequate resources and expertise. As a result, some targets are not pursued or bank accounts investigated (e.g. in instances where multiple targets and accounts are involved), and LEA efforts are focused on easier targets where the chances of the investigations being cost effective are greater.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

135. According to the NRA, fraud, corruption, counterfeiting, drug trafficking, tobacco smuggling, and (although a recent phenomenon) third-party ML pose very high ML threats in Canada. The LEAs generally agreed with the NRA findings and have prioritized their resources on OCGs, which are

mostly involved in drug and fraud related offenses (see table below). As described above, LEAs, in particular the RCMP, have a prioritization process, which is continually evolving to address the current threats, taking into account a number of factors. At the time of the assessment, that process did not take the NRA's findings sufficiently into account.

Prosecuted ML-Related Cases	2010	2011	2012	2013	2014	Total	%
Money Laundering (CC s462.31)	88	86	130	108	114	526	51.2%
Fraud	12	27	57	61	53	210	20.4%
Drug Offenses	14	18	9	14	14	69	6.7%
Others	27	52	45	51	47	222	21.6%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100.0%**

Source: Statistics Canada's Uniform Crime Reporting Survey (UCR) – all police services' records

Prosecuted ML-Related Cases	2010	2011	2012	2013	2014	Total	%
PPOC (CC 354, 355)	11930	11955	11179	10904	10292	56260	37.7%
Drug Offenses	4260	4351	4504	4020	3889	21024	14.1%
Fraud	3013	2690	2467	2352	2144	12666	8.5%
Others	13144	12602	12079	11656	9638	59119	39.7%
Total	**32347**	**31598**	**30229**	**28932**	**25963**	**149069**	**100%**

Source: Statistics Canada's Uniform Crime Reporting Survey (UCR) – all police services' records

136. The authorities provided in the above tables the number of prosecution cases, broken down by the most serious offense (MSO) of the case, in which at least one ML or PPOC charge was laid in 2010 to 2014. [54] This information does not distinguish third-party ML from self-laundering. These statistics show that high-threat predicate offenses, i.e. drug trafficking and fraud, account for 27.1% of ML or 22.6% of PPOC prosecutions only, which does not match the ML threats and risks identified in the NRA (which suggest that a higher percentage would be necessary to mitigate the risks). The figures provided do not show related prosecutions in the context of corruption, counterfeiting, and tobacco smuggling cases, but these cases could be embedded in the "others", "ML" or "PPOC" categories, when they were not the MSO. Canada provided further information to show that there were 68 counterfeiting related ML/PPOC cases, examples of tobacco smuggling related ML cases and one case (Project LAUREAT highlighted below) of a successful prosecution of corruption-related ML cases[55].

[54] RCMP also provided that between 2010 and 2014, it laid 130 630 PPOC charges against 35 600 persons and 1 904 ML charges against 503 persons.

[55] Two other corruption related ML cases, Project Ascendant and Project Assistance, were provided but both cases were under court proceedings.

Box 5. **Case study: Project LAUREAT**

In 2010, in order to obtain the CAD 1.3 billion contract of modernization of a Health Centre ("HC"), the president ("P") and vice-president ("VP") of an engineer company ("EC") had bribed the top officials, "Y" and "Z," of the HC to get the award. Upon the announcement of the award to EC, the VP transferred a total of CAD 22.5 million to the shell companies in foreign countries owned by Y and Z. Y further transferred the crime proceeds to the accounts of his wife's (Y's wife) shell companies. Numerous MLAT requests were executed and bank accounts in nine other countries, worth more than CAD 8.5 million, were blocked. Y, Z, P, VP were also extradited from other countries. The syndicate was charged with corruption, fraud, ML along with other offenses. For Y's wife, who has only been involved in laundering the CAD 22.5 million, was sentenced to 33 months of imprisonment.[1] Upon her conviction, seven buildings (value at CAD 5.5 million) were confiscated.

1. The sentence of Y's wife expires in December 2016, but she was granted full parole in September 2015.

137. While Project LAUREAT was relatively successful, overall, on the face of the statistics and cases provided as well as of the discussions held on-site, it was not established that Canada adequately pursues ML related to all very high-risk predicate offenses identified in the NRA.

138. As indicated in the statistics on standalone ML / PPOC prosecutions below, there were 35 (3.4%) and 14 271 (9.6%) standalone ML and PPOC concluded respectively in the last five years. As professional money launderers are mostly involved in ML (rather than PPOC) cases, the fact that Canada only led 35 prosecutions and obtained 12 convictions of single-charge ML cases in the last five years is a concern. It is possible and, according to the authorities, very likely that a professional money launderer would also be charged with another charge such as conspiracy, fraud, or organized crime in addition to ML, but the numbers nevertheless appear too low in light of the risk.

Table 6. **Results of Single Charge ML Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	2	2	4	3	1	12	34.3%
Acquitted	0	0	0	0	1	1	2.9%
Stayed	0	1	3	1	0	5	14.3%
Withdrawn	2	4	4	2	2	14	40.0%
Other decisions	0	0	1	0	2	3	8.6%
Total	**4**	**7**	**12**	**6**	**6**	**35**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 7. **Results of Single Charge PPOC Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	1332	1199	1108	1017	947	5603	39.3%
Acquitted	115	84	76	127	98	500	3.5%
Stayed	589	642	640	611	581	3063	21.5%
Withdrawn	1158	1077	1022	904	806	4967	34.8%
Other decisions	53	23	24	23	15	138	1.0%
Total	**3247**	**3025**	**2870**	**2682**	**2447**	**14271**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

139. Canada's NRA also identified very high ML vulnerabilities in the use of trusts and corporations. LEAs confirmed that corporate vehicles and trusts are misused to a relatively large extent for ML purposes. As the case study Dorade (below) indicates, the authorities have been successful in identifying the legal persons and arrangements involved in the ML schemes and in confiscating their assets in some instances. However, overall, it was clear from the discussions held with police forces and prosecutors that legal persons are hardly ever prosecuted for ML offenses, mainly because of a shortage of adequate resources and expertise. Investigators are nevertheless aware of the risk of misuse of corporate entities in ML schemes and that more focus should be placed on this risk.

Box 6. **Case study: DORADE**

During the investigation of a fraud syndicate, it was revealed that the director of a loan company had set up, with the assistance of various professional accomplices, foreign shell companies located in tax havens for receiving the crime proceeds and lending the sum back to loan company for its legitimate loan business, thereby facilitating the director to evade tax payment and recycle crime proceeds. It was estimated, between 1997 and 2010, a total of CAD 13 million of tax was evaded. With the assistance of MLAT requests, the syndicate members were identified and the proceeds, whether domestic or abroad, were restrained and eventually confiscated. The director and the professionals were convicted of fraud and ML and sentenced to 36–84 months of imprisonment. However, all the ML charges attracted an imprisonment term of less than 18 months and to be served concurrently with the Fraud sentence.

140. Overall, while there are exceptions, law enforcement efforts are not entirely in line with Canada's NRA risk profiles. As previously noted, LEAs' prioritization processes place strong attention to National Security investigations, OCGs, and, to a lesser extent, more recently third-party ML in an international context. Other instances of high threat predicate offenses, especially fraud, corruption, counterfeiting, tobacco smuggling, and related ML, as well as laundering activities in Canada of the proceeds of foreign predicate offenses, third-party ML and ML schemes involving corporate structures are not adequately ranked in the prioritization process and, consequently, are not pursued to the extent that they should.

Types of ML cases pursued

141. Different types of ML and PPOC cases are prosecuted, but there is insufficient focus on the types of ML that are more significant in Canada's context, i.e. ML related to high-risk predicate offenses. In addition, prosecutions of ML-related cases focus on the predicate offenses, with the ML charge(s) often withdrawn or stayed after plea bargaining and re-packaging of charges. The number of standalone ML cases is comparatively low, indicating few investigations and hence prosecutions of third-party ML and foreign predicate offenses despite their high ranking in the NRA. According to the authorities, as far as third-party ML is concerned, the low number of investigations and prosecutions is that the magnitude of the threat has only recently reached a high level. Finally, legal persons are frequently misused for ML purposes, but not often pursued for ML offenses. The tables below show the results of ML cases brought before the courts and the charges laid in these cases.

Table 8. **Results of ML-Related Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	82	108	140	136	146	612	59.6%
Acquitted	2	0	0	4	7	13	1.3%
Stayed	8	12	15	26	18	79	7.7%
Withdrawn	49	63	74	64	53	303	29.5%
Other Decisions	0	0	12	4	4	20	1.9%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 9. **Results of ML-Charges**

	2010	2011	2012	2013	2014	Total	%
Guilty	38	21	35	31	44	169	9.4%
Acquitted	5	1	8	6	9	29	1.6%
Stayed	17	26	144	45	31	263	14.6%
Withdrawn	132	190	366	327	294	1309	72.7%
Other Decisions	2	2	14	7	5	30	1.7%
Total	**194**	**240**	**567**	**416**	**383**	**1800**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

142. Between 2010 and 2014, a total of 1,800 ML charges were concluded in 1,027 cases. Although about 60% of these cases were led to convictions, only 169 ML charges (i.e. some 9%) resulted in a conviction. Some 87% of the ML charges were either withdrawn or stayed. The reasons provided for the withdrawal of the ML charges included insufficient evidence, the lack of public interest in the pursuit of the charges, the avoidance of overcharging, as well as repackaging of charges and plea bargaining (as the ML/PPOC charge will not normally add any additional sentence to the defendant and it is easier for the defendant to accept the guilty plea of the predicate offenses in order to contribute to a fair and efficient criminal justice system). The consultation with prosecutors at an earlier stage of the ML cases is clearly useful in securing the necessary evidence

and avoiding a waste of investigative efforts. The length of criminal proceedings in ML cases is also a concern. Proceedings may take a number of years during which the subjects of the investigation and prosecution may continue their unlawful businesses and dispose of the POCs (as was the case in Project Chun for example).

143. Over the last years, although 68.4% of PPOC cases resulted in convictions, 74.6% of the PPOC charges were withdrawn / stayed or dealt with by other means, and the defendants were only charged with and convicted of the predicate offenses.

Table 10. **Results of PPOC-Related Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	22 974	21 728	20 525	19 611	17 191	102 029	68.4%
Acquitted	388	349	339	404	391	1 871	1.3%
Stayed	2 769	3 193	3 157	3 148	2 857	15 124	10.1%
Withdrawn	5 961	6 140	6 021	5 606	5 380	29 108	19.5%
Other Decisions	255	188	187	163	144	937	0.6%
Total	**32 347**	**31 598**	**30 229**	**28 932**	**25 963**	**149 069**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 11. **Results of PPOC-Related Charges**

	2010	2011	2012	2013	2014	Total	%
Guilty	13 493	12 782	11 178	10 996	10 072	58 521	23.6%
Acquitted	736	715	1 716	674	817	4 658	1.9%
Stayed	9 178	9 715	9 183	9 132	6 894	44 102	17.8%
Withdrawn	28 776	28 388	27 402	27 375	25 130	137 071	55.2%
Other decisions	1 120	912	883	753	416	4 084	1.6%
Total	**53 303**	**52 512**	**50 362**	**48 930**	**43 329**	**248 436**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

144. Overall, of the 1 027 ML-related cases and 102 029 PPOC-related cases that entered the court system, over 60% resulted in convictions, though most of the defendants were convicted of the predicate offenses rather than the ML or PPOC charges. This indicates that Canada is able to investigate and prosecute predicate offenses in ML/PPOC-related cases and disrupt some of the ML/PPOC activities. One hundred sixty-nine ML charges were led to a conviction in the past five years (i.e. 33.8 charges on average annually), which appears very low in light of the magnitude of the ML risks identified. Canada does not pursue the ML charges sufficiently.

Effectiveness, proportionality and dissuasiveness of sanctions

145. The totality principle[56] always applies in the sentencing, and a ML/PPOC sentence is usually ordered to be run concurrently with the predicate offenses. The statistics below indicate the sanctions imposed for ML in instances where the ML charges were the most serious offenses (MSO). The vast majority of natural persons (i.e. 89%) convicted for ML have been sentenced in the lower range of one month to two years of imprisonment or awarded non-custodial sentences.[57] This is proportionate with the type of ML activities most frequently pursued in Canada. However, although this is not made evident in the statistics provided, it is apparent from the case examples provided, and in Projects Dorade and Laurent mentioned above, that many sanctions imposed on money launderers are low even in the (relatively few) cases of complex ML schemes and/or of professional launderers brought before the courts. None of the PPOC convictions attracted a sentence of more than two years. In these circumstances, the sanctions applied do not appear to be of a level dissuasive enough to deter criminals from ML activities.

Table 12. **Sanctions in ML Cases Where ML was the Most Serious Offense, from 2010 to 2014**[1]

	Number	Percentage
Custodial Sentence	**80**	**55.2%**
• Less than 12 months	47	32.4%
• 12 to 24 months	17	11.7%
• More than 24 months	16	11.0%
Conditional sentence, probation, fine, restitution	**65**	**44.8%**
Total	**145**	**100.0%**

1. There are other undisclosed cases where the ML offense runs concurrently with another MSO.

Extent to Which Criminal Justice Measures are Applied Where Conviction is Not Applicable

146. Information provided under IO.8 reveals that non-conviction based forfeiture amounted to 17% of the total forfeiture. Whilst it is not encouraged to drop the criminal charges during the judicial process, Canada's use of civil confiscation is not to be discounted. Plea bargaining and repackaging of charges have also been used in the prosecution stage for shortening the length of court proceedings.

Overall Conclusions of Immediate Outcome 7

147. **Canada has achieved a moderate level of effectiveness for IO.7**.

[56] Totality principle is a common law principle, which applies when a court imposes multiple sentences of imprisonment. Section 718.2(c) of the CC stipulates that when a court that imposes a sentence shall take into consideration of, amongst others, where consecutive sentences are imposed, the combined sentence should not be unduly long or harsh.
[57] A breakdown of sanctions for third-party ML cases and against legal persons is not available.

Immediate Outcome 8 (Confiscation)

148. Since its last assessment, Canada improved its ability to collect information on seizures and confiscations and produce related statistics. It uses both criminal and civil (non-criminal based) proceedings to confiscate proceeds and property related to an unlawful activity. At the Federal level, there is an agency to manage seized and confiscated assets (SPMD). At the provincial level, the management of these assets rests with the prosecution services. Canada also confiscates with no terms of release any undeclared currency and monetary instruments from travellers entering and exiting the country when there is reasonable grounds to suspect they are from illicit origin or that the funds are intended for use in the financing of terrorist activities. It shares confiscated assets with countries with which it has a sharing agreement.

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

149. While confiscation of criminal proceeds and instrumentalities is a policy objective, that objective is pursued to some extent only. Canada is not able to confiscate property of equivalent value; instead, it imposes fines in lieu. As a result of the deficiencies described in IO.7 confiscation relate mainly to proceeds of criminal activities and offence related property conducted by OCGs, in particular drug offenses, fraud, theft, and to the proceeds of tax evasion.

150. Canada's Integrated Proceeds of Crime (IPOC) Initiative aims at the disruption, dismantling, and incapacitation of OCGs by targeting their illicit proceeds and assets. It brings together the CBSA, CRA, PPSC, Public Safety Canada, PSPC (more specifically, its Forensic Accounting Management Group, and the Seized Property Management Directorate), and the RCMP, which cooperate and share information to facilitate investigations. According to the authorities, the IPOC is a distinct program and a corner stone of the AML/CFT regime as a whole as modified in 2000. However, it is not identified as one of the key goals of the latest articulation of the AML/CFT program.

151. The RCMP's Federal Policing Serious and Organized Crime/Financial Crime Teams (which investigate ML cases) target the proceeds of organized crime for seizure. The return of frozen or seized POC and instrumentalities to the defendant is avoided in the context of a plea bargain; in line with the PPSC policy, both POC and instrumentalities must be sought.[58] According to the authorities, the accused normally agree with the confiscation request when they plead guilty. At the provincial level, measures aimed at tracing and seizing assets in view of confiscation are in some cases conducted jointly by the RCMP and the provincial LEA. In the province of Quebec, for instance, the cooperation between the RCMP and the relevant provincial police, i.e. the *Sûreté du Québec*, has shown a number of cases of successful recovery of assets. At the municipal level, the Service de Police of the City of Montreal has a unit specialized in the recovery of POC and in the investigation of ML (*Unité des produits de la criminalité*—Programme UPC-ACCEF). The priority of the investigations in Quebec and in Montreal in particular is clearly to identify assets for confiscation, especially in

[58] According to the PPSC Deskbook, Guideline issued by the Director under Section 3(3)(c) of the Director of Public Prosecutions Act, Chapter 5.3 Proceeds of Crime, in the context of ORP, "partial forfeiture is not a negotiation tool. If the facts justify and application for total forfeiture, Crown counsel may not, as part of negotiations, suggest partial forfeiture."

cases involving OCGs. These clear priorities and effective specialized units have resulted in greater recovery of POC and instrumentalities by criminal law means both in scope and in type of assets, including in more complex ML cases. Other provinces rely more on non-conviction based forfeiture, where roughly CAD 100 million have been confiscated, nationally, during the relevant period.

152. As a general rule, however, LEAs in other provinces and at the federal level do not seem to adopt a "follow the money" approach in practice, nor to initiate a parallel financial investigation, notably because of resource constraints. Overall, as a result of the shortcomings explained under IO.6 and IO.7, asset recovery is pursued to a limited extent only.

Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

153. The total amounts recovered yearly have increased significantly since the previous assessment,[59] but, nevertheless, appear to be low in the Canadian context (see table below). This is likely to be due to the lack of focus on asset recovery mentioned above and the shortcomings mentioned in IO.6 and IO.7, as well as the length of time needed to bring cases to closure: The delays encountered (especially at the tracing stage) are likely to encourage and facilitate the flight of assets.

Table 13. **Amounts Forfeited in Canada**[1]
(in Canadian Dollars)

	Criminal Federal Forfeiture	Federal Fines in Lieu	CBSA Cash Forfeitures	Civil Forfeiture Results (Nationally)	Québec Criminal Provincial Forfeiture	Total
2009/10	46 368 327	101 600	5 277 676	7 600 000	---	59 347 604
2010/11	58 872 881	71 650	4 698 404	12 400 000	9 070 456	85 113 392
2011/12	77 698 566	31 700	1 960 038	18 900 000	10 905 959	109 496 264
2012/13	83 935 230	105 939	3 468 888	41 700 000	11 498 811	140 708 870
2013/14	75 997 602	312 178	4 054 089	18 900 000	12 453 244	111 717 114
2014/15	72 869 240	314 217	4 076 586	---	---	77 260 044
Total In CAD	415 741 848	937 285	23 535 683	99 500 000	43 928 471	583 643 289

The table is a consolidation of statistics maintained by different authorities, using different criteria and does not include forfeitures undertaken by federal departments that do not involve or are not reported to the SPMD. At the provincial level, figures were provided for Quebec only (federal criminal results for Quebec appear in the first column). They do not differentiate domestic from foreign predicate offenses (though IO.2 shows that there have been forfeitures based on the direct enforcement of foreign orders) and proceeds which have moved to other countries. According to the authorities, the link between seized and forfeited assets cannot easily be made, as these actions occur over multiple years.

154. Different types of assets are seized or restrained in federal criminal proceedings (see table below) but, overall, Canada does not restrain businesses, company shares—despite the high risk of misuse of legal entities—or property rights. [60] In general, Canadian authorities seem to be managing

[59] An average of Can$ 27 million a year were forfeited from 2000 to 2007 (2008 MER, page 62).
[60] The only exception appears to be a golf course seized on behalf of another country.

effectively the seized and confiscated assets on both federal and provincial levels. Assets are generally not sold before the conclusion of the criminal proceeding to maintain their value or reduce the costs of management of the property, unless they are rapidly depreciating or perishable, or the accused authorizes their disposal.

Table 14. **Federally Seized/Restrained Assets by Appraisal Value**
(in Canadian Dollars)

Asset Type	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015
Aircraft	108 000	-	15 000	-	250 000	0
Cash	20 878 443	21 456 803	22 665 264	28 833 075	18 036 703	21 680 932
Financial Instruments	365 247	961 557	5 938 052	732 443	26 924 056	723 834
Hydroponics	6 291	2 748	808	1 240	259	12
Other Property (incl. jewellery)	138 410	684 780	605 054	274 601	203 956	269 866
Real Estate	52 785 401	54 220 901	37 336 935	25 445 169	26 532 406	16 758 250
Vehicle	5 940 355	5 947 937	6 256 389	4 839 410	4 479 067	4 433 720
Vessel	311 200	156 101	79 296	121 661	39 700	518 000
Grand Total	**80 533 349**	**83 430 829**	**72 896 801**	**60 247 601**	**76 466 149**	**44 384 616**

155. Revenue agencies, both at the federal and provincial level, have been successful in recovering evaded taxes, including in instances where the monies were held offshore. In FY 2013/2014, Revenue Quebec alone recuperated over CAD 3.5 billion of evaded taxes, both by criminal sanctions and civil compliance actions. During the same period, FY 2013/2014 the CRA recuperated CAD 10.6 billion in its criminal and civil actions. As a result of the CRA's investigations into suspected cases of tax evasion, fraud and other serious violations of tax laws, and recommendations to the PPSC, Canada secured convictions for tax crimes for CAD 162.3 million and levied a total of CAD 70.7 million in criminal fines. However, it should be noted that these figures do not solely represent confiscations related to the proceeds of crime, and that the Canadian authorities were unable to provide such separate figures.

156. Between 2008 and 2015, in an effort to recover proceeds that have been moved to other countries, Canada sent 135 requests for tracing assets (bank or real estate records) to other countries 43 requests for restraint of funds or assets and 4 requests for forfeiture. Discussions with the authorities and the cases provided nevertheless established that the authorities pursue assets abroad to some extent only, notably because such actions require resources that are currently dedicated to other priorities. The fact that LEAs seem to have little expertise in pursuing complex international ML schemes or in the investigation of professional money launderers also explain the relatively low level of effort in seeking the recovery of assets abroad. Considering that there is no possibility for the authorities to seize property of equivalent value, when POC cannot be forfeited, fines in lieu are ordered, in addition to the custodial sentence. The total fines collected by the federal Crown are CAD 937 285.95 for 2009-2015. The authorities share parts of the confiscated assets with

their foreign counterparts, both in criminal and civil actions, when the property is in Canada, the foreign country assisted Canada in the case and there is a signed sharing agreement. This would be the case when the offense was committed partly or entirely abroad and laundered in Canada.[61] The major part of the sharing occurred with the US, which appears justified in the Canadian context, and property was also shared with Cuba and the UK.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

157. CBSA agents seize monies when there is a suspicion that the latter are POC or funds intended to be used to fund terrorism. As indicated in the table below, between 2009 and 2015, Canada seized about CAD 263 million at the border, of which less than 9% were confiscated and more than 91% were returned to the travellers. In the latter cases, according to the authorities, there was no suspicion of ML, TF, or other illicit activities; therefore, the monies were returned to the traveller and an administrative fixed fine (of CAD 250, CAD 2 500, or CAD 5 000) levied. In practice, however, falsely or undeclared cross-border movements of currency and other bearer negotiable instruments are analysed by the FIU, or investigated by the RCMP to a very limited extent, namely only when they pertain to an ongoing analysis or investigation (See IO.6). Moreover, the level of the sanctions for noncompliance with the obligation of disclosure of cross-border movements and the frequency which it is applied does not seem effective, proportionate nor dissuasive.

(in Canadian Dollars)

FY	Seized Amount	Returned at Seizure by CBSA	Final Penalty Amount Forfeited	Cash Seizures Forfeited	Amount Returned by SPMD[1]
2009/2010	99 430 742	94 448 985	2 150 500	5 277 676	731 782
2010/2011	12 447 605	6 277 108	223 000	4 698.404	1 458 233
2011/2012	4 361 463	1 871 650	50 750	1 960 038	522 035
2012/2013	28 273 318	23 949 256	545 500	3 468 888	853 173
2013/2014	52 508 920	47 564 857	1 340 000	4 054 089	873 782
2014/2015	65 989 388	61 808 579	1 732 000	4 076 586	1 328 046
Total	263 011 436	235 920 435	6 041 750	23 535 681	5 767 054

1. This column contains only the amounts for closed cases where an appeal or other legal means of challenging are no longer available to the travellers.

[61] Canada shared the following amounts: 2007/2008: CAD 199 390; 2008/2009: CAD 75 620; 2009/2010: CAD 357 844; 2010/2011: CAD 0; 2011/2012: CAD 93 013; 2012/2013: CAD 237 577; 2013/2014: CAD 244 846.

Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities.

158. Law enforcement actions, including asset recovery efforts focus mostly on illicit drug trafficking, fraud, and theft.[62] While drug-related offense and fraud are identified as very high ML threats in Canada's NRA, theft is not. In addition, the recovery of proceeds of other very high threats identified in the NRA is pursued, but not to the same extent (this is notably the case for proceeds of corruption and bribery, third-party ML, and tobacco smuggling, although some success was achieved in a case of tax evasion perpetrated from 1991 to 1996 in relation to a large scale tobacco smuggling operation[63]).[64] As a result, Canada's confiscation results are not entirely consistent with ML/TF risks or national AML/CFT policy.

Overall Conclusions on Immediate Outcome 8

159. **Canada has achieved a moderate level of effectiveness in Immediate Outcome 8.**

[62] As stated in the Research Brief-Review of Money Laundering Court Cases provided by FINTRAC, p. 1 and the Authorities Submissions to IO.7, p. 12 and 13. This is consistent with the assessor's findings after the interviews with Canadian authorities during the on-site.
[63] Project Oiler, where charges of tax fraud (through smuggling) and the possession of proceeds of crime were laid in 2003 and ultimately a plea of guilty accepted for violations of the Excise Tax Act in 2008 and 2010. This case resulted in the imposition of criminal fines and penalties totalling CAD 1.7 billion.
[64] The authorities provided the assessment team with a table showing the seizures in relation to the offenses (Seizures by Act), from 2009 until 2015. The higher values are related to the Controlled Drug and Substance Act, followed by the offense of Possession of property obtained by crime, laundering of proceeds, PCMLTFA, tax offenses and conspiracy. The values seized in relation to bribery of officers are insignificant (except in one case where some CAD 4 million were confiscated). It is not possible to identify third-party ML in the statistics provided. Seizures for possession of tobacco appear only in fiscal years 2012/2013 and 2013/2014, and seizure for bribery of officers appear only in FY 2010/2011, 2011/2012 and 2013/2014. In FY 2009/2010, 2012/2013 and 2014/2015 the value of seizures in relation to bribery is zero.

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

IO.9

The authorities display a good understanding of TF risks and close cooperation in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations.

Canada accords priority to pursuing terrorism and TF, with TF investigation being one of the key components of its counter-terrorism strategy.

The RCMP duly investigates the financial components of all terrorism-related incidents, considers prosecution in all cases and the prosecution services proceed with charges when there is sufficient evidence and it serves the public interest. Two TF convictions were secured since 2009. Sanctions imposed were proportionate and dissuasive.

Canada also makes frequent use of other measures to disrupt TF.

IO.10

Implementation of TF-related targeted financial sanctions (TFS) is quite effective for FIs but not for DNFBPs.

Canada takes a RBA to mitigate the misuse of NPOs (i.e. charities). A specialized division within CRA-Charities focuses specifically on concerns of misuse of organizations identified as being at greatest risk. In addition, CRA-Charities has developed an enhanced outreach plan, which reflects the best practices put forward by the FATF.

In practice, few assets have been frozen in connection with TF-related TFS.

IO.11

Canada's Iran and DPRK sanction regimes are very comprehensive and in some respects go beyond the UN designations.

Cooperation between relevant agencies is effective and some success has been achieved in identifying and freezing the funds and other assets belonging to designated individuals.

Large FIs have a good understanding of their TFS obligations and implement adequate screening measures but some limit their screening to customers only. DNFBPs, however, are not sufficiently aware of their obligations and have not implemented TFS.

There is no formal monitoring mechanism in place; while some monitoring does occur in practice, it is limited to FRFIs and is not accompanied by sanctioning powers in cases of non-compliance.

4

Recommended Actions

Canada should:

IO.9

- Pursue more and different types of TF prosecutions.

IO.10

- Require DNFBPs to conduct a full search of their customer databases on a regular basis.
- Consider increasing the instances of proactive notification of changes to the lists to REs other than FRFIs.
- Consider enhancing the number of seizures and confiscations related to TF offenses.

IO.11

- Monitor and ensure FIs' and DNFBPs' compliance with PF-related obligations.
- Conduct greater outreach. This should include information on the PF-risk that can be published without compromising Canada's security, as well as more detailed guidance on the implementation of TFS and indicators of potential PF activity.

The relevant Immediate Outcomes considered and assessed in this chapter are IO9-11. The recommendations relevant for the assessment of effectiveness under this section are R.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

160. The RCMP investigates all occurrences of TF. This includes investigations into a wide range of TF activities, such as the collection of funds and their movement and use by individual, entities or wider organizations. The RCMP lays TF charges when approved by PPSC based on sufficient evidence and when the prosecution would best serve the public interest. Between 2010 and 2015, charges were laid against one individual, resulting in a conviction for TF in 2010 (see Box 7 below). Charges were also laid in another case, but subsequently withdrawn for tactical and operational enforcement reasons.

Box 7. **R v. THAMBITHURAI 2008**

It came to the knowledge of the RCMP's Integrated Security Enforcement Team (INSET) that a man was in the process of collecting funds from his place of residence and businesses for the Liberation Tigers of Tamil Eelam (LTTE), a listed terrorist entity in Canada. The person was arrested in Vancouver. INSET found various materials in his possession, including donation forms for the LTTE which were used for a CAD 600 donation and a CAD 300 pledge. The accused was charged with four counts of "Providing or making available property for a terrorist organization" under CC 83.03, three of which were later withdrawn. He pled guilty in 2010 and was sentenced to six months of imprisonment.

161. LEAs actively pursue the threat of individuals radicalized to violence, and in particular, those seeking to travel abroad for terrorist purposes. The RCMP's priority is to pursue charges that are in the best interest of public safety, and to mitigate the possible threat of terrorist activity as efficiently as possible. TF charges are not always determined to be the most appropriate means to mitigate threat. In these instances, alternative measures are used. The below case showed that while a boy obtained funds by robbery for travel abroad to join a terrorist organization, RCMP had pursued terrorism and criminal charges instead of TF charges.

Box 8. **Young Foreign Terrorist Fighter**

In 2014, a 15-year-old boy who had become radicalized to violence became determined to travel abroad to join a terrorist organization. He had previously tried unsuccessfully to purchase an airline ticket for Syria with his father's credit card. In October 2014, the father discovered CAD 870, a knife, and a balaclava in the boy's backpack. Feeling suspicious of money might have been stolen, the father made a report to police. Investigation revealed that the boy had committed an armed robbery in order to purchase ticket for Syria. The boy was charged and convicted of armed robbery. Additional national security investigation by C-INSET resulted in the youth being convicted of attempting to leave Canada to participate in the activity of a terrorist group (CC 83.131) and commission of an offense for a terrorist group (83.2). He was sentenced to 24 months in youth custody plus one-year probation, consecutive to the sentence of armed robbery.

162. This and other cases discussed establish the authorities' ability to pursue TF activities. However the results obtained so far are not entirely commensurate with Canada's risk profile, which, as assessed in the NRA, points to more frequent and diverse TF occurrences. As a result, Canada has demonstrated to some extent that it pursues the different types of TF activities that it faces.

TF identification and investigation

163. The RCMP investigates the financial component of all terrorism-related incidents. It employs various avenues to identify and investigate potential TF activities including human source

or intelligence, referrals from international or domestic partners (e.g. the US Federal Bureau of Investigations (FBI), FINTRAC, CRA, and CSIS, direct reporting from Canadian FIs), and national security investigations.

164. FINTRAC regularly provides proactive disclosures and responses to VIRs on TF cases, which supports the prioritization of TF investigations. It mostly disseminates disclosures related to TF to CSIS, but also to the RCMP, CBSA, CRA, municipal and provincial police, and foreign FIUs. According to FINTRAC, roughly half of TF disclosures were proactive, and half in response to VIRs. The authorities do not keep figures on the results of TF investigations arising from proactive disclosures.

Table 15. **TF-Related VIRs and FINTRAC Disclosures (from and to RCMP only)**

	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Number of TF Disclosures	100	110	125	188	206	729
Number of TF-Related VIRs	26	65	78	84	61	314

165. LEAs and FINTRAC accord priority to TF investigations, although there are exceptions where priority would be accorded to other terrorism files, as highlighted in the Project Investigation below. In urgent cases, FINTRAC provides TF-related financial intelligence to the RCMP within hours. In normal circumstances, it may take days or weeks to respond to the VIRs. In one of the cases provided, which dated back more than 10 years, timely intelligence from FINTRAC was instrumental in identifying domestic and foreign accounts, as well as in establishing the foundations for the necessary judicial authorization applications.[65] The CBSA also assists in the identification of an investigation into TF activities.

166. For example in the case of Project Investigation, a person was intercepted by the CBSA at a Canadian airport for carrying undeclared currency in excess of CAD 10 000. CBSA notified the RCMP, which assumed control of the investigation because of the nexus to TF. The investigation revealed that funds destined to a foreign country to support an organization listed by Canada as a terrorist entity had been collected across Canada by multiple individuals. Information received from FINTRAC resulted in the identification of the funding networks of the entity and of its key members. Due to operational and resource constraints imposed by higher priority national security investigations, the RCMP was unable to proceed further with the file. A different approach was therefore adopted: the suspect was charged under PCMLTFA for not reporting the importation or exportation of currency

[65] The case in question was the Project Saluki: In 2002, the RCMP conducted a TF investigation to determine whether monies were being raised in Canada by a front organization, the World Tamil Movement (WTM), for the LTTE in Sri Lanka. Financial Intelligence provided by FINTRAC and banking records from FIs obtained by a court order indicated that funds were being sent from a bank account in Canada to a bank account in a foreign country registered to a legal entity. With the assistance of the foreign country, the RCMP gathered the bank documents of the foreign account and identified the holders and the persons associated with or who maintained control over the account, which involved a private deed of trust as well as a list of the appointed trustees. RCMP officers went to the foreign country, interviewed the trustees and signatories of the foreign bank account and determined details of their involvement and position with the legal entity. No person was charged upon the conclusion of the investigation. The PPSC applied for civil forfeiture and in 2010 the Court ordered forfeiture of the WTM building in Montreal and other property under terrorism legislation.

or monetary instruments. He pleaded guilty and was fined CAD 5 000, and the funds previously seized were forfeited to the Crown.

167. All TF investigations are conducted by the RCMP's INSET field units. These units are located in Vancouver, Edmonton, Calgary, Toronto, Ottawa, and Montreal, and are comprised of officers deployed from other partners (including municipal and provincial LEAs and the CSIS) in numbers that fluctuate depending on operational needs. They are tasked by FPCO, which it is responsible for the prioritization of investigations. TF activities are investigated in proportion with their scope and complexity. As investigations become more complex and require more resources, the RCMP uses a management tool to ensure that investigations align with national security priorities. Between 2009 and 2013, it identified five investigations as major TF cases, which led to two charges being laid (see previous core issue).

Table 16. **TF Investigations**

	2010	2011	2012	2013	2014	Total
Assistance Files[1]	235	162	117	201	179	**894**
Participate/Contribute to Terrorist Group Activity	40	29	33	45	52	**199**
Provide/Collect Property for Terrorist Activity	31	26	17	21	9	**104**
Information Files[2]	30	31	15	25	34	**135**
Crime Prevention3	0	2	1	2	79	**84**
Facilitate Terrorist Activity	15	3	6	10	15	**49**
Make Available Property/Service for Terrorist Act	10	15	8	5	8	**46**
Suspicious Person/Vehicle/Property	0	1	6	9	2	**18**
Use/Possess Property for Terrorist Activity	4	1	2	1	0	**8**
National Security Survey Codes[4]	1	1	0	4	0	**6**
Instruct/Commit Act for Terrorist Group	2	3	0	1	3	**9**
Others (Criminal Intelligence, Fraud, etc.)	5	3	6	5	4	**23**
Total	**373**	**277**	**211**	**329**	**385**	**1 575**

1. An Assistance file is created when assisting domestic or foreign non-PROS/SPROS units or agencies.
2. Information File is information received, it is not a call for service, or the person or agency supplying the information does not expect police action.
3. Crime Prevention are activities directed toward the tangible objective of preventing a specific type of crime, e.g. breaking and entry, approved or accepted community-based policing program such as Drug Abuse Resistance Education (DARE).
4. National Security Survey Codes are the combined collection of two different survey types: Threat Assessments and VIP/Major Events.

TF investigation integrated with -and supportive of- national strategies

168. CFT is an integral part of Canada's strategy to combat terrorism. The RCMP confirms that it assesses the existence of a TF component in every national security investigation. Cases provided (including IRFAN-CANADA described in IO.10) showed that the authorities use TF investigations to identify the structures, key persons, and activities of terrorist organizations. TF investigations are integrated with, and used to support, national counter-terrorism strategies and investigations.

Effectiveness, proportionality and dissuasiveness of sanctions

169. Canada successfully pursued and convicted two individuals on TF charges. The first case (*R v. THAMBITHURAI* described above) only attracted a six-month imprisonment despite PPSC appealing against the sentence. In the second case (*R v. KHAWAJA*, see Box 9 below), the Court sentenced the defendant to two years imprisonment for TF and to life imprisonment for "developing a device to activate a detonator."

Box 9. **R v. KHAWAJA**

In 2004, Canada initiated an investigation into a Canadian citizen linked to a terrorist group under investigation in the United Kingdom (UK) for planning a fertilizer bomb attack targeting pubs, nightclubs, trains and utility (gas, water and electric) supply stations in the UK. The evidence collected indicated that the Canadian subject attended a training camp in Pakistan in July 2003 and transferred on three occasions a total of about CAD 6 800 to his associates in the UK with the help of a young woman to avoid suspicion of link. His parents were persuaded to evict tenants from their residence in Pakistan so that the subject may make the facility available for use by the group's members. He also planned 30 devices to strap explosives onto model airplanes with remote triggers. He was arrested by the RCMP in 2004, detained, and charged in 2008 with seven counts of offenses under the CC, including one count of TF under 83.03(a). MLA requests were sent to the US authorities for the subject's Internet Service Provider and payment records as well as the testimony of a US witness. In December 2010, upon the appeal by the PPSC, the subject was sentenced to life imprisonment for "developing a device to activate a detonator" and 24 years of imprisonment for the other offenses, including two years' imprisonment for TF.

170. While low, the number of instances prosecuted appears in line with Canada's threat profile and considering the alternative mitigating measures taken (see below). Sanctions applied appear to be proportionate with the amounts involved and dissuasive. No legal person has been convicted of TF offenses. No designations were made to the relevant UN bodies but Canada has been co-sponsor to a number of designations.

Alternative measures used where TF conviction is not possible (e.g. disruption)

171. Canada's primary goal in counter terrorism efforts is to maintain public safety, and Canada places a strong focus on disrupting terrorist organizations and terrorist acts before they occur. The RCMP defines disruption in national security matters as the interruption, suspension or elimination, through law enforcement actions of the ability of a group(s) and/or individual(s) to carry out terrorist or other criminal activity that may pose a threat to national security, in Canada or abroad. It includes disruption of TF activities

172. During national security investigations, activities of participants and peripheral participants may be tactically disrupted for a variety of reasons, including triggering reactions or behavioural changes of the main targets. TF investigations therefore do not always result in TF

charges, if other charges for terrorism or other offenses are being laid and the evidence is most cogent and appropriate or would best serve the public interest. The authorities shared several cases (including Project Smooth below) where despite clear evidence to substantiate a TF charge, other means were preferable to ensure the public interest.

Box 10. **Project SMOOTH**

In August 2012, CSIS reported to RCMP that a male ("CE") residing in Montreal had met another male ("RJ") in Toronto. RJ was known to the RCMP for recently distributing pro Al-Qaeda propaganda. Investigation, including the use of an undercover US FBI agent who had gained the trust of CE and RJ, revealed that the two men had plotted to cut a hole in a railway bridge to derail the Canadian Via Rail passenger train between Toronto and New York. The FBI agent had surreptitiously recorded their conversations, which made up the bulk of the case's evidence, including CE's description on the hierarchical structure and mode of communication of a terrorist group and that CE was receiving orders from Al Qaeda through a middleman. It was also unveiled during the investigation that CE had or intended to finance a total of CAD 4 200 to the terrorist group. In 2013, CE and RJ were arrested. CE and RJ were both charged with four offenses: conspiring to damage transportation property with intent to endanger safety for a terrorist organization, conspiring to commit murder for a terrorist group, plus two counts of participating or contributing to a terrorist. CE was found guilty of all four charges plus another he faced alone for participating in a terrorist group. RJ was convicted of all charges except that of "conspiring to damage transportation property with intent to endanger safety for a terrorist organization." In March 2015, both men were sentenced to life imprisonment.

173. In other cases, TF prosecutions were not possible, especially in cases based largely on intelligence that may fall short of the evidentiary threshold required by criminal courts. In instances where prosecution is not deemed to be the best avenue to protect the public or human sources, or is not possible, a wide-range of disruption techniques is employed. Such techniques typically include: arrests; search-and-seizure raids; "intrusive surveillance" (in which police make it obvious to the suspects that they are being watched); civil forfeiture; inclusion of specific persons in Canada's no fly list (which is particularly relevant considering the growing threat of foreign fighters); revocation of the charitable status of NPOs identified as having been used for TF purposes; listing of terrorist entity under the CC, barring of individuals who pose a threat to the security of Canada and prohibition from entering or obtaining status in Canada or from obtaining access to sensitive sites, government assets or information; and extradition. Canada frequently uses other criminal justice and administrative measures to disrupt TF activities when a prosecution for TF is not practicable.

Overall Conclusions on Immediate Outcome 9

174. **Canada has achieved a substantial level of effectiveness for IO.9**.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

175. Canada implements UNSCR 1267 and UNSCR 1373 (and their successor resolutions) through three separate domestic listing mechanisms: the United Nations Al-Qaeda and Taliban Regulations (UNAQTR); the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST); and the CC. Canada plays an active role in co-sponsoring the listing of new terrorist entities, as appropriate, and delisting defunct entities. The lists of entities whose assets are to be frozen under UNSCR 1267 and its successor resolutions are automatically incorporated into Canadian law by reference through UNAQTR. Accordingly, UNSC decisions to list or delist an individual are given immediate effect in Canada; no additional action by Canadian authorities is needed to give legal effect to a designation. These decisions are rapidly brought to the attention of FRFIs, but not of other REs.

176. The CC is Canada's primary listing mechanism, and allows it to satisfy the obligations under UNSCR 1373. While the RIUNRST also satisfies UNSCR 1373, no listings have been added to the RIUNRST since 2006. In practice, this CC process entails a criminal intelligence report prepared by the RCMP or a security intelligence report prepared by the CSIS, which is subjected to a legal review by independent counsel to ensure that it meets the CC listing threshold (i.e. reasonable grounds to believe), as well as interdepartmental consultations. The authorities can list an entity to Canada's domestic list (under the CC) in an expedited manner if necessary.[66] The Canadian authorities provided a concrete example (IRFAN Canada, below) of the domestic listing of a NPO.

Box 11. **IRFAN-Canada**

In 2010, CRA-Charities suspended the receipting privileges of IRFAN-Canada. The suspension was based on the organization's failure to provide and maintain records, which interfered with CRA-Charities' ability to carry out the audit that began in 2009. CRA-Charities continued with the audit during the period of suspension and ultimately revoked IRFAN-Canada's charitable registration in 2011. It shared information regarding IRFAN-Canada's possible association with the listed organization, Hamas, with partner organizations, including the RCMP. A CRA-Charities analyst seconded to the RCMP was able to provide expertise to facilitate the sharing of information, as authorized by legislation. The RCMP collaborated with and received financial intelligence from FINTRAC.

In 2014, the RCMP officially opened the investigation, which resulted in an RCMP recommendation to PS Canada to have IRFAN-Canada listed as a terrorist organization. The financial intelligence provided by FINTRAC also served to inform deliberations on the listing of IRFAN. The RCMP, PS Canada, and the DOJ worked together to prepare the documentation required for the Government to make a decision as to the listing. In April 2014, IRFAN-Canada was listed as a terrorist entity by the Government of Canada. Following the listing, criminal investigations were initiated by the RCMP's INSETs in Ontario and Quebec, and were still ongoing at the time the assessment.

[66] Several factors may be considered, as for example: operational imperative to list more quickly to freeze known assets; nexus to Canada; national security concerns; allied concerns, etc.

177. Third-party requests from foreign jurisdictions are considered under the CC framework. Canada has received numerous requests from foreign jurisdictions since the establishment of the regime and has given effect to both formal and informal requests, though it does not keep records on the number of third-party requests for listing under the CC. The authorities also indicated that they were able to list an entity on an expedited manner when necessary, following third-party requests.

178. As of 7 April 2015, 54 entities were listed pursuant to the CC and 36 terrorist entities under the RIUNRST. Once an entity has been listed, PS issues a news release advising of the new listing and provides a notification on its sanctions website, and the listings are published in the Canada Gazette, approximately two weeks after listing. To assist FIs search their list of customers against these listed terrorist names, OSFI maintains on its website a database of all terrorist names (and known identifiers) subject to Canadian laws, and notifies FIs without delay by posting instantly a notification to its website and by notifying all its e-mail subscribers each time a new terrorist name is listed under Canadian law, or there are changes to existing information. FRFIs are also required to report to OSFI monthly that they have conducted the name screening and report any terrorist property that they have identified and frozen. FINTRAC also provides a link to OSFI's website on its own website, as well as guidance to REs on the reporting requirements related to terrorist property. Other than in the case of OSFI, the mechanism for informing the private sector about listed entities appears to be rather passive, as it relies on REs consulting the Official Gazette and the websites of the competent authorities and/or, when they are aware of this possibility, subscribing to RSS feeds (or the UN notification system).

179. The FRFIs met during the on-site had a good understanding of their screening obligation regarding targeted financial sanctions (TFS) and implemented sanctions without delay. DNFBPs, however, do not have a good understanding of their obligations (see IO.4). Furthermore, while they are required to check the listings at the beginning of a business relationship, they are not required to conduct a full search of their customer databases on a regular basis, which is a major limitation to an effective implementation of TFS.

180. Persons listed in Canada may apply for revocation of the designation under the framework detailed in R.6.[67] Examples of delisting were shared with the assessors. One entity was delisted in December 2012.

181. Canada has not proposed a designation to the UN Sanctions Committees, but acted as co-sponsor on several occasions.

Targeted approach, outreach and oversight of at-risk non-profit organisations

182. The Canadian NRA concluded that registered charities present a high risk of TF, due to the fact that a large number of the financial transactions that charities conduct may be performed via delivery channels with a high degree of anonymity and some level of complexity (i.e. multiple

[67] Under the Criminal Code regime, there are several ways an entity could be delisted. The Minister of Public Safety and Emergency Preparedness can recommend to the Governor in Council that an entity be delisted at any time, the entity could be recommended for delisting as part of the two-year review, or an entity can apply for delisting as per the process outlined under section 83.05(2).

intermediaries are involved). The NRA also highlights that the significant use of cash may make it difficult for the authorities to establish the original source of funds, and that it may be difficult to know how the funds or resources will be used once transferred to partner organizations or third parties.

183. Canada has implemented a targeted approach regarding the NPO sector vulnerability to TF. In 2015, the CRA, which regulates charities under the Income Tax Act, conducted a review in addition to the NRA, to examine the size, scope and composition of the NPO sector in Canada and to determine which organizations, by virtue of their activities and characteristics, were at greater risk of being abused for terrorist support purposes. The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse because of the nature of their activities and characteristics are charities. As a result, the authorities concluded that, in the Canadian context, NPOs that fall within the FATF definition are charities. Four reports had previously been published regarding the sector, notably a "Non-profit Organisation Risk identification project" in 2009. Canada has a large NPO sector, comprising of approximately 180 000 organizations. The sector can be divided into two groups: charities and NPOs, depending on their legal structures. While both are exempt from paying taxes, federally registered charities (of which there are approximately 86 000) receive additional fiscal privileges and submit annual information returns, which include notably the names of the directors or trustee, a description of its activity and financial information, including sources of funding. Non-charity NPOs (of which there are approximately 94 000) having assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 are not required to register, but must file an annual NPO Information Return with the CRA.[68] In addition, non-charity NPOs incorporated provincially or federally would be required to file certain information with the provincial or federal governments on an annual basis depending on the statute under which the organization is formed. This typically includes information related to address, directors, and the date of the last general meeting. In certain cases, organizations may have to provide detailed financial information depending on value of assets or fund received.

184. CRA-Charities reviews all applications for charitable registration and conducts audits of registered charities. From 2008–2014, CRA-Charities completed approximately 5 000 audits in total; 16 these audits comprised a national security concern, eight of which resulted in revocation of registration.[69] If an applicant charity does not meet the requirements of registration, e.g. due to terrorism concerns, the CRA denies its application.[70] Through its work, CRA-Charities may take administrative action to disrupt an organization's activities where it has identified a risk of terrorist abuse, and/or relay the information to LEAs. If a registered charity no longer complies with the requirements of registration, for any reason including connections to terrorism, the division can

[68] The annual NPO Information Return includes information about their activities, assets and liabilities.
[69] Two led to penalties totalling CAD 440 000; four led to compliance agreements with the charity involved and two resulted in education letters.
[70] The Income Tax Act requires that charities devote their resources to charitable purposes and activities. An organization that supports terrorism would be denied registration for carrying on activities contrary to public policy, which would not qualify as charitable. Additionally, the Charities Registration (Security Information) Act provides a prudent reserve power to deny or revoke registration when terrorist connections are suspected.

apply a range of regulatory interventions and, in the most the serious cases, may revoke the registration.

185. CRA-Charities conducts outreach to advise charities of their legislative requirements and how to protect themselves from terrorist abuse. This includes general guidance on topics related to sound internal governance, accountability procedures, and transparent reporting, as well as specific tools such as a checklist on avoiding terrorism abuse and a web page on operating in the international context. CRA-Charities will build on this existing outreach through its enhanced outreach plan. CRA-Charities has begun consultations with the sector to educate them on the risk of terrorist abuse and to gain a better understanding of their needs in terms of outreach and guidance.

186. National coordination has been enhanced. The CRA shares information with relevant partners where there are concerns that a charity is engaged in providing support to terrorism. If the division encounters information that is relevant to a terrorism investigation when carrying out its regulatory duties, it shares that information with national security partners and LEAs. The division shared information with domestic national security partners in support of their mandate in 47 cases. Similarly, the division received information from partners in 51 cases to assist with its analysis, in 2014/2015. In addition, to facilitate the sharing of information, a secondment program between the CRA and its partners has been instituted: CRA employees are seconded to the partner agencies and employees from the partner agencies are seconded to the CRA.

187. According to the CRA's NPO Sector Review of 2015 the 86 000 registered charities represent 68% of all revenues of the NPO sector and nearly 96% of all donations (see R.8). CRA registered charities also account for a substantial share of the sector's foreign activities as about 75% of internationally operating NPOs are registered as charities. In addition, as detailed above, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 must file an annual information return with the CRA, which includes the provision of financial information. In addition, registered charities with revenue in excess of CAD 100 000, and/or property used for charitable activities over CAD 25 000, and/or that have sought permission to accumulate funds, must provide more detailed financial information. The authorities identify charities as being the organizations falling under the FATF definition of NPOs and reviewed the NPO's sector (see Box 12).

Box 12. **Canadian NPO's Sector Review**

The national regulator of registered charities, i.e. the CRA, conducted a domestic review of the entire NPO sector in Canada in order to identify which organizations, by virtue of their activities and characteristics, were at greater risk of being abused for terrorist support purposes. The review aimed to ensure that Canada (i) is not taking an overly broad interpretation of the FATF definition of NPO, (ii) focuses on those organizations that are at greatest risk, and (iii) does not burden organizations that not at risk with onerous reporting requirements for TF purposes.

The CRA reviewed existing publications and research by governmental, academic, and non-profit organizations related to the non-profit sector, including reports by Statistics Canada on non-profit institutes, consultations on regulations affecting the sector, and studies on trends in charitable

giving and volunteering. In addition, it looked at existing laws and reporting requirements affecting NPOs. To determine where there is risk, NPOs were categorized based on shared characteristics such as purpose, activities, size and location of operation. The CRA compared those characteristics with the elements of the FATF definition of NPO. It also took into consideration the findings of the FATF typologies report Risk of Terrorist Abuse in NPOs to identify features that put organizations a greater risk.

The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse are charities. As a result, the authorities concluded that, in the Canadian context, only charities fall within the FATF definition of NPO. While organizations at greatest risk are charities, not all charities are at risk. The insight obtained from the sector review allowed Canada to focus on charities as the starting point for its NRA.

Source: FATF (2015), Best practices paper on combating the abuse of NPOs—October 2015.

188. The registered charity met during the assessment is large and has a number of international connections. It has a good understanding of its vulnerability to TF and has implemented adequate measures to mitigate that risk, without disrupting legitimate NPO activities.

Deprivation of TF assets and instrumentalities

189. As of February 2015, the total amount of frozen assets belonging to designated entities is CAD 131 235 in 12 bank accounts, CAD 29 200 in six life insurance policies, nine house insurance policies, and one automobile insurance policy, totalling CAD 3 248 612 frozen. The number of entities that had their assets frozen was not provided.

190. Despite the high number of TF occurrences (see IO.9), no assets and instrumentalities related to TF were seized or confiscated in circumstances other than designations. There are several reasonable explanations for this. LEAs indicated that, in several cases, no assets or instrumentalities were found. In others cases, the lack of confiscation can be due to the fact that TF investigations do not always result in TF charges and other means of disruption (see IO 9). The authorities also provided cases of TF investigations unrelated to the UN designations where the RCMP seized some assets and instrumentalities,[71] but did not proceed to seek their confiscation.

Consistency of measures with overall TF risk profile

191. While the terrorist threat has grown in the recent years, in particular in light of an increased number of Canadian nationals who have joined terrorist groups abroad,[72] not all terrorist entities identified have financing or support in Canada. In October 2014, Canada was victim of two

[71] The assets seized included over CAD 10 000 in cash, in one case, and tractor trailers in another.
[72] As stated by the Director of CSIS following his appearance at the Senate Committee on National Security and Defence, as of the end of 2015, the Government was aware of approximately 180 individuals with Canadian a nexus who were abroad and suspected of engaging in terrorism related activities. The Government was also aware of a further 60 extremist travellers who had returned to Canada.

terrorist attacks in Saint-Jean-sur-Richelieu and Ottawa, perpetrated by two Canadian citizens who intended to travel abroad for extremist purposes, but had been prevented from doing so. The TF investigation related to these events was still ongoing at the time of the assessment. In other instances, the authorities detected the transfer of suspected terrorist funds to international locations. These transfers had been conducted through a number of methods, including the use of MSBs, banks, and NPOs, as well as smuggling bulk cash across borders.

192. Canada has demonstrated to some extent only that it pursues the TF threat that it faces (see IO.9). The system suffers from inadequate implementation of UNSCRs by DNFBPs. Nevertheless, it must also be noted that, in some respect, Canada goes beyond the standard—this in particular the case with respect to the CC terrorist list, which Canada reviews every two years to ensure that the legal threshold for listing continues to be met for each entity listed.

Overall Conclusions on Immediate Outcome 10

193. **Canada has achieved a substantial level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

194. Canada's framework to implement the relevant UN CFP sanctions relies on three main components: (i) a prohibition to conduct financial transactions to Iran and the DPRK, with a few regulated exceptions, (ii) an obligation to freeze assets of designated persons; and (iii) an obligation to notify the competent authorities of any frozen assets.

195. Canada implemented the UNSCR 1737 and 1718 obligations, including part of the freezing obligations, by issuing within the UN-requested timeline two regulations dealing with Iran and the DPRK respectively. Both regulations impose freezing obligations that are generally comprehensive (see R.7). The lead agency for their implementation is GAC. Canada also went beyond the standard by imposing additional unilateral sanctions under the Special Economic Measures Act (SEMA). As a result of its Controlled Engagement Policy towards both countries, the Canadian Government does not engage in active trade promotion with Iran and the DPRK, and, with almost all commercial financial transactions between Canada and Iran prohibited, the volume of existing bilateral trade with both countries has dropped considerably. Canada also ensured that the exceptions to the general prohibition of conducting financial transactions[73] do not apply with respect to designated persons and entities.

196. Decisions taken by the UNSC under 1737 and 1718 take immediate effect in Canada. The current lists of designated persons and entities are published on the OSFI website. To facilitate the

[73] Examples of these exceptions include: non-commercial remittances to the DPRK; financial banking transactions of CAD 40 000 and under between family members in Canada and family members in Iran; and other transactions permitted on a case-by-case basis, at the discretion of the Minister of Global Affairs. In practice, exceptions have been granted mainly in the case of prospective Iranian immigrants for the purposes of immigration fees and related transactions.

implementation of the TFS, guidance is provided on the GAC and OSFI website.[74] In addition, OSFI notifies the FRFIs of any changes to the lists on the same day as the changes occur, or on the day that follows the receipt of the note verbale. It also reminds FRFIs on a monthly basis of their screening and freezing obligations, either per web post or per email. Its guidance requires FRFIs to search their records for designated names in two ways: (i) by screening new customers' names against the official lists at the time such customers are accepted; and (ii) by conducting a full search of all customers' databases "continuously," which the guidance defines as "weekly at a minimum." No other authorities provide notifications to other REs of changes made to the lists. As a result, while the legal obligations to implement PF-related TFS are the same across the range of REs, swift action is actively facilitated in the case of FRFIs only. REs may nevertheless subscribe to the RSS feeds on the GAC website, or to the UN notification system, in order to be notified of changes to the Iran and DPRK regulations.

Identification of assets and funds held by designated persons/entities and prohibitions

197. Canada has had some success in identifying funds and other assets of designated persons, and preventing these funds from being used, as indicated in the table below. Two of the larger banks, as well as one provincial FI and two life insurers have identified assets of designated persons, frozen those assets (where available), and reported the case to the RCMP, OSFI, and FINTRAC. The assets were detected through timely screening of the FIs' customers' (but not other parties such as the beneficial owner, despite OSFI's guidance in this respect) against the UN lists. While the freezing are occurrences are low, they nevertheless indicate that FIs and in particular D-SIBs are taking measures to prevent their potential misuse for PF activities. No information was provided on the timing of the freezing measures.

Table 17. **Assets Reported Under the Regulations Implementing the United Nations Resolutions on both Iran and the DPRK, as of September 2015**

Reporting Entity	Number of Accounts/Contracts	Assets Frozen		Assets Reported but Not Frozen (no cash surrender value) in CAD
		CAD equivalent of amounts in foreign currencies	Amounts in CAD	
Bank X (DTI)	1		78 838	
Bank Y (DTI)	2	591.2	845	
Provincial FI	4		30 647	
Total re. Accounts	**7**	**591.2**	**110 330**	
Federal Life Insurer X	6			29 200
Life Insurer Y	10			3 248 612
Total re. Insurance Contracts	**16**			**3 277 812**

[74] See Global Affairs Canada (nd), Canadian Sanctions Related to Iran, www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; Canadian Sanctions Related to North Korea, www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.

198. Canada went beyond the UN listings by investigating the financial components of proliferation activities detected on their territory. The authorities successfully prosecuted one individual for the export of prohibited dual-use goods. The enforcement function is shared between the RCMP and the CBSA, with the former taking the lead in instances that include a potential nexus with national security or OCGs, and the CBSA taking the lead in other instances. So far, the investigations revealed no need for freezing measures: the individuals had little assets, most of which had been used to purchase unauthorized dual use goods.

199. Through the analysis of STRs and other information, FINTRAC has detected potential violations of the SEMA and import-export legislation which it disclosed to the CBSA and CSIS.[75] The analysis of STRs notably pointed to some instances of potential wire stripping and sanctions evasion. No figures were provided as the system does not keep track of STRs that also mention suspicion of PF. According to the authorities, in most instances, the REs may not specifically refer to suspicions of PF, but simply highlight that the transactions does not make economic sense. FINTRAC has discussed some of these cases with its partner agencies in the operation meetings of the Counter-Proliferation Operations Committee.

FIs and DNFPBs' understanding of and compliance with obligations

200. Large FIs, and in particular the D-SIBs, have a good understanding of their freezing obligations, including with respect to PF. They generally have staff dedicated to the implementation of TFS that regularly check the UN lists. They are also aware of the risk of wire stripping and have reported instances of potential wire stripping to FINTRAC. Smaller FRFIs have a relatively good understanding of their obligations, although several do not distinguish the PF-related from the TF-related sanctions. DNFBPs, however, are far less aware of their PF-related obligations, so far, none of them have frozen assets belonging to designated persons.

201. Some outreach has been conducted, notably by the RCMP, with a view to increase the general public's awareness of the proliferation risk. Although some of the outreach activities include information on red flags for potentially suspicious PF activities, these efforts have, so far, mainly focused on proliferation activities rather than the implementation of related TFS.

Competent authorities ensuring and monitoring compliance

202. There is no formal mechanism for monitoring and ensuring compliance by FIs and DNFBPs with PF-related obligations. Nevertheless, some monitoring does take place in practice with respect to FRFIs: OSFI, in the exercise of its general functions, has examined the systems put in place by FRFIs to implement the sanctions regimes for both TF and PF. It has also identified shortcomings (in particular the lack of screening of persons other than the customer) and requested improvements in the screening processes. As a result of a sanction recently imposed by the US regulator on a foreign bank with subsidiary operations in Canada and the US for violations of the PF-related sanctions, OSFI

[75] While FINTRAC does not have an explicit mandate to receive reports of suspicions of PF, it is required by law to disclose financial intelligence to assist in investigations and prosecutions for ML, TF and other threats to the security of Canada, which could include PF.

increased its dialogue with and monitoring of that specific bank. Ultimately, it was satisfied that the activities conducted in Canada were different than those conducted in the US and that the risk was limited in Canada. OSFI is not, however, habilitated to sanction any potential breach of PF-related obligations.

203. While this ad hoc monitoring by the OSFI is proving helpful with respect to FRFIs and useful in identifying shortcoming in their implementation of TFS, it does not entirely compensate the lack of a more comprehensive monitoring system.

Overall Conclusions on Immediate Outcome 11

204. **Canada has achieved a moderate level of effectiveness with IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

Several, but not all REs listed in the standard are subject to Canada's AML/CFT framework:

- AML/CFT requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada, and, as a result, are inoperative with respect to legal counsels, legal firms, and Quebec notaries. The exclusion of these professions is not line with the standard and raises serious concerns (e.g. in light of these professionals' key gatekeeper role in high-risk activities such as real-estate transactions and formation of corporations and trusts).
- TCSPs (other than trust companies), non FI providers of open loop pre-paid card, factoring companies, leasing and financing companies, check cashing business and unregulated mortgage lenders, online gambling, and virtual currencies do not fall under the AML/CFT regime, but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies.

FIs including the D-SIBs have a good understanding of the ML/TF risks and of their AML/CFT obligations. While a number of FIs have gone beyond existing requirements (e.g. in correspondent banking), technical deficiencies in some of the CDD requirements (e.g. related to PEPs) undermine the effective detection of some very high-risk threats, such as corruption.

Requirements—on FIs only—pertaining to beneficial ownership were strengthened in 2014 but there is an undue reliance on customers' self-declaration for the purpose of confirming beneficial ownership.

Although REs have gradually increased the number of STRs and threshold-based reports filed, the number of STRs filed by DNFBPs other than casinos remains very low.

With the exception of casinos and BC notaries, DNFBPs—and real estate agents in particular—are not adequately aware of their AML/CFT obligations.

Recommended Actions

Canada should:

- Ensure that legal counsels, legal firms, and Quebec notaries are subject to AML/CFT obligations when engaged in the financial transactions listed in the standard.
- Ensure that TCSPs (other than trust companies) open loop pre-paid cards, including non FI providers, virtual currency and on line gambling to AML/CFT requirements.
- Require DNFBPs to identify and verify the identity of beneficial owners and PEP in line with the standard.

- Require FIs to implement preventive measures with respect to PEPs, and wire transfers in line with the FATF standards, and monitor (e.g. through targeted inspections) and ensure compliance by all FIs of their obligation to confirm the accuracy of beneficial ownership in relation to all customers.
- Enhance the dialogue with DNFBPs other than casinos to increase their understanding of their respective ML/TF vulnerabilities and AML/CFT obligations, in particular with real estate agents, dealers in precious metals and stones (DPMS) (with greater involvement of the provincial regulators and the relevant trade and professional associations). Update ML/TF typologies and specific red flags addressed to the different categories of DNFBPs to assist in the detection of suspicious transactions.
- Consider introducing a licensing or registration regime, or other controls for DPMS.
- Monitor and ensure DNFBPs' and small retail MSBs' compliance with TFS obligations.
- Issue further guidance, especially to non-FRFIs, on the new requirements related to domestic PEPs.
- Strengthen feedback to small banks and the insurance sector on the use of STRs.
- Issue guidance for all REs to facilitate the detection of the possible misuse of open loop prepaid cards in ML and TF schemes.

The relevant Immediate Outcome considered and assessed in this chapter is I04. The recommendations relevant for the assessment of effectiveness under this section are R9-23.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF Risks and the Application of Mitigating Measures

205. The level of understanding of ML/TF risks and AML/CFT obligations, as well as the application of mitigating measures vary greatly amongst the various REs.

206. FIs are aware of the main threats and high-risk sectors identified in the NRA, as well as of the level of ML/TF vulnerabilities associated to their activities. Recent trends in the FIs' understanding of risks and AML/CFT obligations is not immediately apparent in the supervisory data (because the latter aggregates as "partial deficiencies" both minor and more severe failures), but, according to the authorities, have been positive. The major banks have developed comprehensive group-wide risk assessments and implement mitigating measures derived from detailed consideration of all relevant risk factors (including lines of business, products, services, delivery channels, customer profiles). Several other FIs stated that their risk assessment and mitigating measures are already in line with the findings of the NRA. Specific attention is paid to cash (including potentially associated to tax evasion) and to the geographic risk (which, especially in the case of large banks, takes into account the index of corruption developed by relevant international organization and includes offshore financial centres). Some FIs also consider trust accounts held by lawyers and other legal professions as presenting a higher risk and, as a result, conduct enhanced

monitoring of these accounts. Specific products associated to real estate transactions, such as mortgage loans, are also considered as high-risk products. Over the last three fiscal years, a total of 9 556 STRs were filed with FINTRAC regarding suspected ML/TF activities in relation to real estate, which represents 3,8% of the overall amount of STRs received, with most STRs coming from banks, credit unions, *caisses populaires*, and trust and loan companies. The main typologies identified in this respect range from the use of nominees by criminals to purchase real estate or structuring of cash deposits to more sophisticated schemes where, for example, loan and mortgage schemes are used in conjunction with the use of lawyer's trust account.

207. In some instances, however, the regulator's on-site inspections revealed issues with the quality and scope of the risk assessments, especially in relation to the elements taken into account as inherent risk of individuals, and to the consistency among business-lines. Smaller FRFIs display a weaker understanding of ML/TF risks, and tend to regard AML/CFT obligations as a burden.

208. The life insurance sector appears to underestimate the level of risk that it faces. According to FINTRAC supervisory findings, life insurance companies and trust and loan companies that are non-FRFIs show the highest level of deficiency in their risk assessment, as well as the weakest understanding of their AML/CFT obligations. Non-federally regulated life insurance companies have a weak understanding of their ML/TF risks than federally regulated companies, and appear particularly refractory to improving AML/CFT compliance.

209. The representatives of the securities sector recognized the high risk rating of their activities, but also noted that the higher level of risk lie mainly in smaller security firms and individuals. Firms not involved in cross-border activities seem to underestimate their vulnerability to ML risk, having a limited notion of geographic risk, as mainly referred to offshore countries. Overall, securities dealers have a good understanding of their AML/CFT obligations, although supervisory findings highlight that the level of understanding is weaker in more simplified structures and that internal controls are a recurring area of weakness.

210. MSBs' level of awareness of AML/CFT obligations is consistent with their size and level of sophistication of their business model. MSBs that operate globally as part of larger networks are aware of the specific ML/TF risks that they face (i.e. risks emanating mainly from the fact their activity is essentially cash-based). They have developed specific criteria to evaluate certain risk (e.g. the risks posed by their agents) to enable them to determine the appropriate level of controls. While the assessment team did not have an opportunity to meet with representative from the smaller independent MSBs,[76] representatives from other private sector entities as well as FINTRAC confirm that smaller MSBs are far less aware of their AML/CFT obligations and their vulnerabilities to ML/TF. According to FINTRAC, community-specific MSBs are reluctant to apply enhanced due diligence to higher risk customers. To assist mainly small MSBs in the development of a RBA, on 1 September 2015 FINTRAC developed an RBA workbook for MSBs.

[76] Under the glossary of the NRA the said category has been defined as these MSBs are focused on retail transactions, and have stand-alone computer systems and street-level retail outlets across Canada. Of these, one sub-group offers currency exchanges only, typically in small values, and is often found in border towns (e.g. duty-free shops), while the other sub-group offers currency exchanges, but may also offer money orders and EFTs, typically as an agent of a national full-service MSB.

211. Casinos vary greatly in size, complexity, and business models. All the relevant gaming activities are subject to AML/CFT requirements where (on the basis of the model in place) the province or the Crown corporation is responsible for their compliance. Representatives from casinos demonstrated a good understanding of their AML/CFT obligations and of the most frequent ML typologies in their sector. Nevertheless, their implementation of CDD measures seems to follow a tick-box approach rather than be based on an articulated risk-assessment. Moreover, casinos seem to be essentially focused on cash, and appear to underestimate to some extent the risk posed by funds received from accounts with FIs.

212. DPMS are highlighted as a high-risk in the NRA. Compliance examinations conducted between 2012 and 2014 revealed industry-wide non-compliance. FINTRAC has worked with two DPMS associations (namely the Canadian Jewelers Association, CJA, and the Jewelers Vigilance Canada, JVC, which, together, represent about one quarter of the Canadian DPMS) to strengthen compliance of this sector. This has led to an increase in these DPMS' understanding of their AML/CFT obligations, as shown in subsequent examinations. Nevertheless, the absence of licensing or registration system or other forms of controls applicable to the sector in its entirety creates major practical obstacles for FINTRAC to properly establish the precise range of subjects that it should reach out to.

213. The real estate agents met, despite being aware of the results of NRA, consider that they face a low risk because physical cash is not generally used in real estate transactions. As the normal practice is to accept bank drafts—agents consider banks have mitigated the ML/TF risk. In the province of Quebec, notaries trust accounts are used to deposit the funds involved in real estate transactions—real estate agents therefore consider that notaries are in a better position to detect possible ML activities, but Quebec notaries are not currently covered by the AML/CFT regime. Real estate agents are overly confident on the low risk posed by "local customer," as well as non-resident customer originating from countries with high levels of corruption.

214. The accountants' level of awareness of AML/CFT obligations is quite low. The competent professional association underlined that, in the absence of guidance and outreach efforts, accountants are often unclear as to when they are subject to the AML/CFT regime.

215. BC notaries provide a wide range of services related to residential and commercial real estate transfers. They are, however, not fully aware of the risk and their gatekeeper role in relation to real estate transactions. Like real estate agents, they consider that all risks have been mitigated by the bank whose account the funds originated from.

216. In May 2015, FINTRAC issued guidance to assist REs in the implementation of their RBA. Most representatives of DNFBPs considered this helpful, but also expressed the need for further initiatives focused on their respective activities.

217. AML/CFT obligations are inoperative towards legal counsels, legal firms and Quebec notaries involved in the activities listed in the standard. In February 2015, the Supreme Court of Canada declared that a portion of Canada's AML/CFT legislation is unconstitutional as to attorneys, because it violates the solicitor-client privilege. Representatives from the private sector and the Canadian authorities confirmed that lawyers in Canada are frequently involved in financial transactions, often related to high-risk sectors, such as real estate, as well as in the formation of trust

and companies. In the context of real estate transactions, in particular, lawyers and Quebec notaries provide not only legal advice, but also trading services,[77] and receive sums from clients for the purchase of a property or a business, deposited and held temporarily in their trust accounts. Representatives of the Federation of Law Societies, although aware of the findings of the NRA, did not demonstrate a proper understanding of ML/TF risks of the legal profession. In particular, they appeared overly confident that the mitigation measures adopted by provincial and territorial law societies (i.e. the prohibition of conducting large cash transactions[78] and the identification and record-keeping requirements for certain financial transactions performed on behalf of the clients)[79] mitigate the risks. While monitoring measures are applied by the provincial and territorial law societies, they are limited in scope and vary from one province to the other. The on-site visit interviews suggested that the fact that AML/CFT requirements do not extend to legal counsels, legal firms and Quebec notaries also undermines, to some extent, the commitment of REs performing related functions (i.e. real estate agents and accountants).

CDD and Record-Keeping

218. CDD obligations, and especially those dealing with beneficial ownership, politically exposed foreign persons (PEFPs) and, for FIs, wire transfers, are not fully in line with FATF standards. In addition, some DNFBPs are not subject to AML/CFT requirements and monitoring (see TCA for more details).

219. Since February 2014, FIs are required to obtain, take reasonable measures to confirm, and keep records of the information about an entity's beneficial ownership. In practice, FIs seem to interpret this new provision as requiring mostly a declaration of confirmation by the customer that the information provided is accurate, to be followed, in some cases, by an open source search. Only a few of the FIs interviewed stated that they would spend time to check the information received and verify the information through further documents and information, which raises concerns. The undue reliance on a customer's self-declaration (as a way to replace the duty to confirm the accuracy of the information provided) appears to be a significant deficiency in the implementation of preventive measures and OSFI has issued findings to FRFIs requiring that more robust beneficial ownerships confirmation measures be undertaken. Moreover, REs have limited methods to confirm the accuracy of beneficial ownership information (see IO.5). Several FIs are in the process of implementing the new requirement by reviewing the information gathered for their existing customers, but most of the FIs interviewed were unable to establish the current stage of this review.

220. Due to the recent entry in force of the new beneficial ownership requirements, there is limited information on how well FRFIs are complying with the new obligations. Recent supervisory findings—albeit limited in numbers- suggest that serious deficiencies remain.

---

[77] This is notably confirmed by the exemption from the requirement to be licensed as real estate agent granted under the relevant provincial legislation (for example in British Columbia, Real Estate Service Act, Section 3, (3) lett. f, and, for Quebec Notaries, Quebec Notary Act, Art.18).

[78] Model Rule on Cash Transactions adopted by the Council of the Federation of Law Societies of Canada on July 2004.

[79] Model Rule on Client Identification and Verification Requirements, adopted by the Council of the Federation of Law Societies of Canada on 20 March 2008 and modified on 12 December 2008.

221. Discussions with DNFBPs, in particular those with real estate representatives, highlighted that even basic CDD requirements are not properly understood and that the implementation of the "third-party determination rule" seems to be mainly limited to asking the customer whether he/she is acting under the instructions of other subjects, without further enquiry.

222. Measures to prevent and mitigate the risks emanating from corruption and bribery (classified as very high threats in the NRA) are insufficient, because of shortcomings in the legal framework (see TCA) and weak implementation of existing requirements. REs' capacity to properly detect these criminal activities is significantly undermined. This is in particular the case with DNFBPs considering that they are not required to take specific measures when dealing with PEPs. In order to determine whether they are in a business relationship with foreign PEPs (i.e. PEFPs) or their family members, FIs combine the information gathered through the client identification forms and the screening process (realized mainly through commercial databases). Most FIs interviewed limited their search to the customer and did not seem to establish whether they were dealing with "close associates" of PEFPs. Furthermore, the range of information required by FIs is limited to the source of funds, and does not always include the source of wealth. Most FIs appear to be over-reliant on the self-declaration of the customer to determine the source of funds, and do not perform further verification of the accuracy of the information provided. The approval of senior management can be obtained "within 14 days" from the day on which the account is activated, which will be extended to 30 days when the new provisions on domestic PEPs enter into force. Some FIs confirmed that, during that timeframe, the PEPs can operate the account—the business relationship can therefore be conducted without adequate controls having taken place. According to OSFI's supervisory findings, in some cases, the involvement of senior management occurs even beyond the prescribed timeframe.

223. There are nevertheless some encouraging signs: over the last four fiscal years, FINTRAC assessed non-FRFIs' determination of PEFPs[80] in the context of 2 508 examinations in four different sectors (credit unions and *caisses populaires*, trust and loan companies, MSB and securities dealers), and identified shortcomings were identified in only 4% of the cases.

224. Several FRFIs, including the D-SIBs,[81] interviewed, apply an onboarding procedure for all customers who include the same determination in relation to "domestic PEPs" and the same enhanced due diligence measures; in order to determine whether a customer is a "domestic PEP," the large banks rely mainly on the information contained in commercial databases. The notion of "domestic PEP" that they apply varies greatly from one institution to the other, and focuses on customers only, i.e. without taking the beneficial owners into account. Some non-FRFIs expressed the need for timely guidance to clarify and facilitate the implementation of the new requirement regarding domestic PEPs and their close associates.

[80] The said determination is considered in relation to the following cases: the opening of new accounts (financial entities and securities), when an EFT over CAD 10 000 is sent or received (financial entities and MSBs) or a lump sum payment of CAD 100 000 or more in respect to an annuity or life insurance policy.

[81] In this respect, OSFI Guidelines B-8, Deterring and detecting ML/TF, explain that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, nevertheless, where a FRFI is aware that a client is a domestic PEP, the FRFI should assess what effect this may have on the overall assessed risk of the client. If the assessed risk is elevated, the FRFI should apply such enhanced due diligence measures as it considers appropriate.

225. DNFBPs, however, are not required to determine whether they are dealing with foreign PEPs. The interviews conducted confirmed that the political role of customers is not an element that DNFBPs take into account in practice to determine whether further mitigation measures are necessary.

226. While FRFIs have adequate record-keeping measures in place, the smaller credit unions, retail money services business and DNFBPs active mainly in the real estate sector implement weaker measures, which are mainly paper based or based on a combination of paper and manual procedures. FINTRAC identified several deficiencies in record-keeping procedures of BC notaries as well, especially with respect to the conveyancing of real estate.

227. Correspondent banking services are mostly offered by D-SIBs. The D-SIBs have a centralized global management and monitoring of correspondent banking relationships. In some cases, they go above and beyond the current requirements: for example, when reviewing correspondent bank relationships, they also take the quality of AML/CFT supervision into account. Controls on correspondent banking seem to be also reviewed through visits on site and testing procedures by the internal audit. According to OSFI supervisory findings, FRFIs properly assess these services as a higher risk activity, taking necessary mitigation measures.

228. Before introducing new technologies and products, banks typically conduct an assessment of the potential ML/TF risks (and, in doing so, go beyond the requirements of Canadian law). Some banks indicated the lack of information from the authorities regarding typologies on possible exploitation of emerging products that would be helpful in their risk assessment. Among the new products it is worth noting that pre-paid cards are used in Canada but are not currently subject to AML/CFT requirements.[82] Nevertheless, OSFI has alerted FRFIs in the context of its inspections to the need to consider that reloadable prepaid cards operate similarly to deposit accounts, and therefore require equivalent mitigation measures. OSFI supervisory findings reveals that in two cases, FIs had failed to integrate their risk assessment regarding prepaid cards into their overall risk assessment methodology as well as to establish effective controls over their agents. Following OSFI's supervisory interventions, the two institutions are now implementing prepaid access controls in reloadable card programs similar to controls over deposit accounts. Regulatory amendments to include prepaid cards in the regulations are being developed. Other new products currently used—albeit to a very limited extent—include virtual currencies,[83] which fall outside the current framework but which the government has proposed to regulate for AML/CFT purposes.[84]

[82] Global open loop prepaid card transaction volumes have grown by more than 20% over the past four years and were expected to reach 16.9 billion annually in 2014. Despite pre-paid open loop access (thus meaning any financial product that allows customers to load funds to a product that can then be used for purchases and, in some cases, access to cash or person-to-person transfers) has been considered under the NRA of high vulnerability rating, pre-paid cards are not currently subject to AML/CFT requirements.

[83] According to the Canadian Payments Association, as of 10 April 2014, there were between 1 000 and 2 000 daily transactions in Canada involving bitcoin, which represent 1/100 of 1% of the total volume of Canada's daily payments transactions. See Senate Canada, Digital Currency: you can't flip this coin!, June 2015, p. 23.

[84] The legislation to include dealing in virtual currencies among MSBs has been passed, and the associated enabling regulations are being developed.

229. Some of the larger FIs and money transfer companies go beyond current requirements for wire transfers and the filing of EFTRs by applying stricter measures: they notably monitor such transfers on a continuous basis through sample checks of wires received on behalf of customers in order to verify whether they contain adequate originator information, and, if not, take up the matter with the originating banks.

230. FIs have a good understanding of their obligations with respect to TFS (see IO.10). MSBs belonging to large networks, although they are not required to screen on a continuous basis their customer base against the sanctions lists, in practice do so. On-site supervisory inspections revealed, however, deficiencies in the timeliness of the name-screening processes, as well as in their scope (because they do not always extend the screening to the beneficial owners and authorized signers of corporate entities). According to industry representatives and FINTRAC, this is not the case in smaller independent MSBs, where less sophisticated procedures of record-keeping and monitoring are in place.

231. DNFBPs, in particular in the real estate sector, acknowledged that they do not fully understand the requirements related to TFS. They also recognized that their implementation of these requirements is weak, largely because their procedures are mainly paper-based.

Reporting Obligations and Tipping Off

232. With the exception of casinos, reporting by the DNFBPs sectors is very low, including in high-risk sectors identified in the NRA.

Table 18. **Number of STRs Filed by FIs and DNFBPs**

	2011–2012	2012–2013	2013–2014	2014–2015
FIs				
Banks	16 739	17 449	16 084	21 325
Credit Unions/*Caisses populaires*	11 473	12 217	12 522	16 576
Trust and Loan Company	617	757	702	729
Life Insurance	379	379	453	427
MSB	35 785	42 246	46 158	47 377
Securities dealers	811	1 284	2 087	1 825
DNFBPs				
Accountants	-	1	-	-
BC Notaries	1	-	-	1
Casinos	4 506	4 810	3 472	3 994
DPMS	66	129	235	243
Real Estate	15	22	22	34
Total	**70 392**	**79 294**	**81 735**	**92 531**

233. Nevertheless, FINTRAC is of the view that the quality of STRs is generally good and improving. The 1 256 examinations conducted in this respect from 2011/12 to 2014/15, revealed

that 82% of REs examined complied with their obligation. In particular, the REs' write-up for Part G of the reporting form (which relates to the reason for the suspicions) has evolved over the years from a basic summary to a very thorough and complex analysis of the facts. FINTRAC also noted that the percentage of STRs submitted with errors has significantly decreased, namely from 84% (in July 2011) to 17% (in July 2015). Most FIs interviewed rely on both front line staff and automated monitoring systems to detect suspicions. At the end of their internal evaluation process, if the STR is not filed, a record is kept with the rationale for the lack of reporting. STRs are generally filed within 30 days.

234. Awareness and implementation of reporting obligations vary greatly amongst the various sections. In particular: casinos are adequately aware of their reporting obligations. The larger casinos detect suspicious transactions not only through front-line staff, but also through analytical monitoring tools developed at the corporate level on the transaction performed and on the basis of video-investigation in order to identify possible unusual behaviours (such as passing chips). They also report to FINTRAC suspicious transactions that were merely attempted. The real estate sector, however, appears generally unaware of the need to report suspicious transactions that have not been executed. In brokerage firms, the detection of suspicious transactions is mainly left to the "feeling" of the individual agents, rather than the result of a structured process assisted by specific red flags. MSBs, securities dealers and DPMS have significantly increased the number of STRs filed, mainly in response to the outreach, awareness raising and monitoring activities performed by FINTRAC. The *caisses populaires* have also increased their reporting as a result of the centralized system of detection of suspicious transactions developed by the *Fédération des Caisses Desjardins du Quebec*.

235. The larger REs interviewed had good communication channels with FINTRAC and receive adequate feedback on an annual basis on the quality of their STRs and on the number of convictions related to FINTRAC's disclosure. In particular, a Major Reporter Group was established in FINTRAC to foster dialogue. In this context, FINTRAC hosted, in May 2014, a first forum for D-SIBs to enhance compliance with STRs obligations and targeted feedback sessions, and another, in 2015, for casinos. D-SIBs and casinos met considered these forums particularly helpful. Small banks and most categories of DNFBPs do not to receive the same kind of feedback.

236. Tipping off does not appear to be a significant problem in Canada. REs have included in their internal policies, controls and training initiatives some provisions that address the prohibition of tipping off. The measures are considered effective by FINTRAC. So far, no charges have been laid as regards tipping off.

Internal Controls and Legal/Regulatory Requirements Impending Implementation

237. OSFI supervisory findings conducted in the last three years confirm that FRFIs apply sufficient internal controls to ensure compliance with AML/CFT requirements with the five core

elements of the compliance regime.[85] A key OSFI finding is the scope of the two-year review, which is frequently more limited to the existence of controls rather than to their effectiveness.

238. REs with cross-border operations include their overseas branches in their AML/CFT program and extend their internal controls to their foreign subsidiaries. They also adopt the more stringent of Canadian or host jurisdiction rules in their group-wide AML/CFT framework on areas where host country requirements are stricter or more in line with FATF standards. The larger banks reported that they had sharing information mechanisms at group level and, in cases where the local jurisdiction had created obstacles to the information sharing, the local branches were closed.

239. Three of the D-SIBs have branches in Caribbean countries: the two REs interviewed took specific risk mitigating measures by adopting an enterprise-wide management to the highest level. As a result, every high-risk client in the Caribbean must be pre-approved both by senior management in the business and the compliance officer.

240. The data provided by FINTRAC indicates an uneven level of compliance among non-FRFIs. Credit unions and *caisses populaires* have good internal controls in place, which is not the case for trust and loan companies, securities dealers, insurance sector and MSBs: several deficiencies have been identified, including incomplete or not updated policies and procedures, the limited scope of controls, a lack of comprehensive assessment of effectiveness, and no communication to senior management.

241. DNFBPs other than casino and BC notaries have either no or weak internal controls. The discussions with real estate sector representatives also revealed some concerns about the effective control of the proper implementation of AML/CFT requirements by their agents. Some DNFBPs professional associations are working with their members to assist them in increasing their level of compliance and in increasing their awareness with their obligations. In this context, the associations felt that further engagement with FINTRAC would be useful.

Overall Conclusions on Immediate Outcome 4

242. **Canada has achieved a moderate level of effectiveness for IO.4**.

[85] Under PCMLTFR s. 71 (1), the five elements of the compliance regime are the following: appointment of a compliance officer, development and application of written compliance policies and procedures, assessment and documentation of ML/TF risks and of mitigating measures, written ongoing training program, a review of the compliance policies and procedures to test their effectiveness. The review has to be done every two years. Failure to implement any of these five elements is considered serious violation under AMPR and shall lead to an administrative monetary penalty of up to CAD 100 000 for each one (ss 4 and 5).

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

FINTRAC and OSFI have a good understanding of ML and TF risks; and FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and DPMS sectors is not entirely commensurate to the risks in those sectors.

The PCMLTFA is not operative in respect of legal counsels, legal firms, and Quebec notaries—as a result, these professions are not supervised for AML/CFT purposes which represents a major loophole in Canada's regime.

A few providers of financial activities and other services fall outside the scope of Canada's supervisory framework (namely TCSPs other than trust companies, and those dealing with open loop pre-paid card, including non FI providers on line gambling and virtual currency, factoring companies, leasing and financing companies, check cashing business, and unregulated mortgage lenders), but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies.

Supervisory coverage of FRFIs is good, but the current supervisory model generates some unnecessary duplication of effort between OSFI and FINTRAC.

FINTRAC has increased its supervisory capacity to an adequate level but its sector-specific expertise is still somewhat limited. OSFI conducts effective AML/CFT supervision with limited resources.

Market entry controls are good and fitness and probity checks on directors and senior managers of FRFIs robust. There are, however, no controls for DPMS, and insufficient fit-and-proper monitoring of some REs at the provincial level.

Remedial actions are effectively used but administrative sanctions for breaches of the PCMLTFA are not applied in a proportionate and/or sufficiently dissuasive manner.

Supervisory actions have had a largely positive effect on compliance by REs. Increased guidance and feedback has enhanced awareness and understanding of risks and compliance obligations in the financial sector and to a lesser extent in the DNFBP sector.

Recommended Actions

Canada should:

- Ensure that all legal professions active in the areas listed in the standard are subject to AML/CFT supervision.
- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resources and expertise and review implementation of Canada's supervisory approach to FRFIs.
- Ensure that FINTRAC develops sector-specific expertise, continues to have a RBA in its

examinations, and applies more intensive supervisory measures to the real estate and DPMS sectors.

- Ensure that there is a shared understanding between FINTRAC and provincial supervisors of ML/TF risks faced by individual REs and ensure adequate controls are in place after market entry at the provincial level to prevent criminals or their associates from owning or controlling FIs and DNFBPs.
- Ensure that the administrative sanctions regime is applied to FRFIs and that AMPs are applied in a proportionate and dissuasive manner including to single or small numbers of serious violations and repeat offenders. Ensure that OSFI's guidelines relating to AML/CFT compliance and fitness and probity measures are subject to the administrative sanctions regime for non-compliance.
- Provide more focused and sector-specific guidance and typologies for the financial sector and further tailored guidance for DNFBPs, particularly with respect to the reporting of suspicious transactions.

The relevant Immediate Outcome considered and assessed in this chapter is IO3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

243. Market entry controls are applied at federal and provincial level. After market entry, there are effective measures in place at the federal level to ensure that when changes in ownership and senior management occur, FRFIs conduct appropriate fitness and probity (F&P) checks. The federal prudential regulator, OSFI, applies robust controls when licensing a federally regulated financial institution (FRFI). Due diligence measures, including criminal background checks on individuals, are carried out at the market entry stage and OSFI has refused or delayed applications when issues arise. OSFI provided an example where it became aware of misconduct by a small domestic bank's former CEO and ultimately undertook a suitability review of the person. OSFI concluded that he was not suitable to be an officer of the bank and recommended that he not be a member of the board. The bank removed the officer and as a result, OSFI's supervisory oversight strategy of the bank was downgraded. After market entry, FRFIs are responsible for implementing controls around the appointment of senior managers and directors of FRFIs under OSFI Guidelines. OSFI supervises FRFIs for compliance around conducting background checks but this control is not as robust as it is the responsibility of FRFIs to apply fit and proper controls after market entry stage rather than OSFI's in the approval of the appointment of senior managers in FRFIs. Provincial regulators apply market entry controls for non-FRFIs (e.g. securities dealers, credit unions, and *caisses populaires*). These controls include criminal checks to verify the integrity of applicants and to ensure that RE's

implement fit and proper controls. The controls are usually conducted by the RE but are subject to oversight by the provincial regulators. These market entry controls differ between provinces and sectors but, overall, the market entry controls being applied by provincial regulators are robust.

244. Since its last MER, Canada has implemented a money service business (MSB) registration system under the supervision of FINTRAC. One exception to the federal system of registration is in Quebec, where MSBs register with the *Autorité des marchés financiers* (AMF) and FINTRAC. Applicants for registration undergo criminal record checks and fitness and probity checks by FINTRAC and AMF. Individuals convicted of certain criminal offenses are ineligible to own or control an MSB. FINTRAC monitors the control of MSBs as they are required to submit updated information on owning or controlling individuals or entities when changes occur and again when the MSB applies for renewal of its registration every two years. FINTRAC has refused to register applicants and has revoked registration when the applicant was convicted for a criminal offense. An example was given where FINTRAC revoked the registration of two MSBs after the conviction of two individuals that owned both MSBs. Another example was provided where an MSB terminated its relationship with an agent due to fitness and probity concerns about the agent as part of follow-up activity conducted after an examination by FINTRAC. When an MSB registration is denied, revoked, expired, or pending, FINTRAC follows-up appropriately, for example by conducting an offsite review or on-site visit to the MSBs' last known address to ensure that the entity is not operating illegally.

245. There are market entry controls for most DNFBPs in Canada that require them to be licensed or registered by provincial regulators or by self-regulatory bodies (SRBs). Criminal checks are applied by supervisors and SRBs to casinos, BC notaries, accountants, and real estate brokers and agents during the licensing or registration process. The only exception to this is in the DPMS sector where there is no requirement to be registered or licensed or to be subjected to other forms of controls to operate in Canada. All casinos are provincially owned and apply thorough fit and proper procedures for employees.

246. After market entry, provincial regulators conduct some ongoing monitoring of non-FRFIs and DNFBPs and withdraw licenses or registration for criminal violations. The assessment team was provided with examples of restrictions or cancellations of investment dealers' registration by the Investment industry Regulatory Organization of Canada (IIROC) due to misconduct or a violation of the law. However, FINTRAC does not have responsibility for the licensing or registration of FIs or DNFBPs (apart from MSBs) and non-federal supervisors do not appear to implement the same level of controls to monitor of non-FRFIs and DNFBPs to ensure that they are not controlled or owned by criminals or their associates after the licensing or registration stage.

Supervisors' understanding and identification of ML/TF risks

247. Supervisors in Canada participated in the NRA process and understand the inherent ML/TF risks in the country. FINTRAC and OSFI have a good understanding of ML/TF risks in the financial and DNFBP sectors.

248. FINTRAC is the primary AML/CFT supervisor for all REs in Canada and is relied upon by provincial regulators to understand ML/TF risks within their population and to carry out AML/CFT

specific supervision. Provincial supervisors integrate ML/TF risk into their wider risk assessment models and leverage off FINTRAC for their assessment of ML/TF risks as FINTRAC has responsibility for AML/CFT compliance supervision in Canada.

249. OSFI is the prudential regulator for FRFIs and conducts an ML/TF specific risk assessment that applies an inherent risk rating to entities on a group-wide basis rather than an individual basis. It is also able to leverage off its prudential supervisors to better understand the vulnerabilities of individual FRFIs complementing the results of the NRA. OSFI demonstrated that it understands the FRFIs' ML/TF risks through its risk assessment model that appropriately identifies the vulnerabilities in the different sectors and REs under its supervision. It also collaborates well with FINTRAC and other supervisors on their understanding of ML/TF risk. This is very important strength of Canada's system because FRFIs account for over 80% of the financial sector's assets in the country. The sector is dominated by a relatively small number of FRFIs: the six D-SIBs control the banking market and hold a significant portion of the trust and loan company and securities markets in Canada. The largest life insurance companies in Canada are also federally regulated. OSFI has identified 34 FRFIs as high-risk, 32 as medium-risk, and 66 as low-risk. The D-SIBS are all rated as high-risk, given their size, transaction volumes and presence in a range of markets. OSFI updates its risk category for an FRFI or FRFI group on an ongoing basis following on-site assessments, ongoing monitoring and follow-up work. The outcomes from OSFI's risk assessment are effective.

250. FINTRAC has recently developed a sophisticated risk assessment model that assigns risk ratings to sectors and individual REs: the model was reviewed in detail by the assessment team and was compared against the data being collected and analysed in FINTRAC's case management tool. The model is a comprehensive ML/TF analytical tool that considers various factors to predict the likelihood and consequence of non-compliance by a RE. On the basis of its analysis, it rates reporting sectors and entities and the rating is then used to inform its supervisory strategy. FINTRAC's risk assessment has rated all 31 000 REs under the PCMLTFA and identified banks, credit unions, *caisses populaires*, securities dealers, MSBs and casinos as high-risk. FINTRAC has incorporated the findings of the NRA into the model to take account of the inherent risk ratings identified in the real estate and DPMS sectors.

251. Other supervisors, notably AMF and IIROC, integrate ML/TF risk into wider operational risk assessment models of entities that they supervise. They rely on FINTRAC to understand the ML/TF risks among all REs and to disseminate this information to prudential or conduct supervisors, given FINTRAC's role as primary supervisor for AML/CFT compliance in Canada. This appears to be happening in cases where AML/CFT issues arise in the course of prudential or conduct supervision. However, FINTRAC does not share with other supervisors its understanding of ML/TF risks in particular sectors on a regular basis. Provincial supervisors are therefore not aware of the ML/TF risks faced in their respective sectors, particularly around vulnerabilities relevant to ownership and management controls in the non-FRFI and DNFBP sectors. Similarly, FINTRAC and OSFI do not sufficiently share their understanding of detailed risks in FRFIs, e.g. through sharing of existing tools to carry out an integrated risk assessment of all FRFIs. As a result, they do not adequately leverage off their respective knowledge of the different business models and compliance measures in place.

Risk-based supervision of compliance with AML/CTF requirements

252. The regulatory regime involves both federal and provincial supervisors. FINTRAC is responsible for supervising all FIs and DNFBPs for compliance with their AML/CFT obligations under the PCMLTFA. Other supervisors may incorporate AML/CFT aspects within their wider supervisory responsibilities although the assessment team found that in instances where an AML/CFT issue arose, the primary regulator would refer the issue to FINTRAC. Given the primary responsibility held by FINTRAC for all REs and the federal and provincial division of powers for financial supervision other than in the areas of AML/CFT, combined with the geographical spread of the Canadian regulatory regime, the assessment team focused primarily on FINTRAC and OSFI's supervisory regime, but also met with provincial supervisors (e.g. AMF in Quebec) and other supervisors (e.g. IIROC for investment dealers).

253. FINTRAC has increased its resources and the level of sophistication of its compliance and enforcement program ("supervisory program") in recent years. In 2014/2015, there was 79 full-time staff employed in FINTRAC's supervisory program. Of this, 57 staff members were involved in direct enforcement activities including outreach and engagement (10), reports monitoring (5), examinations (37), and AMPs/NCDs (5). It has also developed, and continues to develop, its supervisory capabilities on a RBA. Its understanding of the different sectors and business models and of how AML/CFT obligations apply taking into account materiality and context is somewhat limited. This was communicated to the assessors by REs in the banking and real estate sectors during the on-site visit. FINTRAC has nevertheless increased its understanding of its different reporting sectors which is a challenge given the large number and diverse range of entities it supervises.

254. A range of supervisory tools is used by FINTRAC to discharge its supervisory responsibilities and, for the most part, those tools are applied consistently with the risks identified. A case management tool determines the level and extent of supervision to be applied to sectors and individual REs scoping specific areas for examinations, recording supervisory findings and managing follow-up activities. High-risk sectors are subject to on-site and desk examinations (details of which are contained in this report). Less intensive supervisory tools are used for lower-risk sectors. These tools include self-assessment questionnaires (Compliance Assessment Reports or CARs); observation letters (setting out deficiencies that require action); Voluntary Self Declarations of Non-Compliance (VSDONC); and policy interpretations on specific issues that require clarification. The use of observation letters was piloted with the *caisses populaires* sector in 2013/2014. FINTRAC had identified that *caisses populaires* were reporting large cash transactions of more than CAD 10 000 through automated teller machines which was not possible given the low limit on transactions through such machines. Observation letters were used to correct a misinterpretation of reporting obligations and clarify the correct way to report these types of transactions. FINTRAC also uses outreach tools for lower-risk sectors assistance and awareness building tools among smaller REs with limited resources, compliance experience and works with industry representatives. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in higher risk areas such as the real estate and DPMS sectors. FINTRAC

has updated its risk assessment to identify those sectors as high-risk, in line with the findings of the NRA.

255. OSFI applies a close touch approach to AML/CFT supervision of FRFIs. It engages with FRFIs through its prudential supervisors on an ongoing basis and is well placed to supervise higher-risk entities from an AML/CFT perspective given its knowledge of RE's business models OSFI has a particular focus on the large banking groups (D-SIBs) and insurance companies that dominate the financial market in Canada. These are identified as not only high-risk for prudential purposes but also for ML/TF as identified by OSFI and in the NRA. There is a specialist AML compliance (AMLC) division solely responsible for AML/CFT and sanctions supervision in OSFI and allocates its resources on a risk sensitive basis to supervise FRFIs. OSFI's "AML and ATF (i.e. CFT) Methodology and Assessment Processes" assesses the adequacy of FRFIs' risk management measures through its program of controls and assesses FRFIs' compliance with legislative requirements and OSFI guidelines. The AMLC division has expertise in the sectors it supervises and is covering the principal FRFIs leveraging off prudential supervision. OSFI has a good understanding of its sector, its staff has a high degree of expertise and it is adequately supervising FRFIs for AML/CFT compliance (in conjunction with FINTRAC). The number of OSFI AML/CFT supervisors (i.e. currently 10 supervisors including senior management) is, however, too low given the size of supervisory population and the market share and importance of FRFIs in the Canadian context.

256. FINTRAC and OSFI provided comprehensive statistics, case studies, and sample files relating to examinations of FIs and DNFBPs. There were a greater number of examinations of FIs than DNFBPs; in line with Canada's understanding of ML/TF risk and there were more desk-based than on-site examinations. Between April 2010 and March 2015, 3 431 examinations (1 949 desk-based and 1 482 on-site) of FIs were conducted. During the same period, there were 1 300 examinations (895 desk-based and 405 on-site) of DNFBPs.

Table 19. **AML/CFT Examinations Conducted by FINTRAC/OSFI in Canada 2009–2015**

Sector	Activity Sector	Number of ERs (primary population)	FINTRAC/OSFI Examinations						
Financial Institutions (FIs)			**2009/10**	**2010/11**	**2011/12**	**2012/13**	**2013/14**	**2014/15**	**Total**
Financial Entities	Banks	81	11	10	15	10	19	16	81
	Trusts and Loans	75	6	6	13	7	6	7	45
	Credit Unions /*Caisse Populaire*	699	173	205	432	301	170	165	1 446
Life Insurance	Life Insurance	89	70	54	8	13	123	61	329
Money Service Businesses	Money Service Businesses	850	210	201	426	222	161	143	1 363
Securities Dealers	Securities Dealers	3 829	83	120	136	129	167	85	720
Total FI – Desk Exam			270	260	668	389	409	223	2 219
Total FI – On-site Exam			283	336	362	293	237	254	1 765
Total FIs			553	596	1 030	682	646	477	3 984

Sector	Activity Sector	Number of ERs (primary population)	FINTRAC/OSFI Examinations						
DNFBPs			**2009/10**	**2010/11**	**2011/12**	**2012/13**	**2013/14**	**2014/15**	**Total**
Accountants	Accountants	3 829	48	20	0	25	11	10	114
BC Notaries	BC Notaries	336	0	0	0	16	1	6	23
Casinos	Casinos	39	12	12	5	10	1	6	46
Dealers of Precious Metals and Stones	Dealers of Precious Metals and Stones	642	0	0	10	166	276	2	454
Real Estate	Real Estate	20 784	90	70	40	270	203	140	813
Total DNFBP – Desk Exams			83	41	27	322	391	114	978
Total DNFBP – On-site Exams			67	61	28	165	101	50	472
Total DNFBPs			150	102	55	487	492	164	1 450
Total FIs and DNFBPs – Desk Exams			353	301	695	711	800	337	3 197
Total FIs and DNFBPs – On-site Exams			350	397	390	458	338	304	2 237
Total FIs and DNFBPs			**703**	**698**	**1 085**	**1 169**	**1 138**	**641**	**5 434**

257. Both FINTRAC and OSFI demonstrated that they apply scoping mechanisms within their examination strategies. Factors used by FINTRAC to prioritize examinations include: its follow-up strategy; concurrent assessments (with OSFI); market share; cycles; risk score; theme-based; regional selections and compliance coverage (used for lower risk where the preceding factors may not apply). OSFI primarily relies on its risk rating of FRFIs to inform its examination strategy and supervises on a cyclical basis with high-risk entities supervised on a three-year cycle, medium risk on a four-year cycle and low risk on a five-year cycle. It does, however, also supervise on a reactive basis arising out of information received from FRFIs, prudential supervisors or FINTRAC. An average on-site examination conducted by FINTRAC lasts between 2-3 days typically involving 2-3 supervisors, whereas on-site examinations of FRFIs typically last between 1 and 3 weeks and involves 10 or more supervisors from both OSFI and FINTRAC.

Supervision of FRFIs

258. Since 2013, FRFIs have been supervised by OSFI and FINTRAC concurrently. This involved examinations of high and medium risk FRFIs by each agency concurrently but with OSFI taking a top down (i.e. group wide) approach and FINTRAC taking a bottom up (i.e. individual entities/sector) approach with the two agencies coordinating their approaches during examinations but issuing separate supervisory letters setting out their respective findings. At the time of the on-site, it was planned to move to a more coordinated approach through joint examinations. Between 2009 and 2015, OSFI and FINTRAC conducted 126 assessments of FRFIs (OSFI carried out 78, FINTRAC carried out 48, and 22 were concurrent). During that period, OSFI and FINTRAC assessed all 6 D-SIBs (18 assessments in total) that hold a significant share of the Canadian financial market. OSFI issued 373 findings, including 97 requirements relating to lack of processes to comply with AML/CFT obligations and 276 recommendations relating to broader prudential AML/CFT risk management findings. The largest number of findings reflected changes that were required to correct or enhance

policies or procedures and the failure to ensure that risk assessment processed included prescribed criteria, and weaknesses in applying these criteria.

259. There is good supervisory coverage of FRFIs in Canada, which is being applied on a risk-sensitive basis. The level and intensity of the supervision of FRFIs was detailed to the assessment team by FINTRAC and OSFI, sample files were reviewed and feedback was also received from individual FRFIs during the on-site. OSFI provided examples of examinations and its follow-up activity including an AML/CFT examination of a major bank (D-SIB). A 2010 assessment of the bank found its AML/CFT program to be basic or rudimentary and there were 27 major findings ranging from instances of non-compliance with the PCMLTFA and weak risk management processes and policies. OSFI conducted an extensive follow-up program in tandem with the host regulators. When OSFI determined that the action plan to remedy deficiencies was not progressing satisfactorily it met with senior management in the bank. Enhanced monitoring by OSFI was implemented up until 2013 when the bank had adequately addressed the deficiencies to OSFI's satisfaction. Another example was provided involving a bank, which was a small subsidiary of a foreign bank and identified significant issues in its AML/CFT program, OSFI conducted quarterly monitoring of the bank which resulted in all recommendations being addressed by the bank. OSFI and FINTRAC provided examples where they have leveraged off each-others' supervisory findings including where a conglomerate life insurance company had issues with the process for submitting electronic fund transfer reports to FINTRAC that was subsequently reported to OSFI by FINTRAC that led to a prudential finding by OSFI. FINTRAC has also used OSFI's observations of compliance regime gaps to expand its standard scope of that RE to include a review of the compliance regime.

260. OSFI is taking measures to ensure that FRFIs heighten monitoring around overseas investment in Canada to mitigate any risk of illicit flows of funds entering the financial system. OSFI is also monitoring overseas branches of FRFIs as part of its group wide supervisory approach. There are three D-SIBs with branches in the Caribbean and South America. OSFI supervises FRFI on a group wide basis and FRFIs apply group wide policies and procedures and oversee controls (including ongoing monitoring of transactions) applied in overseas branches in Canada. From the discussions held and the material submitted it was found that OSFI exercises rigorous oversight of parent banks' group-wide controls in this key area.

261. Despite there being good supervisory coverage of FRFIs, the split of AML/CFT supervision generates some duplicative efforts. There are currently two agencies supervising FRFIs for AML/CFT compliance, which may be desirable given the size and importance of FRFIs, but suffers to some extent from insufficient coordination between the two agencies and duplication of supervisory resources. OSFI has a good understanding of its sectors and is implementing an effective supervisory regime with limited resources. FINTRAC has more resources but has a very wide population to supervise for AML/CFT compliance that may hinder a full appreciation of FRFIs' business models.

Supervision of non-FRFIs and DNFBPs

262. FINTRAC is applying its supervisory program to non-FRFIs and DNFBPs on an RBA. It is conducting more examinations in higher-risk sectors and using assistance, outreach, and compliance questionnaires to a large extent in sectors that it sees as lower-risk.

263. FINTRAC has shown that it is focusing mostly on high-risk non-FRFIs, securities, MSBs, and credit unions/*caisses populaires* for on-site examinations. It is, however, also conducting on-site examinations in lower-risk sectors, although it is conducting more desk exams in those sectors. FINTRAC also uses other supervisory tools for lower risk REs in the financial sector. On-site examinations have been undertaken by FINTRAC of non-FRFIs including securities dealers, credit unions and *caisses populaires*. The market share of credit unions is concentrated in a relatively small number of credit unions that are being supervised by FINTRAC and credit unions in Canada do not have cross-border operations. Another priority area for FINTRAC is the supervision of MSBs given the high-risk assigned to the sector. It has conducted a high number of examinations of MSBs relative to the size of the primary population figures provided to the assessment team. There appears to be ongoing cooperation between primary regulators and FINTRAC concerning the supervision of non-FRFIs based on details of referrals from other supervisors under MOU arrangements that were provided to the team. FINTRAC is adopting an adequate RBA to supervision of the non-FRFI sector.

264. FINTRAC applies intensive supervisory measures to casinos in line with the risks identified in the sector. This involves in-depth on-site examinations that are conducted on a cyclical basis that ranges from a two to five year cycle based on key factors such as size, risk level and market share. The three largest casinos (that represent 80% of the sector's market share) are examined on a two-year cycle. For other sectors, it has been relying on less intensive activities such as assistance and outreach to DNFBPs to build awareness of compliance obligations. FINTRAC identified the real estate sector and DPMS as medium-risk and accordingly is applying less intensive supervisory tools to those sectors. In the NRA, however, both sectors have been identified as high-risk. FINTRAC is therefore updating its risk assessment of these two sectors in line with the findings of the NRA with a view to applying more intensive measures in the future (including on-site examinations). FINTRAC is relying on the risk model (amongst other factors) of real estate agents to decide on examination selections to cover the sector. It also does not appear to identify adequately DPMS businesses in Canada that fall within the definition of the PCMLTFA.

265. FINTRAC utilizes lower intensity activities to good effect for lower-risk REs. Between 2011 and 2013, close to 10 000 compliance questionnaires (CARs) were issued to mainly sectors identified as lower or medium ML/TF risk. The questionnaire results were used to initiate close to 250 "themed-CAR" risk-informed examinations based principally on the significant non-compliance identified in the CAR. Observation letters are also used to highlight repeated non-compliance or reporting anomalies and remedial action is taken if the entity fails to respond or does not resolve the issues.

266. The legal profession is not currently subject to AML/CFT supervision due to a successful constitutional challenge that makes the PCMLTFA inoperative in respect of legal counsels, legal firms, and Quebec notaries. There is therefore no incentive for the profession to apply AML/CFT measures and participate in the detection of potential ML/TF activities. The exclusion of the legal profession from AML/CFT supervision is a significant concern considering the high-risk rating of the sector and its involvement in other high-risk areas such as the real estate transactions as well as company and trust formation. This exclusion also has a negative impact on the effectiveness of the supervisory regime as a whole because it creates an imbalance amongst the various sectors, especially for REs that perform similar functions to lawyers.

Remedial actions and effective, proportionate, and dissuasive sanctions

267. Supervisors in Canada take a range of remedial actions. There is also an administrative monetary penalties (AMPs) regime in place that is the responsibility of FINTRAC to apply under the PCMLTFA. OSFI and FINTRAC require REs to remediate any deficiencies identified during the assessment process. OSFI has implemented a graduated approach to applying corrective measures or sanctions for FRFIs. Both OSFI and FINTRAC issue supervisory letters to entities subject to AML/CFT assessment that contain supervisory findings and REs are required to take appropriate remedial action. OSFI has provided examples of follow-up action it has taken when FRFI fails to take remedial action.

268. OSFI and FINTRAC have thorough ongoing monitoring and follow-up processes to ensure remediation and have provided examples of steps taken to ensure that deficiencies have been addressed in the FRFI sector, MSBs and a large FI. Measures taken by supervisors include follow-up meetings, further examinations, action plans, and sanctions. OSFI may "stage" FRFIs, which is an enhanced monitoring tool involving four stages where severe AML/CFT deficiencies remain unaddressed. Staging is an effective tool to improve compliance as demonstrated by the Canadian authorities in case studies. There were examples provided where a small bank had not applied AML/CFT obligations correctly and where a staged RE underwent follow-up examinations demonstrated the process increased compliance. FINTRAC also provided examples of monitoring activities of non-FRFIs and DNFBPs where follow-up meetings and re-examinations of MSBs and large FIs resulted in significant improvements in compliance. Remedial actions have also been applied when REs failed to respond to mandatory CARs in the real estate sector. Follow-up activities on all non-responders found that of 55 non-responders, 37 were inactive REs, 1 was a late responder, 10 had inaccurate addresses, and 7 were true non-responders (i.e. increasing RE's risk profile). Where low levels of reporting have been identified, FINTRAC has conducted examinations and put in place remedial actions to increase reporting. This appears to have had an effect on reporting in the institutions concerned, but does not address the wider issue of general low levels of reporting. Supervisors have demonstrated that effective steps have been taken to a large extent to ensure that remediation measures are in place to address AML/CFT deficiencies.

269. FINTRAC can apply sanctions on all REs (including FRFIs) under the AMP regime. AMPs have been imposed and non-compliance disclosures (NCD) have been made to LEAs by supervisors for serious AML/CFT breaches and failure to address significant deficiencies. A notice of violation (NOV) is issued to the RE outlining the violation and penalty prior to an AMP being imposed. The most common violations cited in a NOV were for compliance regime deficiencies and reporting violations. AMPs are not always made public but can be published in egregious cases. AMPs have been imposed in the credit unions and *caisses populaires*, securities, MSBs, casinos, and real estate sectors but at the time of the on-site an AMP had not been applied to a FRFI. The imposition of AMPs in the MSB and casino sector was reported to have had a significant dissuasive effect in those sectors and FINTRAC confirmed that compliance had improved in those sectors as a result. However, the level of AMPs being applied is low relative to the reporting population and the size of the Canadian market. AMPs had not been applied to FRFIs at the time of the on-site is an issue that needs to be addressed. The non-sanctioning of FRFIs, the low number of AMPs applied to other FIs and the low

level of fines imposed to date is unlikely to have a dissuasive effect on FRFIs/larger FIs given their market share and the resources available to them. FINTRAC provided the assessors with current statistics at the time of the on-site (see table below) and with figures for NOVs, which included, among others, the FRFI sector, but for which proceedings were not concluded. OSFI has published guidelines for FRFIs on AML/CFT compliance, and while these guidelines cannot result in a financial penalty under OSFI's regulatory enforcement regime they are subject to measures such as staging.

Table 20. **Administrative Monetary Penalties for AML/CFT Breaches Between 1 April 2010 and 31 March 2015**

Sector	NOV Issued	Reporting Entity Size				Total Value of NOVs Issued (in CAD)	Publicly Named
		Micro	Small	Medium	Larger		
Casino	4	0	0	0	4	2 435 500	0
Financial Entities	15	0	6	9	0	897 705	3
MSB	28	22	5	1	0	768 375	16
Real Estate	7	6	1	0	0	197 310	2
Securities	5	0	3	2	0	587 510	4
Total	**59**	**28**	**15**	**12**	**4**	**4 886 400**	**25**

270. FINTRAC can submit an NCD to LEAs for failure to comply with the PCMLTFA, but this is only done in the most serious cases. Between 2010/2011 and 2014/2015, FINTRAC submitted seven NCDs (all from the MSB sector). These resulted in five investigations being commenced with two cases leading to criminal charges and one conviction (two individuals and one RE).

271. There are proportionate remedial actions being taken by supervisors, in particular extensive follow-up activities by supervisors (e.g. staging by OSFI) that demonstrated their dissuasive effect on the RE involved in the process as it exposes the RE being "staged" to costly remedial activities over a long period of time and ancillary costs such as higher deposit insurance premiums. While remedial actions, as opposed to AMPs, appear effective with respect to the individual RE they apply to, their wider dissuasive impact on other entities is limited, notably because they are not made public. More importantly, the lack of AMPs being applied to FRFIs and the relatively low level of fines imposed negatively impact the effectiveness of the enforcement regime as it affects its dissuasiveness. The non-application of the AMP regime to OSFI guidelines also affects the effectiveness of the Canadian supervisory regime.

Impact of supervisory actions on compliance

272. FINTRAC and OSFI provided examples where their actions have had an effect on compliance through the use of action plans, follow-up activities and findings from subsequent examinations. Feedback from the private sector indicates that supervisors' actions have led to increased compliance in the financial sector. There were examples given of increased compliance in

the FRFI, MSB and insurance sectors arising out of examinations and follow-up activities conducted by supervisors. It was reported by the private sector that the "close touch" nature of OSFI's supervision has enhanced compliance by FRFIs with their AML/CFT obligations. There has been an increase in compliance by REs as FINTRAC's compliance activities increased in recent years, e.g. MSB and casinos, and with the publication of additional information about PCMLTFA obligations.

273. FINTRAC and OSFI have provided written examples of examination findings and follow-up outcomes that demonstrate their effect on compliance by specific FIs and DNFBPs. There has been an increase in compliance among FRFIs and non-FRFIs (casinos) that are subject to cyclical examinations. The more intensive focus on higher risk areas in examination selection strategies has increased compliance in sectors such as FRFIs, MSBs, securities dealers and credit unions.

274. OSFI and FINTRAC supervisory measures to ensure compliance and their remedial actions are having a clear effect on the level of compliance of the individual RE that they apply to. OSFI has a robust follow-up system to monitor the remediation of deficiencies identified. OSFI requires FRFIs provide documentary evidence supporting progress on a continuous basis and requires validation prior to closure of every finding. Quarterly monitoring meetings are conducted with every D-SIB, and meetings with other FRFIs are frequently conducted at the request of OSFI or the FI when there are significant concerns or outstanding issues. Significant remedial steps have been taken by FRFIs based on findings by supervisors and OSFI has demonstrated that it has comprehensive supervisory measures to ensure compliance including the use of more intensive supervision (staging). FINTRAC's follow-up activities have been shown to have a positive effect on compliance by non-FRFIs and DNFBPs. It conducted 515 subsequent examinations across non-FRFIs and DNFBPs over a three-year period and by comparing previous performance indicators with the follow-up indicators revealed that the average deficiency rate had reduced by 13% due to increased compliance. AMPs, when applied, have also had a positive effect on the compliance of REs as demonstrated in follow-up examinations.

275. FINTRAC uses a supervisory tool that assigns "deficiency rates" to REs that are examined. It rates the levels of non-compliance on each specific area of the examination that leads to an overall deficiency rating being assigned to the RE. The overall rating is high, medium, or low and the RE's rating is used to tailor appropriate remedial measures to be put in place. Once remediation has occurred, a follow-up rating is applied and this is compared with the previous rating to identify whether compliance improvements have been made by the RE. The use of deficiency rates at RE and sector level is a useful tool to measure the effect the examination and follow-up process has on compliance by REs. Overall, supervisory measures taken in Canada are having an effect on compliance with improvements demonstrated –albeit to varying degrees- both in the financial and DNFBP sectors. Information provided indicates that compliance has improved in the financial sector, but less so in DNFBPs particularly in the real estate and DPMS sectors.

Promoting a clear understanding of AML/CTF obligations and ML/TF risks

276. There is a good relationship and open dialogue between OSFI and FRFIs. The private sector reports that OSFI has a good understanding of the compliance challenges faced by FRFIs and provides constructive feedback. OSFI has published compliance guidelines and raises awareness

through participation in outreach activities. FINTRAC has published a substantial amount of guidance on its website and increased its level of feedback and guidance to both the financial and, albeit to a lesser extent, the DNFBP sectors. FINTRAC deals with general enquiries through a dedicated call line and has published query specific policy interpretations, both of which are reported by the private sector to be good guidance tools. FINTRAC has dealt with a substantial amount of queries and it has a "Major Reporters" team that provides guidance directly to the largest reporters (mostly financial sector and casinos). It has also taken good steps to raise awareness amongst the MSB sector around the requirement to register and to explain AML/CFT obligations. However, more focused and sector-specific guidance and typologies is required for the financial sector as well as further tailored guidance for DNFBPs to enhance their understanding of the ML/TF risks that they face and of their AML/CFT obligations, particularly with respect to the reporting of suspicious transactions.

277. Supervisors have increased AML/CFT awareness through the use of presentations, seminars, public-private sector forums, establishment of OSFI supervisory colleges, and meetings with the industry. FINTRAC has engaged with non-FRFIs and DNFBPs conducting 300 presentations between 2009 and 2015. It has also hosted events to raise awareness on compliance obligations including a Major Reporters Forum in the financial sector in 2014 and a Casino Forum in 2015.

278. Overall, in light of supervisors' efforts and ML/TF risks in Canada, FINTRAC provides good quality general guidance to REs, but not enough sector-specific compliance guidance and typologies especially in the real estate and DPMS sectors.

Overall Conclusions on Immediate Outcome 3

279. **Canada has achieved a substantial level of effectiveness with IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

Canadian legal entities and arrangements are at a high risk of misuse for ML/TF and mitigating measures are insufficient both in terms of scope and effectiveness.

Some basic information on legal persons is publicly available. However, nominee shareholder arrangements and, in limited circumstances bearer shares, pose challenges in ensuring accurate, basic shareholder information.

Most TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information. These pose significant loopholes in the regime (both in terms of prevention and access by the authorities to information).

FIs do not verify beneficial ownership information in a consistent manner.

The authorities rely mostly on LEAs' extensive powers to access information collected by REs. However, there are still many legal entities in Canada for which beneficial ownership information is not collected and is therefore not accessible to the authorities.

Access to beneficial ownership is not timely in all cases and beneficial ownership information is not sufficiently used.

For the majority of trusts in Canada, beneficial ownership information is not collected.

LEAs do not pay adequate attention to the potential misuse of legal entities or trusts, in particular in cases of complex structures.

Recommended Actions

Canada should:

- As a matter of priority, increase timeliness of access by for competent authorities to accurate and up-to-date beneficial ownership information - consider additional measures to supplement the current framework.
- Take the necessary steps to make the AML/CFT requirements operative with regards to all legal professions providing company or trust-related services.
- Ensure that FIs and DNFBPs identify and take reasonable measures to verify the identity of beneficial owners based on official and reliable documents.
- Take appropriate measures to prevent the misuse of nominee shareholding and director arrangements and bearer shares.
- Ensure that basic information indicated in provincial and federal company registers is accurate and up-to-date.
- Apply proportionate and dissuasive sanctions for failure by companies to keep records; to file

information with the relevant registry; or to update registered information within the required 15-day period.

- Determine and enhance the awareness of the ML and TF risks from an operational perspective and the means through which legal persons and trusts are abused in Canada, taking into account ML schemes investigated in Canada as well as international typologies involving legal entities and legal arrangements.

The relevant Immediate Outcome considered and assessed in this chapter is IO5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25.

7

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

280. Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) provides a comprehensive overview and comparison on its internet homepage of the various types, forms, and basic features of federal corporations under CBCA, and gives detailed guidance on the incorporation process.[86] Similar information and services are provided through the homepages of all provincial governments except that of New Brunswick. The relevant web links are easy to find through ISEDC's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity. In addition, the Canada Business Network, a collaborative arrangement among federal departments and agencies, provincial and territorial governments, and not-for-profit entities aimed at encouraging entrepreneurship and innovation also provides comprehensive information on the various types of legal entities as well as various forms of partnerships available at the federal and provincial/territorial levels.[87] For legal arrangements, the CRA provides on its homepage comprehensive information on the various trusts structures available under Canadian law.[88]

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

281. Both legal entities and legal arrangements in Canada are at a high risk of being abused for ML/TF purposes. The NRA indicates that organized crime and third-party ML schemes pose a very high ML threat in Canada. Some of FINTRAC's statistics reflected in the NRA suggest that well over 70% of all ML cases and slightly more than 50% of TF cases involved legal entities. Canadian legal entities play a role in the context of channelling foreign POC into or through Canada, as well as in the

[86] See www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.

[87] See Canada Business Network (nd), Sole proprietorship, partnership, corporation or co-operative?, www.canadabusiness.ca/eng/page/2853/#toc- corporations.

[88] See Canada Revenue Agency (nd), Types of trusts, www.cra-arc.gc.ca/tx/trsts/typs-eng.html.

laundering of domestically generated proceeds.[89] Typologies identified include: foreign PEPs creating legal entities in Canada to facilitate the purchase, of real estate and other assets with the proceeds of corruption; laundering criminal proceeds through shell companies in Canada and wiring the funds to offshore jurisdictions; and utilization of Canadian front companies to layer and legitimize unexplained sources of income and to commingle them with or mask them as profits from legitimate businesses.[90]

282. LEAs generally concurred with the NRA's findings, and have observed a high number of companies being established without carrying out any business activities, and the use of corporate entities and trusts in Canada to facilitate foreign investment. LEAs also stated that they encounter difficulties in identifying beneficial owners of Canadian companies owned by entities established abroad, particularly in the Caribbean, Middle East, and Asia. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities and legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. Some LEAs are therefore less familiar with ML typologies involving corporate structures. Also, in a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners.

Mitigating measures to prevent the misuse of legal persons and arrangements

283. Canada has a range of measures available to collect information on the control and ownership structures of legal entities as outlined below, and comprehensive investigation powers to locate and obtain such information if and as needed (see also R. 24). (i) In cases where a legal entity enters into a business relationship with a Canada FI, that FI must collect and keep beneficial ownership information. (ii) The federal register or the provincial register where the legal entity is incorporated must collect information; and the CRA collects information on legal entities as part of the tax return. (iii) The legal entities themselves are required to keep records of their activities, shareholders and directors. For public companies listed on the stock exchange disclosure requirements exist for shareholders with direct or indirect control over more than 10% of the company's voting rights. Only measure (iii) —maintenance of records by the companies— apply to all legal entities created in Canada.

284. Legal entities in a business relationship with a Canadian FI must provide basic and beneficial ownership information to the FI which has an obligation under the PCMLTFA to maintain this information and confirm its accuracy as needed (see R.10). Many of the FIs that the assessors met confirmed that beneficial ownership would generally be obtained through self-disclosure by the customer, and, in some instances, be followed by an open data search to confirm the accuracy of the information provided. Most FIs stated that they would not require the customer to provide official

[89] FINTRAC Research Brief: Review of Money Laundering Court Case between 2000 and 2014 determines that one of the most frequently used vehicles for ML (in a sample of 40 Canadian Court Cases reviewed) were companies acting as shells for or allowing for a commingling of illicit proceeds with regular business transactions.
[90] Ibid. as well as Project Loupe and Project Chun.

documents to establish the identity of the beneficial owners, nor carry out any independent verification measures other than the open data search. Of the 2.5 million registered legal entities in Canada and customers of a Canada FI, only a fraction had accuracy checks performed with respect to beneficial ownership. In addition, the mitigation of risks is limited by the fact that TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information.

285. Federal and provincial registers record basic information on Canada companies and their directors, as well as on partnerships with businesses in Canada, but do not require the collection of beneficial ownership information. Alberta and Quebec have slightly more comprehensive registration mechanisms, which also cover shareholder information. All information maintained in the federal and provincial registers is publicly available. Updating requirements exist and violations thereof can be sanctioned criminally, but no sanction has been imposed in practice. The reliability of the information recorded raises concerns because there is no obligation on registrars to confirm the accuracy of the basic company information provided at the time of incorporation. Once the incorporation has been completed, companies are obliged to update their records held by the government registrar when there is a material change (e.g. a change in directors) and on an annual basis, and may do so electronically. The same situation applies to partnerships that register for a business permit. The updating process of registered information involves the company reviewing the information indicated in the register and confirming that the information is still correct. There is no need to submit any supporting documents. Despite the absence of verification process at the company registration stage, LEAs stated that basic company information would generally be reliable and comprehensive both on the provincial and federal levels, but they also raised concerns with respect to the accuracy and completeness of shareholder information in the registers of Quebec and Alberta. The CRA, as part of its tax revenue collection obligation, also obtains information on legal entities. However, such information does not include beneficial ownership information.

286. All legal entities, whether incorporated or registered at the federal or provincial level, are subject to record-keeping obligations. All statutes require the keeping of share registers, basic company information, accounting records, director meeting minutes, shareholder meeting minutes and the company bylaws and related amendments. While the relevant obligations are relatively comprehensive, their implementation raises serious concerns. ISEDC and provincial company registries indicated that they would consider company laws to be "self-enforcing" by shareholders, interested parties and the courts, and that they would have no mandate to enforce the implementation of the relevant provisions. While the Director of Corporations Canada has statutory powers to inspect company records, this power has been used only in the context of a shareholder's complaint and not to verify whether a company complies with its record-keeping obligations or to assist the RCMP in obtaining relevant information. So far, no company has been sanctioned criminally for failure to keep accurate and comprehensive company records. The LEAs expressed concern over the accuracy and completeness of companies' records, and stated that it would often be difficult to establish the true shareholder of a company as shareholder registers would often be either outdated or imprecise as they would not indicate whether the registered shareholder is the actual beneficial owner of the share or a proxy for another person.

287. Disclosure obligations for publicly listed companies are comprehensive and include beneficial ownership information.

288. Both bearer shares and nominee shareholders and directors are permitted in Canada. According to the authorities, bearer shares are rarely issued, but nominee shareholder arrangements are a frequent occurrence, and typically involve the issuance of shares in the name of a lawyer, who holds the shares on behalf of the beneficial owner. While companies are generally obliged to keep share registers, there is no obligation on nominees to disclose their status and information on the identity of their nominator, nor to indicate when changes occur in the beneficial ownership of the share.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

289. For information that is not publicly available, Canada has a wide range of law enforcement powers available to obtain beneficial ownership information as discussed in R.24. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities or legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. In a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners. This was due mainly to foreign jurisdictions not responding to requests by the Canadian authorities for beneficial ownership information.

290. As indicated in IO 6, other important practical limitations hamper the effectiveness of investigations relating to legal entities and legal arrangements. Despite the adequacy of their powers, it is often difficult for LEAs to obtain beneficial ownership information. As a result, their access to that information is not timely. The relevant Director under each corporate statute has the power to request company records but in practice this power has never been used to assist the RCMP in obtaining beneficial ownership information on a specific legal entity. Equally, at the time of the on-site visit the CRA had not made use of its newly acquired power to refer information to the RCMP in case of a suspicion of a listed serious offense.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

291. The level of transparency of legal arrangements is even lower than in the case of legal entities. There are two mechanisms in place to collect information on trusts: (i) the CRA, as part of the tax collection process, requires the provision of information on the trust assets and the trustee; and (ii) FIs are required to obtain information in relation to customers that are or represent a trust. These two measures suffer from significant shortcomings, both in terms of their scope and effective implementation, for the same reasons as in the context of legal persons, and only a small fraction of Canadian trusts file annual tax returns. There is also a fiduciary duty under common law principles of trustees vis-a-vis those who have an interest in the trust. While this makes it necessary for the

trustee to know who the beneficiaries are, it does not necessarily mean that trustees keep records or obtain information on the beneficial ownership of the trust in practice.

292. The information collected by FIs about legal arrangements raise the same concerns of reliability as outlined for legal entities because FIs rely mostly on the customer to declare the relevant information, they do not require official documentation to establish the identity of the beneficial owners, and do not conduct an independent verification of the information provided. Furthermore, there is no obligation on trustees to declare their status to the FI. As a result, in many cases, the FI may not know that the customer is acting as a trustee. It is unclear how many of the millions of trusts estimated to exist under Canadian law are linked with a Canadian FI.

Effectiveness, proportionality and dissuasiveness of sanctions

293. Proportionate and dissuasive criminal sanctions are available under the PCMLTFA, the CBCA and provincial laws for failure by any person to comply with the record-keeping obligations or registration or updating requirements under the law (see write up for R.24 for more details), but none have been imposed between 2009 and 2014.

294. So far, there seems to have been few instances in which administrative measures were applied for a failure by FIs to identify the beneficial owner or confirm the accuracy of the information received. Similarly, no legal entity in Canada has been struck off the company registry based on in its involvement in illicit conduct. In sum, sanctions have not been applied in an effective and proportionate manner.

Overall Conclusions on Immediate Outcome 5

295. **Canada has achieved a low level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

International cooperation is important given Canada's context, and Canada has the main tools necessary to cooperate effectively, including a central authority supported by provincial prosecution services and federal counsel in regional offices.

The authorities undertake a range of activities on behalf of other countries and feedback from delegations on the timeliness and quality of the assistance provided is largely positive. Assistance with timely access to accurate beneficial ownership information is, however, challenging, and some concerns were raised by some Canadian LEAs about delays in the processing of some requests.

The extradition framework is adequately implemented.

Canada also solicits other countries' assistance to fight TF and, to a somewhat lesser extent, ML.

Informal cooperation appears effective amongst all relevant authorities, more fluid and more frequently used than formal cooperation, but the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs filed by DNFBPs limit the range of assistance it can provide.

Recommended Actions

Canada should:

- Ensure that, where informal cooperation is not sufficient, LEAs make greater use of MLA to trace and seize/restraint POC and other assets laundered abroad.
- Ensure that good practices, such as consultation with prosecution services are applied across police services with a view to improve the use of MLA to identify and pursue ML, associated predicate offenses and TF cases with transnational elements.
- Assess and mitigate the causes for the delays in the processing of incoming and outgoing MLA requests.
- Consider amending the MLACMA to include the interception of private communications (either by telephone, email, messaging, or other new technologies) as a measure that can be taken by the authorities in response of a foreign country's MLA request without the need to open a Canadian investigation.

The relevant Immediate Outcome considered and assessed in this chapter is IO2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Cooperation)

Providing constructive and timely MLA and extradition

296. Since its previous assessment, Canada has greatly improved its statistics on MLA, and is now able to show several different aspects of MLA related to ML and TF. Canada receives a large number of MLA requests each year. From 2008 to 2015, it received a total of 4,087 MLA requests across all offenses, including 383 for ML investigations and 34 related to TF investigations.

297. The IAG[91] prioritizes the requests (in terms of urgency, court date or other deadline, seriousness of the offense, whether the offense is ongoing, danger of loss of evidence, etc.); it contacts the foreign authorities to obtain further information if the request is incomplete or unclear; and forwards it to the Canadian police for execution (if no court order is needed), or to the IAG's provincial counterparts, or to a counsel within federal DOJ Litigation Branch, if a court order is required.

298. Canada generally provides the requested assistance, both in the context of ML and TF cases:

Table 21. **Outcome of Incoming MLA Requests for ML**

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	24	0	4	2
2009–2010	23	1	1	0
2010–2011	21	1	5	1
2011–2012	42	5	4	0
2012–2013	39	1	8	3
2013–2014	56	5	8	0
2014–2015	48	4	6	1
TOTAL	253	17	36	7

Table 22. **Outcome of Incoming MLA Requests for TF**

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	10	0	0	0
2009–2010	2	1	2	0
2010–2011	6	0	0	0
2011–2012	3	1	1	0
2012–2013	5	0	0	0
2013–2014	0	1	0	0
2014–2015	8	0	0	0
TOTAL	34	3	3	0

[91] The IAG is part of the Litigation Branch of the federal DOJ, and which assists the Minister of Justice as central authority for Canada.

299. The assistance provided is of good quality, as was confirmed by the feedback received from 46 countries. There have been numerous good cases of assistance, especially with the US, including covert operations, joint investigations and extraditions. This is an important positive output of the Canadian framework in light of the risk context (e.g. the extensive border with the US, the size of the US economy, and the opportunities it offers to criminal activity).

300. Canada undertakes a range of activities on behalf of other countries. It is, however, limited in its ability to provide in a timely manner accurate beneficial ownership information of legal persons and arrangements established in Canada, for the reasons detailed in IO.5 and IO.7. The fact that Canada cannot intercept, upon request, private communications (either telephone or messaging) in the absence of a Canadian investigation can also hamper foreign investigations, especially those pertaining to OCGs from or with links to Canada or international ML. While this measure is not specifically required by the standard, it is particularly relevant in the Canadian context given the high risk emanating from OCGs, including those with ties to other countries. The scope of this practical shortcoming is, however, limited by the fact that, in most instances, a domestic investigation is likely to be initiated, thus enabling the Canadian authorities to share evidence collected from wiretaps.

301. To facilitate MLA, Canada entered into 17 administrative arrangements with non-treaty partners over the past two years. It also executed over 300 non-treaty requests, mostly to interview witnesses and to provide publicly available documents.

302. Measures were also taken to expedite MLA. The IAG may now send the information requested by a foreign country directly, without the need for a second judicial order. The evidence shared includes, for example, transmission data for an electronic or telephonic message, which help identify the party communicating, tracking data that identify the location of a person or an object, information about a bank account and the account holder. In addition, LEAs that have obtained evidence lawfully for the purposes of their own investigation, may share this information with foreign counterparts without the need for a judicial order authorizing this sharing. For example, evidence obtained through wiretapping by Canadian police may be shared with foreign counterparts in this manner, as confirmed by case law.[92]

303. According to the feedback from delegations, the average time for Canada to respond to their requests varies between 4 and 10 months. The majority of delegations stated that assistance was timely, or did not comment on timeliness, with only one country commenting that the process was slow. Some Canadian LEAs also expressed concerns with the length of time taken to process some of the incoming and outgoing requests. The IAG explains that some of the factors that contribute to lengthening the process include: (i) missing information in the request and the requesting state's slow response to requests for clarification or additional information; (ii) litigation (i.e. when a party affected by the request contests the validity of the court order required, particularly in instances the litigation continues into appellate courts; (iii) because the fact that Canada is awaiting the fulfilment of a condition by the foreign authorities (e.g. in cases where Canada has restrained assets, a final judgment of forfeiture issued by the relevant foreign court may be pending); and (iv) the complexity of the file (e.g. cases involving multiple bank accounts, many witnesses, several Canadian provinces and successive supplemental requests). According to the Auditor General Report 2014, the DOJ processes formal requests for extradition and obtains evidence from abroad appropriately, but does not monitor the reasons

[92] See Supreme Court's decision in *Wakeling v. United States of America* 2014 SCC 72.

for delays in the process.[93] The report found that only 15% of the overall time needed to process MLA requests are within Justice Canada's control, and 30% of the overall time to process extradition requests are within its control. Justice Canada can only take actions to mitigate the delays when it develops insight about the reasons for the delays. In response to the comments by the Auditor General of Canada and after consultations with its international partners and closer research of its files in more recent years, there has been a significant reduction in the delays associated with executing MLA requests made to Canada.

304. Canada extradites its nationals. Pursuant to the Supreme Court of Canada's decision in *U.S. v. Cotroni*, where the extradition of a Canadian citizen is sought based on facts that might form the basis for a prosecution in Canada, certain consultations and an assessment of evidence and circumstances must take place before a decision can be made as to whether to prosecute or extradite. In 99% of such cases, the circumstances favour extradition. Between 2008 and 2015, Canada received 92 extradition requests based on a charge for ML. From the 92 requests, 77 came from the US. As a result of these requests, a total of 48 persons were extradited, while 13 were subject to other measures such as deportation, discharge, voluntary return, or were not located or the means of the return not listed. In the seven cases where the request was refused, the grounds were related either to insufficient evidence to show knowledge of ML, concerns with human rights record or prison conditions in the requesting state, or the defendant was not located. Between 2008 and 2015, five persons were extradited for TF.

305. More than half (52%) of the extradition requests take from 18 months to five years to be completed; from which 28% take from three to five years to be completed. An approximate of 4% take more than five years to be completed. Most of the delegations mentioned having successful extradition requests with Canada, although some mentioned having experienced delayed responses from the Canadian authorities regarding those requests.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

306. From 2008 to 2015, Canada sent more than 700 MLA requests, including 124 (i.e. around 17%) on the grounds of ML charges. Some requests were made, e.g. in the context of real estate or to obtain bank records, as well as to freeze and confiscate funds or assets abroad.[94] Most of these requests were made on the basis of investigations conducted in the province of Quebec (which is in line with the findings in IO.7 and IO.8). Between 2008 and 2015, Canada also made 24 requests in the context of TF investigations, 11 of which during fiscal year 2014/2015 in light of increased concern about "foreign fighters."

307. The number of request for assistance on ML cases has increased over the years, but still appears relatively low in light of Canada's risk profile. The authorities explained that they frequently have recourse to informal means of cooperation (see core issue 2.3 below) in lieu of MLA because it is quicker. However, while informal means do simplify and expedite the process

[93] Office of the Auditor General of Canada (2014), Report of the Auditor General of Canada—Fall 2014, p. 11, www.oag-bvg.gc.ca/internet/docs/parl_oag_201411_02_e.pdf. The assessors reviewed 50 extradition and MLA files from between 2011 and 2013, which included incoming and outgoing requests, and both ongoing and closed files.

[94] From 2008 to 2005, Canada sent 113 requests with respect to tracing (bank or real estate records) and 33 requests with respect to freezing/restraint (funds or assets).

of assistance, they cannot substitute formal MLA in all cases (e.g. when there is a need for the tracing or the freezing of assets abroad). The relatively small number of outgoing requests may also be explained by the fact that Canada is not pursuing complex and transnational ML schemes to the extent that it should (see IO.7). Although the outflows of POC generated in Canada appear to be moderate in comparison to the inflows of POC generated abroad, data suggests that Canadian citizens and corporations use tax havens and offshore financial centres to evade taxes, in particular those located in the Caribbean, Europe and Asia- cooperation with the relevant countries in these regions would therefore prove helpful to Canada. Some domestic provincial LEAs mentioned concerns about the delay in the sending of requests to foreign countries. In response to that point, the IAG assures that the same case management prioritization measures are in place for outgoing requests as for incoming requests.

Seeking other forms of international cooperation for AML/CTF purposes

308. Canadian agencies regularly seek and provide other forms of international cooperation to exchange financial intelligence and other information with foreign counterparts for AML/CFT purposes. In particular, the cases studies provided as well as the discussions held on-site indicate a regular use by LEAs of foreign experts, missions abroad to secure evidence and assets, and joint investigations. Canada does not separate the information according to the function (i.e. seeker or provider of assistance), and the information provided therefore combines the objects of core issues 2.3 and 2.4.

309. FINTRAC is both a FIU and a regulator/supervisor:

- As Canada's FIU: FINTRAC is a member of the Egmont Group and shares information only on the basis of MOUs with counterparts. FINTRAC is open to sign a MOU with any FIU, and the process can be concluded very quickly, but sometimes this does not happen due to the absence of interest of the foreign FIU. At the time of the on-site there were 92 MOUs with foreign FIUs. In the absence of an MOU, they cannot share information. According to the feedback provided by other delegations, the information provided by FINTRAC is of good quality. Nevertheless, some limitations have a negative impact on the type of information that FINTRAC can share: more specifically, the fact that (i) FINTRAC is not habilitated to request and obtain further information from any REs; (ii) there are no STRs from lawyers. Canada receives far more requests for assistance than it sends to support Canadian investigations and prosecutions. Although there were fewer queries sent to its foreign counterparts a few years ago, FINTRAC has recently increased the number of requests sent. The queries received and sent to the US (which, as mentioned above, is a major Canadian partner in international cooperation) are generally comparable. In addition to requests sent, the significant increase of FINTRAC's numbers of proactive disclosures sent to its counterparts (2012-2013:52; 2013-2014:93; 2014-2015:190) highlights the Canadian FIU's willingness to share the relevant information it holds with its foreign partners.

- As a supervisor, FINTRAC regularly shares information with foreign supervisors and consults with international partners. In addition to general information, it also exchanges, on an on-going basis, since 2009, compliance information on operational processes with AUSTRAC. After several bilateral meetings, FINTRAC and AUSTRAC are working together in compliance actions on an MSB that operates both in Canada and in Australia. FINTRAC's public MSB registry was also provided to Australia and other jurisdictions, because the comparison of MSB lists is useful during the criminal record check of MSBs, who may operate in more than one country. FINTRAC has also an MOU with FINCEN.

310. The RCMP regularly exchanges information with its foreign counterparts. Cooperation is developed through police channels (Interpol, Europol, Five Eyes Law Enforcement Group), through the Camden Asset Recovery Informal Network (CARIN) and through several MOUs, including one with The People's Republic of China. The existence of this MOU with China is important in light of the risks of inward flow of illicit money generated in China; however, no assistance with this country was reported in the province of British Columbia, despite the fact that it appears to be at greater risk of seeing its real estate sector misused to launder POC generated in China. The RCMP uses a well-established and effective network of liaisons officers (42 officers and 10 intelligence analysts in 26 countries) to seek and provide assistance and other types of information, in ML and TF investigations. It shares intelligence information, carries out investigations on behalf of foreign counterparts, and participates in joint investigations, as demonstrated in several cases studies provided by the authorities. From 2008 to 2013, it sent 98 requests for assistance on PPOC and ML/TF-related occurrences to the US, 94 to Europe and 60 to Asia. The RCMP and other police forces are also the ones who execute incoming requests of assistance, when there is no need for a judicial order, and the information or documentation is publicly available or can be obtained on a voluntary basis.

311. OSFI concluded 30 MOUs with various international prudential supervisors. No statistical information was provided in this respect but the authorities mentioned that OSFI regularly exchanges information regarding FRFIs with its foreign counterparts. In 2012, OSFI hosted an AML/CFT Supervisory College on five conglomerate banks with 19 foreign regulators in attendance. The College provided an opportunity for the foreign regulators to provide information on AML/CFT supervision in the host jurisdictions, and also for the banks themselves to provide an overview of their AML/CFT programs. The OSFI Relationship Management Team also hosts Supervisory Colleges of a general prudential nature, where foreign regulators attend. When OSFI conducts assessments at foreign operations of FRFIs, it seeks cooperation of the host regulator, who usually participates on the on-site with OSFI. The Colleges are an important and effective way for the sharing of information with OSFI's foreign counterparts.

312. The CBSA cooperates on a regular basis with US Immigration and Custom Enforcement (ICE) and US Custom Border Protection for the Sharing of Currency Seizure Information, including in AML/CFT matters. This cooperation is very important due to the extensive border shared by Canada and the US Cases provided by the authorities demonstrated the CBSA's participation in joint operations. CBSA also receives information from the US Department of Homeland Security, which helps the detection of suspected POC and leads to the seizure of the currency. Its participation in the Homeland's Security BEST Program resulted in the CBSA

initiating 103 criminal investigations related to the smuggling of narcotics, smuggling of currency and firearms and illegal immigration. The CBSA also receives international cooperation from foreign governments or law enforcement and maintains strong collaboration with the 5-Eyes Community. It shares FINTRAC results with partner agencies in the US on files that indicate ML activities that cross the Canada/US border (Mexican Mennonites, outlaw motorcycle gangs, Persian organized crime). Nevertheless, the authorities also mentioned that financial information and information on import and export files declared in Canada are difficult to obtain by their counterparts, due to Canada's strong privacy framework.

313. The CRA has 92 Tax treaties and 22 Tax Information Exchange Agreements (TIEA) with international partners. However, CRA and CBSA do not cooperate under the Customs Mutual Assistance Agreement with the US. As is common for Canadian authorities, they would always require and MLAT to share the information regarding trading operations (where there is an important risk of trade-based ML, especially considering that more than 60% of Canada's GDP consists of international trade). Between 2009 and 2015, the CRA sent 72 requests and received 11 requests for exchange of information to foreign counterparts, in the context of criminal investigations.

314. The CSIS regularly receives from and shares financial information with FINTRAC in support of both organizations' mandates. In relation to high-risk travellers, it uses financial intelligence to determine how ready an individual may be to travel by determining whether they have purchased equipment, or if they have saved up money that could be used to support themselves while they are abroad. Due to confidentiality issues and matters of national security, CSIS did not provide the assessors any statistical data.

315. Feedback from the countries on Canada's assistance through other forms of cooperation is generally good. Most of the delegations indicated that the information received from FINTRAC in response to their requests was useful, of good content and of high quality. The limitation to request further information from any REs and bank information was, however, also reported. FINTRAC's average time to respond to request from its counterparts is 35 days (which is in line with the Egmont Group standards).The feedback from the US FIU is very positive. FINTRAC and FINCEN have had a strong working relationship for years, both as FIUs and as AML/CFT supervisory/regulatory agencies, which is very important in light notably of the extensive border between the two countries, the illicit flows of criminal money, as well as the linkages between OCGs active in both countries. The US, which is Canada's main partner in cooperation, also reported and outstanding cooperation exchange with CRA. They indicated that the CRA responds to American requests for records in a very timely manner and has provided assistance in the location and coordination of witness interviews.

International exchange of basic and beneficial ownership information of legal persons and arrangements

316. While the authorities recognize the risk of misuse of Canadian legal persons and arrangements, they do not appear to have identified, assessed and understood with sufficient granularity the extent to which Canadian legal persons and legal arrangements are misused for ML or TF in the international context. In addition, there are serious concerns about the timeliness access to relevant information by competent authorities as well as with respect to the

quality of the information collected by REs. As a result, cooperation in relation to foreign requests regarding BO of legal persons and arrangements cannot be fully effective.

317. Canada, and FINTRAC in particular, regularly receives requests for corporate records and information on beneficial ownership of both corporations and trusts (which points to the relevance of Canadian legal entities and trusts in international ML operations). FINTRAC provides the requested information as long as it already has it (i.e. it has received a STR or other report including VIRs regarding the relevant corporation or trust), it can access it (e.g. information from the corporate registries of Alberta and Quebec, or from the MSB registry, when the ownership is 25% or more, or from any other public source). The IAG also receives requests for basic and beneficial ownership information which it forwards to LEAs for execution. Between 2008 and 2015, it received 222 for corporate or business records, including 78 related to ML and 1 to TF investigations. Most of these requests have been executed.

Overall Conclusions on Immediate Outcome 2

318. **Canada has achieved a substantial level of effectiveness for IO.2**.

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations of Canada in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation (R.). It should be read in conjunction with the Detailed Assessment Report (DAR).

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2008. The report for that assessment or evaluation is available from the FATF website.[95]

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

The requirements of R.1 were added to the FATF standard in 2012 and were, therefore, not assessed during the previous mutual evaluation of Canada.

Obligations and Decisions for Countries

Risk Assessment

Criterion 1.1— The Government of Canada has developed a risk assessment framework to support the identification, assessment and mitigation of ML/TF risks and includes a process to update and enhance this assessment over time. ML and TF threats were documented separately. Canada completed its first National Risk Assessment (NRA), the "Assessment of Inherent Money Laundering and Terrorist Financing Risks in Canada," in December 2014. In April 2015, the senior officials of participating federal departments and agencies endorsed the internal and draft public versions of the report. In July 2015, the Minister of Finance, on behalf of the government, released the public version of the NRA.[96] Canada's ML/TF Inherent RA is supported by a documented NRA Methodology with defined concepts on ML/TF risks and rating criteria. The report, which reflects the situation in Canada up to 31 December 2014, provides an overview of the ML/TF threats, vulnerabilities and risks in Canada before the application of mitigation measures.

The NRA consists of an assessment of the inherent (i.e. before the application of any mitigation measures) ML/TF threats and inherent ML/TF vulnerabilities of key economic sectors and financial products, while considering the contextual vulnerabilities of Canada, such as geography, economy, financial system and demographics.

Pursuant to the Interpretative Note to R.1, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from ML and TF, and which do not fall under the definition of financial institution or DNFBP, they should

[95] See FATF (2008), Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, www.fatf-gafi.org/countries/a-c/canada/documents/mutualevaluationofcanada.html
[96] See Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

consider applying AML/CFT requirements to such sectors. In that regard, the 2008 MER discussed whether Canada had considered extending AML requirements to white-label ATMs (see paragraphs 1357 to 1364). In a 2007 FINTRAC report highlighted the vulnerability of white-label ATMs to ML, and various press articles highlight the risk of misuse of white-label ATMs. The authorities are considering mechanisms to address this risk.

Criterion 1.2— The Department of Finance Canada (Finance Canada) is the designated authority for coordinating the work associated with the ongoing assessment of ML/TF risks. In Canada government responsibilities in regard to AML/CFT are divided between the federal government and the ten provinces (the three territorial governments exercise powers delegated by the federal parliament). In that regard, the execution of AML/CFT actions involves collaboration and coordination across all levels of government.

The terms of reference for (i) the Interdepartmental Working Group on Assessing ML and TF Risks in Canada and (ii) the permanent National Risk Assessment Committee (NRAC; the senior-level AML/CFT Committee) establish Finance Canada as the designated authority for the initiative. The Minister of Finance is the Minister responsible for the PCMLTFA. Therefore, as decided by the Cabinet, the responsibility for coordinating the AML/CFT regime and the NRA falls also to Finance Canada.

Criterion 1.3— Canada's risk assessment framework contemplates a process to update and enhance this assessment over time. In accordance with the document "Proposed Governance Framework for Canada's ML/TF Risk Assessment Framework" (endorsed on 13 November 2014), the NRA update is now coordinated through the NRAC, the successor body to the Working Group that developed the NRA. The Terms of Reference of NRAC were approved at the senior-level AML/CFT Committee in April 2015. NRAC is composed of representatives of the federal departments and agencies that comprise Canada's AML/CFT (and may invite other public and private sector partners to participate), which facilitates sharing findings across the organizations represented to help them understand the evolving risks and ML/TF environment, as well as discuss and propose mitigations. Finance Canada is the permanent co-chair of the NRAC; the other co-chair position rotates every two years among other federal departments or agencies. NRAC is required to prepare a formal update every two years on the results of the risk assessment and an informal update on an annual basis. The reports are addressed to the senior level AML/CFT Committee. As Canada completed its NRA in December 2014, it is relatively up to date. Furthermore, the Committee will meet every six months or more frequently if needed, to review emerging threats and new developments and will report to the senior-level Committee on an annual basis with updates.

Criterion 1.4—Information on the results of the NRA is provided to competent authorities, self-regulatory bodies, FIs and DNFBPs through different working groups, committees and outreach activities. The NRA was released publicly on 31 July 2015 (and is available on the websites of Finance, FINTRAC, and OSFI). The NRA methodology and results were also shared and discussed beforehand by Finance

Risk Mitigation

Criterion 1.5— The risk mitigation is implemented through various thematic national strategies, to wit: National Identity Crime Strategy (2011), Canada's Counter-terrorism Strategy (2013); National Border Risk Assessment 2013–2015; 2014–2016 Border Risk Management Plan; Enhanced Risk Assessment Model and Sector profiles; OSFI's AMLC Division AML and CFT Methodologies and Assessment Processes; OSFI-Risk Ranking Criteria; and the CRA's techniques to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals.

Criterion 1.6— Financial activities are subject to AML/CFT preventive measures as required in the FATF Recommendations, except when these activities are conducted by the sectors that are not subject to AML/CFT obligations under the PCMLTFA. These sectors include check-cashing businesses, factoring companies, and leasing companies, finance companies, and unregulated mortgage lenders, among others. The NRA assessed the ML/TF vulnerabilities of factoring, finance and financial leasing companies as medium risk, while pointing out that these entities were very small players as a proportion of Canada's financial sector. However, the ML/TF risks for these sectors has not been proven to be low and the non-application of AML/CFT measures is not based on a risk assessment. .

Except for the legal profession, all DNFBP sectors are required to apply AML/CFT preventive measures. Lawyers are covered as obliged AML/CFT entities, pursuant to PCMLTR, Section (s.) 33.3; however, the AML/CFT provisions are inoperative in relation to lawyers and Quebec notaries (who provide legal advice and are, therefore, considered legal counsel, PCMLTFA s. 2) as a result of a 2015 Supreme Court of Canada ruling.

Supervision and Monitoring of Risk

Criterion 1.7— REs are required to implement enhanced or additional measures in high-risk situations pursuant to PCMLTFA, ss.9.6(2) and 9.6(3) and PCMLTFR, §71(c) and 71.1(a) and (b) (see discussion on R.10 for additional information on enhanced CDD measures). The REs are expected to integrate the NRA results in their own risks assessments.

PCMLTFA, s.9.6(2) provides that REs develop and apply policies and procedures to address ML and TF risks. PCMLTFA, s.9.6(3) and PCMLTFR, s.71.1(a) and (b) require REs to apply "prescribed special measures" to update client identification and beneficial ownership information, and to monitor business relationships when higher risks are identified through the entity's risk assessment.

Nevertheless, the provisions discussed in the paragraphs above do not apply to the sectors that are not subject to reporting obligations under the PCMLTFA. These include sectors such as the legal counsels, legal firms and Quebec notaries, factoring companies, financing and leasing companies, among others. Of these sectors, the legal counsels, legal firms and Quebec notaries are exposed to ample ML opportunities and are exposed to higher risks. Therefore, as the legal profession is not required to take enhanced measures regarding higher ML risks (or any ML risks, for that matter) the risks associated with this sector are not being effectively mitigated.

Exemptions

Criterion 1.8— PCMLTFR ss.9, 62 and 63 provide for exemptions from the customer identification and record-keeping requirements in certain specific circumstances assessed as low risk by the authorities (for details about the exemption regime, see discussion on R.10 below). OSFI and FINTRAC continuously assess the risks associated with their supervised sectors and the current assessment of low risks appear to be consistent with the findings of the NRA.

Criterion 1.9— PCMLTFA, s.40(e) requires FINTRAC to ensure compliance with PCMLTFA provisions. PCMLTFA, s.9.6(1)-(3) requires REs Act to implement measures to assess ML and TF risks, and monitor transactions in respect of the activities that pose high ML/TF risks. OSFI and FINTRAC apply a risk-based approach to the supervision of their supervised sectors. As discussed previously, the legal profession is not subject to AML/CFT obligations and is, therefore, not monitored by FINTRAC. However, some high-risk DNFBPs are not subject to AML/CFT obligations and are thus not supervised in relation to their obligations under R.1.

Obligations and Decisions for Financial Institutions and DNFBPs

Risk Assessment

Criterion 1.10— PCMLTFA, s.9.6(2) and PCMLTFR, §71(c) requires REs to conduct risk assessments and consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied. PCMLTFR, s.71(e) provides that the REs shall keep their risk assessments up to date. All supervised entities and those subject to examination by FINTRAC are obligated under their sector legislation or PCMLTFA, s.62 to provide any material that FINTRAC or sector regulators may require. FINTRAC Guideline 4 (Implementation of a Compliance Regime, February 2014) provides a checklist of products or services that should be considered high-risk. OSFI Guideline B-8 (Deterring and Detecting Money Laundering and Terrorist Financing) provides instruction on the FRFIs risk assessment policies and procedures. As mentioned above, none of the AML/CFT requirements are applicable to lawyers, legal firms, and Quebec notaries.

Risk Mitigation

Criterion 1.11— *a)* Under PCMLTFA s 9.6(1) and PCMLTFR, s.71, REs are required to develop written AML/CFT compliance policies and procedures, which are approved by a senior officer of the RE in accordance with PCMLFTR s.71(1)(b).

b) These policies and procedures, the risk assessment and training program are required to be reviewed at least every two years (PCMLFTR, ss.71(1)(e) and 71(2)). The REs must also assess and document ML and TF risks (PCMLTFA, s.9.6(2) and PCMLFTR, s.71(1)(c)).

c) There are several different provisions that require REs to implement enhanced or additional measures in high-risk situations: Under PCMLTFA, ss.9.6(2) and 9.6(3), REs are required to assess ML and TF risks and enhanced due diligence, record keeping and monitoring of financial transactions that pose a high risk of ML or TF. The PCMLTFR requires REs to apply enhanced measures when high risks are identified in their activities as a result of ongoing monitoring. The

sectors covered by the PCMLTFR are banks and other deposit-taking institutions (s.54.4); life insurance (s.56.4); securities (s.57.3); MSBs (s.59.02); accountants (s.59.12); real estate (s.59.22); British Columbia Notaries (s.59.32); real estate developers (s.59.52), casinos (s.60.2); and Departments and agents of the Queen in rights of Canada or a Province for the sale or redemption of money orders for the general public (s.61.2). The provisions addressing the legal profession are not applicable to legal counsels, legal firms and Quebec notaries for the reasons stated earlier. FINTRAC, Guideline 4 and OSFI Guideline B-8 provide additional guidance.

Criterion 1.12— The Canadian AML/CFT legislation does not provide for simplified measures.

Weighting and Conclusion:

The main inherent ML and TF risks were identified and assessed for the implementation of appropriate mitigation.

Canada is largely compliant with R.1.

Recommendation 2 - National Cooperation and Coordination

Canada was rated LC in the 2008 MER with former FATF R.31; the cooperation between the FIU and LEAs was not considered to be fully effective.

Criterion 2.1— Several national strategies and policies are in place to inform AML/CFT policies and operations. The main AML policies and strategies are the *National Identity Crime Strategy* (RCMP 2011); *National Border Risk Assessment 2013–2015* (CBSA); *2014–16 Border Risk Management Plan* (CBSA); *Enhanced Risk Assessment Model and Sector profiles* (FINTRAC); *AMLC Division AML and CFT Methodology and Assessment Processes* (OSFI); *Risk Ranking Criteria* (OSFI); *Risk-Based Approach to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals* (CRA) and CRA-RAD Audit Selection process. The RCMP is currently developing their National Strategy to Combat Money Laundering. These AML strategies and policies are linked to the 2011 *Canadian Law Enforcement Strategy on Organized Crime*. In addition, the Government's other main AML/CFT concerns are reflected in Finance Canada's Report on Plans and Priorities,[97] which outlines the AML/CFT regime's spending plans, priorities and expected results. Canada's CFT strategy forms part of the broader Counter-terrorism Strategy.[98] Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological and nuclear weapons.[99]

The TRWG is an interdepartmental body that serves as a forum to enhance dialogue, coordination, analysis and collaboration, among PS Portfolio members and government departments with an intelligence mandate, on issues related to threat resourcing, including ML, TF and proliferation

[97] Department of Finance Canada (2015), Report on Plans and Priorities 2015–16, p. 29, www.fin.gc.ca/pub/rpp/2015-2016/index-eng.asp
[98] Public Safety Canada (2013), Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx
[99] Public Safety and Emergency Preparedness Canada (2005), The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg-rchvd/index-en.aspx

activities, organized crime and other means through which threat actors resource their activities. It also highlights the security and intelligence components of files associated with Canada's AML/ATF Regime.

Criterion 2.2— Finance Canada is the domestic and International policy lead for the whole AML/CFT regime, and is responsible for its overall coordination, including AML/CFT policy development and guiding and informing strategic operationalization of the NRA framework.

Criterion 2.3— The Canadian regime is also supported by various interdepartmental formal and informal working-level bilateral and multilateral working groups and committees, depending on the nature of the issues to be addressed including: NRAC; NCC; IPOC ; IFAC; TRWG, and the ICC.

To combat ML, Canada also coordinates domestic policy on the federal criminal forfeiture regime under the IPOC. IPOC's interdepartmental Director General-level Senior Governance Committee led by Public Safety Canada includes: CBSA, CRA, PPSC, PS, PWGSC and the RCMP. The Committee is mandated to provide policy direction, promote interdepartmental policy coordination, promote accountability, and to support the Initiative.

The NCC is the primary forum that reviews progress of the National Agenda to Combat Organized Crime. NCC's 5 Regional Coordinating Committees communicate operational and enforcement needs and concerns to the NCC, acting as a bridge between enforcement agencies and officials and public policy makers. Canada coordinates domestic AML policy on the federal criminal forfeiture regime under the IPOC Advisory Committee and the IPOC Senior Governance Committee.

The IFAC is an interdepartmental consultative body that has the responsibility for the sharing, analysis and monitoring of information related to ML/TF threats posed to Canada by foreign jurisdictions or entities. The ICC assists the Minister of Public Safety and Emergency Preparedness by providing the requisite analysis and considerations to inform the recommendations to the Governor in Council regarding listing of entities.

OSFI and FINTRAC coordinate their activities through a common approach for supervision of FRFIs, starting in 2013, by conducting simultaneous AML/CFT examinations. FINTRAC informs its compliance enforcement strategies with findings provided by other federal and provincial regulators in order to monitor and enforce AML/CFT compliance by REs. FINTRAC has established 17 Memoranda of Understanding (MOU) with federal and provincial regulators for the purpose of sharing information related to compliance with Part 1 of the PCMLTFA. The RCMP leads the Integrated National Security Enforcement Teams (INSETs) in major centers throughout the country). INSETs are made up of representatives of the RCMP, federal partners and agencies such as CBSA, CSIS, and provincial and municipal police services.

Criterion 2.4— Counter-proliferation (CP) efforts, including proliferation financing, are coordinated via a formalized CP Framework created in 2013. PS chairs the Counter-Proliferation Policy Committee, at which CP partners identify, assess and address policy and programming gaps that may undermine Canada's CP capacity. Global Affairs Canada chairs the Counter-Proliferation Operations Committee, through which CP partners work together to address specific proliferation threats with a

Canadian nexus. FINTRAC is a member of the Operations Committee, and as per PCMLTFA s.55.1(1)(a), is able to disclose designated financial information to the Canadian Security Intelligence Service (CSIS) when it has reasons to suspect that it would be relevant to investigations of threats to the security of Canada, which includes proliferation activities. FINTRAC can also disclose information on threats related to proliferation to the appropriate police force and the CBSA if separate statutory thresholds are met.

Weighting and Conclusion:

Canada has a number of standing committees, task forces and other mechanisms in place to coordinate domestically on AML/CTF policies and operational activities.

Canada is compliant with R.2.

Recommendation 3 - Money laundering offense

Canada was rated LC with former R.1 and 2 based on a number of shortcomings. The range of predicate offenses was slightly too narrow and for one part of the ML offense the *mens rea* requirement was not in line with the FATF standard. Since 2008, the range of predicate offenses for ML was expanded to include tax evasion, tax fraud, and copyright offenses.

***Criterion* 3.1**— ML activities are criminalized through Criminal Code (CC), ss.354 (possession of proceeds), 355.2 (trafficking in proceeds), and 462.31 (laundering proceeds). *Conversion or Transfer:* CC, s.462.31 criminalizes the use, transfer, sending or delivery, transportation, transmission, altering, disposal of or otherwise dealing with property with the intent to conceal or convert the proceeds and knowing or believing that all or part of that property or proceeds was obtained or derived directly or indirectly as a result of a predicate offense. S.462.31 falls somewhat short of the FATF standard due mainly because the perpetrator must intend to conceal or convert the property itself rather than the illicit origin thereof. Additionally, no alternative purpose element of "helping any person who is involved in the commission of a predicate offense to evade the legal consequences of his or her action" is provided for. S.355.2 criminalizes many of the same acts as s.462.31 but without setting out any specific intent requirement. However, the Supreme Court in *Canada in R. v. Daoust, 2004, 1 SCR 217, 2004 SCC 6 (CanLII)* held that "the intention of parliament was to forbid the conversion pure and simple, of property the perpetrator knows or believes is proceeds of crime, whether or not he tries to conceal it or profit from it." *Acquisition, possession or use:* Ss.354 and 355.2. criminalize the sole or joint possession of or control over (s.354) and the selling, giving, transferring, transporting, exporting or importing, sending, delivering or dealing with in any way (s.355.2) of property or things that the person knows were obtained or derived directly or indirectly from an indictable offense. Neither provision explicitly refers to the "acquisition or use," but such acts would be covered by "control over proceeds" in s.354 and the various material elements under s.355.2. *Concealment or disguise:* Under CC, s.354 it is an offense to conceal or disguise property that the perpetrator has possession of or control over, in which case liability is invoked for "possession and trafficking of proceeds." Additionally, the concealment or disguise is covered under s.355.2 and liability is for "trafficking in proceeds."

Criterion 3.2— Ss.354 and 355.2 cover acts relating to proceeds of an "indictable offense;" and s 462.31 to proceeds of a "designated offense." "Designated offense" is defined as "any offense that may be prosecuted as an indictable offense other than those prescribed by regulation". Canada's ML provisions apply to all serious offenses under Canadian law and cover a range of offenses in each FATF designated categories of predicate offenses, including tax evasion.

Criterion 3.3— All serious offenses under Canadian law, defined as offenses with a statutory sanction of imprisonment for more than six months, constitute a predicate offense for ML. As indicated in the 2008 MER, federal laws criminalize a range of serious offenses under each FATF designated categories of predicate offenses.

Criterion 3.4— Ss.354, 355.2, and 462.31 apply to any property or proceeds of property obtained or derived, directly or indirectly, from the commission of an indictable offense. No value threshold applies. "Property" is defined under s.2 of the CC to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, including converted or exchanged property. The definition covers material and immaterial, tangible and intangible, and corporeal and incorporeal property as well as interest in such property.

Criterion 3.5— The legal provisions do not require a conviction for a predicate offense to establish the illicit source of property. Case law further confirmed this principle. [100]

Criterion 3.6— The text of ss.354, 355.2 and 462.31 apply the relevant offenses to indictable offenses committed in Canada and to any act or omission committed abroad that would have constituted an indictable offense had it occurred in Canada.

Criterion 3.7— Nothing in the relevant provisions prevent their application to the person who committed the predicate offense. Canadian case law supports the notion that the ML provisions can also be applied to the person who committed the predicate offense.[101]

Criterion 3.8— As a general rule, Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[102]

Criterion 3.9— Offenses pursuant to s.354 are punishable with imprisonment for up to ten years (if the value of the property exceeds CAD 5 000) or for up to two years (if the value of the property is less than CAD 5 000). S.355.5 applies the same value thresholds but set out slightly stricter sanctions of imprisonment for up to 14 years or up to five years, respectively. S.462.31 provides for a statutory

[100] United States of America and the honorable Allan Honourable Allan Rock, Minister of Justice for Canada v. Dynar, 1997, 2 SCR 462, 1997, CanLII 359 (SCC); R.c.Chun, 2015 QCCQ 2029 (CanLII); and R.c. Lavoie, 1999 CanLII 6126 (QCCQ).

[101] R. v. Tortine, 1998, 2 SCR 972, 1993 CanLII 57 (SCC); and R. v. Trac at R. v. Trac, 2013 ONCA 246 (CanLII).

[102] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

sanction of imprisonment for up to ten years, regardless of the amounts involved. The statutory sanctions may be increased or reduced pursuant to CC, s.718.2 based on aggravating or mitigating circumstances. CC, s.718.1 requires that the sanction in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 3.10— Legal entities may be subject to criminal liability and be held criminally responsible for ML. Pursuant to CC, s.735 (1) a legal entity, partnership, trade union, municipality or association convicted of an indictable offense is liable to a fine with the relevant amount being determined by the court. In determining the relevant sanction, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account. CC, s.718.1 requires that a sentence must in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. Given the wide discretion the court has in determining the sanction, the statutory sanctions are considered to be dissuasive and proportionate. Parallel civil or administrative sanctions may be applied in addition to the criminal process.

Criterion 3.11— Ancillary offenses are criminalized in the general provisions of the CC (s.24— Attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22— counselling, procuring, soliciting or inciting to commit; s.23—accessory after the fact).

Weighting and Conclusion:

Canada is compliant with R.3.

Recommendation 4 - Confiscation and provisional measures

Canada was rated LC with former R.3.

Criterion 4.1— CC, s.462.37 (1) provides for the permanent forfeiture of proceeds of crime based on a conviction for a designated offense. CC, s.490.1 (for all crimes) and Controlled Drugs and Substances Act (CDSA), ss.16 and 17 set out similar forfeiture provisions in relation to property used or intended to be used for the commission of an indictable offense. In all cases, the court will consider forfeiture based on the application by the Attorney General. In the context of convictions for participation in a criminal organization or offenses under the CDSA, extended forfeiture orders may be granted for material benefits received within 10 years before commencement of the proceedings and income from sources that cannot be reasonably accounted for. In a standalone ML case, CC, s.462.37(1) allows for the confiscation of the proceeds of the laundering activity as well as the property laundered, although for the latter a stricter standard of proof would apply. CC, ss.462.37 (1) and 490.1 allow for forfeiture of property from a third party. In cases where the accused has died or absconded, forfeiture *in rem* is available under ss.462.38 and 490.2.

Equivalent value confiscation is not permitted. CC, s.462.37(3) provides for the issuance of a fine in lieu of forfeiture in cases where the court determined that a forfeiture order under CC, s.462.37 cannot be made in respect of any property. While the issuance of a fine may result in the same outcome as an equivalent value confiscation, from a legal point of view the concept of a fine cannot substitute equivalent value confiscation.

Criterion 4.2— The CC and CDSA set out a wide range of measures including search and seize warrants pursuant to CC, ss.487, 462.32 and 462.35 and CDSA, s.11; production orders pursuant to CC, s.487.018 regarding the existence of bank accounts; production orders pursuant to CC, ss.487.014 and 487.015; warrants for transmission of data including computer and telecommunication program recordings under CC, s.492.2; general information warrants under CC, s.487.01 and tax information orders under CC, s.462.48. The power under CC, s.487.01 to "use any device, investigation technique or procedure or do anything described in the warrant" is sufficiently broad to also cover account monitoring, In addition, PCMLTFA, s.23 allows for the seizure and forfeiture of cash or bearer-negotiable instruments for violations of the cross border declaration obligation. Seizing and restraint warrants to secure property or instrumentalities for forfeiture are available under CC, ss.462.33 and 490.8 and CDSA, s.14. Seizing and restraint orders may be issued based on reasonable grounds to believe that a forfeiture order will be made in regards to the relevant property. In both cases, the judge may opt to apply provisional measures ex parte and without prior notice. CC, ss.490.3 and 462.4 permit the judge to void any conveyances of transfers unless the transfer was for valuable consideration to a bona fide third party. Prior to the issuance of a seizing or restraint order, the holder of such property may become subject to criminal liability under CC, s.354(1) provided he acted knowingly. A specific forfeiture provision for property owned or controlled by a terrorist group or property that has been or will be used to carry out a terrorist activity is set out in CC, s.83.14.

Criterion 4.3— Rights of bona fide third parties are protected through CC, ss.462.42, 462.34 (b), 490.4 (3) and 490.5 (4), which allow for exclusion of certain property from a restraining, seizing, or forfeiture order.

Criterion 4.4— The Seized Property Management Act regulates the management of seized or restrained property and the disposal and sharing of forfeited property. Under the Act, the Minister of Public Works and Government Service is competent to take into custody all such property and may take any measures he deems appropriate for the effective management thereof. Forfeited property is to be disposed of and the proceeds to be paid into the Seized Property Proceeds Account. Fines paid in lieu of forfeited property and amounts received from foreign governments under asset-sharing agreements are to be credited to the Proceeds Account as well. Excessive amounts in the Account are to be credited to accounts of Canada as prescribed by the Governor in Council.

Weighting and Conclusion:

The confiscation framework has some shortcomings.

Canada is largely compliant with R.4.

Recommendation 5 - Terrorist financing offence

Canada was rated LC with former SR. II.

Criterion 5.1— TF is criminalized through CC, ss.83.02 to 83.04: S. 83.02 criminalizes the direct or indirect, wilful and unlawful collection or provision of property with the intent that the property is to be used or knowing that the property will be used to carry out a terrorist activity. CC, s.83.04 criminalizes the use of property for the purpose of facilitating or carrying out a terrorist activity, and the possession of property intending that it be used or knowing that it will be used to facilitate or carry out a terrorist activity. CC, s.83.01 defines "terrorist activity" to cover all acts which (1) constitute an offense as defined in one of the conventions and protocols listed in the Annex to the TF Convention, all of which are criminalized in Canada; and (2) any other act or omission carried out with terrorist intent.

Criterion 5.2— CC, s.83.03(a) criminalizes the direct or indirect collection or provision of property with the intent that such property is to be used or knowing that such property will be used to benefit any person who is facilitating or carrying out a terrorist activity. The offense applies also where the property is used by the financed person for a legitimate purpose. CC s.83.03(b) covers the direct or indirect collection or provision of property, knowing that such property, in whole or in part, will benefit a terrorist group. "Terrorist group" includes a person, group, trust, partnership, or fund or unincorporated associations or organizations that has as one of its purposes or activities the facilitating or carrying out of any terrorist activity. The mental element required under subsection (b) is slightly stricter than under subsection (a) as the offense only applies where the perpetrator knows that property will be used for the benefit of a terrorist group, but not where he merely intends for this to be the case. For both CC, ss. 83.03 (a) and (b) the courts have interpreted the term "facilitates" broadly to cover "any behaviour/activity taken to make it easier for another to commit a crime."[103] The term thus includes the "organizing or directing of others" to commit a terrorist activity, or the "contributing to the commission of a terrorist activity by a group of persons acting with a common purpose."

Criterion 5.3— "Property" is defined under CC, s.2 to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property or giving a right to recover or receive money or goods, including converted or exchanged property. CC, ss.83.01 to 83.03 are not limited in scope to financing activities involving illicit property. The source of the property used for the financing activity is irrelevant.

Criterion 5.4— CC, s.83.02 implies that the financing offense can also be applied in cases where a person collects or provides property merely with the intention to finance a specific terrorist activity. Thus, it is neither required that the financed activity has been attempted or committed, nor that the money collected or provided is linked to a specific terrorist activity. CC, s.83.03(b) extends to the collection or provision of funds for the benefit of a terrorist group, regardless of the purpose for which the funds are eventually used, but does not cover financing merely with the intent to benefit

[103] R. v. Nuttall, 2015 BCSC 943 CanLII.

an individual terrorist or terrorist organization. For financing of individual terrorists, CC, s.83.03(a) applies where the financed person is facilitating or carrying out a terrorist activity at the time the financing activity takes place and CC, s.83.03(b) covers situations where the property collected or provided is known to be used by or benefit a terrorist.

Criterion 5.5— Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[104]

Criterion 5.6— The statutory sanctions for a natural person is imprisonment for up to ten years with the possibility of an increased or reduced sentence pursuant to CC, ss.718.2 and 718.21 based on aggravating or mitigating circumstances. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 5.7— Legal entities may be held criminally responsible for terrorism financing. Pursuant to CC, s.735 (1) of the CC, a legal entity, partnership, trade union, municipality, or association may fine in an amount that is in the direction of the court. CC, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account by the court. CC, s.718.1. CC further requires that the sentence be proportionate to the gravity of the offense and the degree of responsibility of the offender. Given the wide discretion by court in determining the sanction, the statutory sanctions are dissuasive and proportionate. Parallel civil or administrative sanctions may be applied.

Criterion 5.8— Ancillary offenses are criminalized in the general provisions of the CC (s.24—Attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22—counselling, procuring, soliciting or inciting to commit; s.23—accessory after the fact). s.83.03 criminalizes inviting another person to provide or make available property for TF and ss.83.21 and 83.22 to knowingly instruct, directly or indirectly, any person to carry out an activity for the benefit of, at the direction of or in association with a terrorist group for the purpose of enhancing the ability of that group to facilitate or carry out a terrorist activity.

Criterion 5.9— Canada takes an all crimes approach to defining predicate offenses for ML. TF is, thus, a predicate offense for ML.

[104] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para. 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

Criterion 5.10— CC, ss.83.02 and 83.03 apply regardless of whether the underlying terrorist activity is committed inside or outside Canada, or whether the terrorist group or financed person is located inside or outside Canada.

Weighting and Conclusion

TF is set out as a separate criminal offense that covers all aspects of the offense set out in the Terrorism Financing Convention, with minor shortcomings.

Canada is largely compliant with R.5.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Canada was rated LC with former SR. III. For certain FIs and other persons or entities that may hold targeted funds the assessors found that the names of designated persons and entities were not effectively communicated, the guidance issued was not sufficient and the implementation of the relevant legal provisions was not effectively monitored. The framework for the implementation of the TF-related targeted financial sanctions remains substantially unchanged. A new Security of Canada Information Sharing Act was adopted in 2015 to facilitate the sharing of information between Canadian government agencies with regards to any activity that undermines the security of Canada, including terrorism.

Identifying and Designating

Under United Nations Act, s.2, the Governor in Council may issue regulations to give effect to decisions and implement measures decided by the UNSC pursuant to Article 41, Chapter VII of the UN Charter. Two Regulations were issued on this basis—the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR) and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST). In 2001, Canada enacted an additional domestic terrorist listing procedure under CC, ss.83.05 to 83.12 in addition to the RIUNRST. Over time, the listing mechanism under the CC has become the primary domestic listing regime and consequently no listings have been added to the RIUNRST since 2006. The Security of Canada Information Sharing Act facilitates implementation of the mechanisms by allowing for the exchange of information between government agencies with regards to terrorism, either spontaneously or upon request.

Criterion 6.1— *Sub-criterion 6.1a*—Department of Foreign Affairs, Trade and Development Act, s.10(2)(b) assigns responsibility to the Minister of Foreign Affairs for all communications between Canada and international organizations, including for proposing designations under UNSCR 1267/1989 or 1988 to the relevant UN Sanctions Committees.

Sub-criterion 6.1b—Based on the above mentioned s.10(2)(b), the Minister of Foreign Affairs identifies, reviews and proposes individuals or entities for designation, in consultation with an interdepartmental committee of security and intelligence officials. The interdepartmental committee on average meets once a month to discuss all listing regimes.

Sub-criterion 6.1c—The authorities stated that the identification process outlined above is based on a standard of "reasonable grounds to believe" and that a criminal conviction was not necessary for proposing the designation of an entity or individual to the UN. In the absence of any written procedures on this point, the assessors were not in a position to verify the authorities' view.

Sub-criterion 6.1d—Canada supports co-designation and co-sponsorship and its experience in proposing designations was so far limited to cosponsoring proposals for designations. To propose designations, Canada would use the UN standard forms and follow the procedures outlined under UNSCR's 2160 and 2161 (2014) and the relevant Sanctions Committee Guidelines.

Sub-criterion 6.1e—The authorities stated that Canada would provide as much relevant information to support a proposal for designation as possible, including identifying information and a statement of case.

Criterion 6.2— *Sub-criterion 6.2a*—Canada implements UNSCR 1373 through two distinct mechanisms: (i) for terrorist groups, CC, s.83.05 grants the Governor in Council the authority to list, on the basis of a recommendation by the Ministry of Public Safety Canada, a person, group, trust, partnership or fund or unincorporated association or organization. Requests for designation from another country can also be considered under the CC process; (ii) the RIUNRST designates the Governor in Council as responsible for making designations on the basis of a recommendation by the Minister of Foreign Affairs (Article 2 RIUNRST). The Minister may recommend a designation under the RIUNRST also based on a request from another country. In practice the mechanisms under the CC is the main one and no listings have been added to the RIUNRST since 2006.

Sub-criterion 6.2b—The CC and RIUNRST include mechanisms for identifying targets for designation and to decide upon designations based on clearly stipulated criteria in line with the designation criteria under UNSCR 1373.

Sub-criterion 6.2c—Foreign requests for designations are processed the same way as domestic designations. As a first step, authorities ensure that a request for listing is supported by verified facts that meet the legal threshold. Verification includes both factual and legal scrutiny. After verification is completed, the proposed listing is presented to the Cabinet and the relevant Minister recommends to the Governor in Council that the foreign request be granted. Authorities stated that the process takes on average six months but can be expedited, if necessary.

Sub-criterion 6.2d—The Governor in Council takes the decision to designate based on "reasonable grounds to believe" that a person meets the designation criteria in CC or the RIUNRST, independently from any criminal proceedings.

Sub-criterion 6.2e—The authorities stated that when making 1373 request to other countries, as much identifying information as possible would be provided to the requesting country to allow for a determination that the reasonable basis test is met Canada stated that it is in regular contact with its allies to discuss potential listings and notifies G7 partners prior to any domestic listing.

Criterion 6.3— The Canadian Security Intelligence Service Act s. 12 grants the CSIS the power to collect and analyse information on activities that may threaten Canada's security and to report and advise the government of any such activities. The Security of Canada Information Sharing Act, s.5 further allows government agencies to share such information. In the context of a criminal suspicion or the designation procedure under CC, s.83.05 the authorities may also collect information under criminal procedures. The outlined measures may in all cases be applied *ex parte* to avoid tipping off.

Freezing

Criterion 6.4— The UNAQTR, CC and RIUNRST set out a wide range of prohibitions to deal with property of or provide financial services to designated persons. The prohibitions apply as soon as any person is designated by the competent UN Sanctions Committee (for UNSCR 1267/1989 or 1988) or is added to the Regulations Establishing a List of Entities pursuant to the CC or is included in Schedule 2 to the RIUNRST (for UNSCR 1373). The prohibitions apply without delays, as soon as a person has been designated by the UN (for UNSCR 1267 and 1988) or was added to the domestic list. The term "person" covers both natural and legal persons.

Criterion 6.5— No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC, and RIUNRST. Sanctions for violations of the Regulations are available but have never been applied in practice.

Sub-criterion 6.5a—The UNAQTR, CC and RIUNRST prohibit that any person or entity in Canada or any Canadian outside Canada knowingly deals with; provides financial or other services to; or enters into or facilitates any financial transaction involving funds or property of a designated person. The prohibition applies as soon as a person is listed and covers all aspects of the freezing obligation, thus also without prior notice.

Sub-criterion 6.5b—The UNAQTR, RIUNRST, and CC target funds or property owned or controlled, directly or indirectly, by any designated person or by any person acting on behalf or at the direction of a designated person. In the case of the UNAQTR but not the CC, does the prohibition extend also to funds derived or generated from such property. The concepts of "ownership and control" also cover property owned and controlled jointly. The obligations under all three procedures apply to property of every kind, including any funds, financial assets or economic resources.

Sub-criterion 6.5c—The UNAQTR, the CC, and RIUNRST prohibit Canadians and any persons in Canada from making property or financial or other services available, directly or indirectly, for the benefit of a designated person (Articles 4 RIUNRST; CC, ss.83.08 and UNAQTR s.4 and 4.1. CC, s.83.03 further criminalizes the provision of property or services to a listed entity, but the prohibition does not extend the provision of services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person.

Sub-criterion 6.5.d—Canada makes public all designations under all three listing regimes on government websites and through notification services. FRFIs have the option of signing up to receive information notices regarding list changes from OSFI and/or directly from the 1267 Al-Qaida

Sanctions Committee and the 1988 Taliban Sanctions Committee. OSFI receives a note verbale from the 1267 Al-Qaida Sanctions Committee and the 1988 Taliban Sanctions Committee in advance of a formal press release (i.e. before the Committees lists the entities publically). OSFI sends out email alerts to those entities that subscribe to its email notifications of any changes to the lists the same day or subsequent day from receiving the note verbale. However, if there are extensive changes to the lists, this process can be delayed by two weeks. The UN 1267 Al-Qaida Committee and 1988 Taliban Sanctions Committee also notify all email subscribers, which can include FIs or any persons, of new listings and de-listings the same day or the next UN business day. REs are informed without delay of any entities listed under the CC and RIUNRST. When an entity becomes listed pursuant to the CC, a notice is published in the *Canada Gazette*, which constitutes official public notice of the listing. These changes are also included in OSFI's email notifications. Public Safety also issues a news release for all new listings and de-listings, and both Public Safety and OSFI include information on its websites.

Sub-criterion 6.5.e—Banks, cooperative credit societies, savings and credit unions, and insurance companies are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must regularly report this and any associated information to the competent supervisory authority (OSFI or FINTRAC depending on whether it is a FRFI or not). A more general obligation applies to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 6.5.f—The CC and the RIUNRST both prohibit persons from "knowingly" dealing with listed entities. Third parties acting in good faith are thus protected in that they would not be covered under these obligations. The CC further clarifies that any person who "acts reasonably in taking, or omitting to take, measures to comply" with the relevant obligations shall not be liable in any civil action if they took all reasonable steps to satisfy themselves that the relevant property was owned or controlled by or on behalf of a terrorist group. The procedures under the UNAQTR, the RIUNRST and the CC for delisting and access to frozen funds also apply to protect bona fide third parties.

De-Listing, Unfreezing and Providing Access to Frozen Funds or other Assets

Criterion 6.6— The UNAQTR, CC and RIUNRST set out mechanisms for the delisting of persons or entities that do not meet the designation criteria (respectively in UNAQTR, ss.5.3. and 5.4.; CC, ss.83.05(5) and 2.1., and RIUNRST, s.2.2). Both Regulations and the CC are published in the official Gazette and the relevant procedures are thus "publicly known." CC, s.85.05(9) requires the Minister of Public Safety and Emergency Preparedness to review the list of entities every two years to determine whether there are still reasonable grounds for the entities to remain listed. The Minister can recommend to the Governor in Council at any time that an entity be delisted, either as part of the review process or upon application by the listed entity. Information on delisting processes is also set out at www.international.gc.ca/sanctions/countries-pays/terrorists-terroristes.aspx?lang=eng.

Sub-criterion 6.6.a—Under the UNAQTR, the Minister based on written receipt of a motion to delist under s 5.3 decides whether to forward a petition for delisting to the UN. The Minister's submission must be in accordance with guidance issued by the relevant UN Sanctions Committee. The possibility

of a judicial review of the Minister's decision is provided for under s.5.4. Procedures to unfreeze funds of de-listed entities are not available but the obligations under the UNAQTR automatically cease to apply once a person is removed from the UN's list.

Sub-criterion 6.6.b—The delisting procedures under the CC and RIUNRST are similar to those under the UNAQTR insofar as a listed entity may apply in writing to the relevant Minister to request to be removed from the list. Upon receipt of a written application for delisting from the relevant Minister, it has 60 days to determine whether there are reasonable grounds to recommend a delisting to the Governor in Council. The applicant can seek a judicial review of this decision.

Sub-criterion 6.6.c—Judicial review of the listing decision is available upon receipt of a motion to delist.

Sub-criterion 6.6d and 6.6e—UNAQTR, s.5.3 provides Canadians and any residents of Canada the option to apply to the Minister to be delisted from the 1988 or 1267 sanctions lists in accordance with the Guidelines of the 1988 and 1267 Sanctions Committees.

Sub-criterion *6.6f*—Pursuant to UNAQTR, s.10 and RIUNRST, s.10 a person claiming not to be a listed entity may apply to the Minister of Foreign Affairs for a certificate stating that the person is not a listed entity. The Minister then has a specific period of time to issue the certificate if it is established that the individual is not a listed entity. CC, s.83.07 allows an entity claiming not to be a listed entity to apply to the Minister of Public Safety and Emergency Preparedness for a certificate stating that it is not a listed entity.

Sub-criterion 6.6.g—Any changes to designations under the UNAQTR, CC or RIUNRST result in the publication of an updated Schedule to the relevant Regulation. For changes to the 1267/1988 lists, FIs and DNFBPs can subscribe to an automatic notification system. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes.

Criterion 6.7— The Minister of Foreign Affairs or the Minister of Public Safety and Emergency Preparedness (for the CC) may grant a person access to frozen funds to cover basic or extraordinary expenses pursuant to UNAQTR, s.10.1, CC, s.83.09 or RIUNRST, s.5.7. Under the UNAQTR, the Minister must notify (for basic expenses) or obtain authorization from (for extraordinary expenses) the relevant UN Sanctions Committee before he/she may grant a motion for access to frozen funds. Once granted, the Minister issues a certification exempting the relevant property or funds from the scope of the Regulations. Under UNAQTR the procedures applied by the Minister have to be in line with the requirements under UNSCR 1452 (2002).

Weighting and Conclusion

There are some shortcomings in regard to the requirements of UN Resolutions 1267, 1988, and 1373.

Canada is largely compliant with R.6.

Recommendation 7 – Targeted financial sanctions related to proliferation

R.7 includes new requirements that were not part of the previous assessment.

Criterion 7.1— Two regulations implementing targeted financial sanctions (TFS) relating to Iran and North Korea were issued under Canada's *United Nations Act*—the *Regulations Implementing the United Nations Resolutions on Iran (RIUNRI)* and the *Regulations Implementing United Nations Resolutions on the Democratic People's Republic of Korea (RIUNRDPRK)*. Both require any person in Canada and any Canadian outside Canada to implement TFS in relation to individuals or companies that have been designated by the UN under paragraph 8(d) of UNSCR 1718 (ss.7, 8, and 9 RIUNRDPRK for North Korea) or paragraphs 10 or 12 of UNSCR 1737 (ss.5, 6, 9 and 9.1 RIUNRI for Iran). Under both regulations, it is clear that the relevant prohibition applies only from the date the relevant UNSCR came into force and not retroactively. Neither regulation specifies that sanctions must be applied "without delay" but the relevant obligations and prohibitions apply as soon as a person or entity is included in the UN's list of designated persons, and the communication procedures described under criterion 7.2(d) are sufficient that new listings are brought to the attention of the public. The Security of Canada Information Sharing Act facilitates the implementation of the two regulations by allowing for the exchange of information between government agencies with regards to proliferation of nuclear, chemical, radiological, or biological weapons, either spontaneously or upon request.

Criterion 7.2— Under UN Act, s.2 the Governor in Council issues regulations to give effect to decisions and implement measures decided by the UN Security Council (UNSC) pursuant to Article 41, Chapter VII of the UN Charter. Section 9 of the RIUNRDPRK and RIUNRI impose freezing obligations by prohibiting any person in Canada and any Canadian outside Canada from dealing with; or entering into or facilitating any financial transaction relating to; or providing financial or other related services in relation to property owned or controlled directly or indirectly by a designated person or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2.a—The legal prohibitions are triggered without delay as soon as a person is designated by the UN.

Sub-criterion 7.2b—The above-mentioned prohibitions apply to property owned or controlled by a designated person, including those owned or controlled jointly, or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2c—Under both regulations it is an offense to make property or any financial or other related services available, directly or indirectly, for the benefit of a designated person. Article 3 of the UN Act prescribes sanctions of a fine of up to CAD 100 000 or imprisonment for not more than two years or both (upon summary conviction); or to imprisonment for a term of not more than 10 years (upon conviction on indictment).

Sub-criterion 7.2d—The communication procedures described in criterion 6.5d are also applicable in the context of the RIUNRI and RIUNRDPRK. Canada publishes new designations in the public Canada

Gazette as well as on government websites and through notification services. The Ministry of Foreign Affairs has issued guidance for both sanction regimes.[105]

Sub-criterion 7.2e—All FRFIs and casualty insurance companies, savings and credit unions, and other provincially regulated FIs are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must freeze such property and regularly report this and any associated information to the competent supervisory authority (ss.11 RIUNRI and RIUNRDPRK). More general obligations apply to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 7.2f—The RIUNRI and RIUNRDPRK prohibitions apply only in cases where a person acts "knowingly." Bona fide third parties acting in good faith are, therefore, protected.

Criterion 7.3— Apart from the notification system outlined, under criterion 7.2.e, Canada does not have a mechanism in place for monitoring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. Sanctions for violations of the Regulations are available, but have never been applied in practice.

Criterion 7.4— Global Affairs Canada provides guidance on its homepage on the procedures and content of the RIUNRI and RIUNRDPRK.[106] While the homepage provides information that needs to be submitted as part of an application to the Minister for delisting, it does not give information on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.

Sub-criterion 7.4.a—Neither the Regulations nor the Global Affairs' homepage provide information on the availability of the UN Focal Point as a direct or indirect way to effect a delisting.

Sub-criterion 7.4.b—Claims of false positives can be filed with and granted by the Minister under RIUNRDPRK, s.14 and RIUNRI, s.16. *Sub-criterion 7.4.c*—RIUNRDPRK, s.15 and RIUNRI, s.17 further provide for the possibility for the Minister to grant access to frozen funds subject to the conditions and procedures set out in UNSCR 1718 and 1737.

Sub-criterion 7.4.d—FIs and DNFBPs can subscribe to the UNs automatic notification system found on its website. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes. Detailed guidance on the provisions of the RIUNRI and RIUNRDPRK is provided on the Global Affairs' homepage.

Criterion 7.5— Neither Regulation allows for additions to frozen accounts but the Minister may permit such additions on the basis of a one-off exemption. Payments from frozen accounts are

[105] Global Affairs Canada (nd), Canadian Sanctions Related to Iran, www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; Canadian Sanctions Related to North Korea, www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.
[106] See footnote 16.

permitted under the circumstances set out in relevant UNSCRs based on RIUNRI, s.19 and RIUNDPRK, s.15.

Weighting and Conclusion

There are minor shortcomings in regard to the implementation of the RIUNRI and RIUNRDPRK.

Canada is largely compliant with R.7.

Recommendation 8 – Non-profit organisations

Canada was rated LC with former SR. VIII, with only one deficiency having been identified regarding coordination amongst competent domestic authorities.

Criterion 8.1— *Sub-criterion 8.1.a*—The adequacy of laws and regulations relating to NPOs is reviewed on an ongoing basis and has recently resulted in amendments of various laws and regulations.

Sub-criterion 8.1.b—Canada has carried out a risk assessment of its NPO sector and determined that registered charities pose the greatest risk of TF in Canada and, thus, shall fall within the functional definition of "non-profit organization" as defined under the FATF standard. Canada's risk mitigation efforts are primarily focused on registered charities.

The NRA, which focuses on inherent risk, indicates that both for domestically and internationally operating charities, it may be difficult in practice to determine the origin or ultimate use of funds. In addition to the NRA, the CRA in 2015 conducted a comprehensive review of the entire NPO sector. Other relevant studies and reviews include the Canadian Non-Profit and Voluntary Sector in Comparative Perspective in March 2005; the Canada Survey on Giving, Volunteering and Participating in 2010; and the CRA's Non-Profit Organization Risk Identification Project, all of which provide insight into the way NPOs are organized and operate in Canada. All registered charities, regardless of the value of their assets, as well as non-charitable NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000, must file an annual Information Return with the CRA, which includes information about their activities, assets and liabilities, and the amount of money received during the fiscal period in question. Incorporated NPOs are subject to additional filing obligations pursuant to the relevant statutes. NPOs must indicate whether they carry out activities outside of Canada (and specify where) and disclose the physical location of their books and records. Through information provided in these returns, the CRA has the capacity to obtain timely information on the activities, size and relevant features of the NPO sector and to identify those NPOs that are particularly at risk of abuse by virtue of their activities or characteristics.

Sub-criterion 8.1.c—The efforts described under the previous sub-criteria are ongoing and continuously integrate new information on the sector's potential vulnerabilities.

Criterion 8.2— Awareness raising events are focused on registered charities as those are the organizations that fall within the FATF definition of NPOs. The CRA is undertaking efforts to increase awareness amongst registered charities of terrorism financing risks and vulnerabilities, including on international best practices for mitigating terrorism financing risks in the charities sector, sound governance, accountability procedures, transparency reporting, as well as consultative processes and presentations by senior management. The CRA also maintains a grants program to motivate and reward the development and application of innovative compliance programs amongst charities. Many of these activities include a TF component.

Criterion 8.3— Canada imposes comprehensive registration and regulatory requirements on charities under the Income Tax Act (ITA). Other NPOs may operate without being subject to any registration requirements, but are subject to record-keeping obligations on their stated purpose, administration, and management pursuant to the federal or provincial legislation under which they were established. In addition, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 must file an annual information return with the CRA. Based on the information provided by the authorities, it is estimated that as of December 2014, a total of 180 000 NPOs existed in Canada of which 86 000 or about 50%, were registered under the ITA. Under the ITA, a failure by a registered charity to comply with the registration requirements, including links to terrorism, may result in denial or revocation of registration. Under the Charities Registration (Security Information) Act the CRA may utilize all information available to determine the existence of terrorism links for new applications or existing registrations, including security or criminal intelligence and otherwise confidential information. Once registered, charities are required to file annual information returns and financial statements, including information on the directors and trustees, the location of activities, the charity's affiliation and the organization's name. Much of the information is made publicly accessible on the CRA's homepage. Donations, spending and record keeping are regulated under the ITA. The CRA is granted wide powers under Part XV of the ITA to administer and enforce the provisions of the law. The CRA is responsible for ensuring compliance by registered charities with the requirements under the ITA and to sanction non-compliance. In addition, law enforcement and intelligence authorities monitor NPOs and investigate those suspected of having links to terrorism.

Criterion 8.4— Based on the information provided by the authorities, it is estimated that as of December 2014 a total of 180 000 NPOs existed in Canada of which 86 000 or about 50%, were registered under the ITA. According to the CRA's NPO Sector Review of 2015, the 86 000 registered charities represent 68% of all revenues of the NPO sector and nearly 96% of all donations. CRA registered charities also account for a substantial share of the sector's foreign activities as about 75% of internationally operating NPOs are registered as charities.

Sub-criteria 8.4.a and b—Charities registered under the ITA have comprehensive annual filing obligations, including on their directors and trustees, and financial statements including balance sheets and income statements. All this information is publicly available at the CRA's webpage.

Sub-criterion 8.4.c—All registered charities, regardless of their assets, and all other types of NPOs with revenue in excess of CAD 200 000, and/or annual investment income exceeding CAD 10 000, must file an annual information return with the CRA, including financial information. In addition, registered charities with revenue in excess of CAD 100 000 and/or property used for charitable activities over CAD 25 000 and/or that have sought permission to accumulate funds, must provide financial information. CRA-Charities must ensure that charities' funds are fully accounted for by reviewing and conducting analysis of information submitted in the annual information return. Where there are irregularities or concerns CRA-Charities may conduct an audit to review charity's finances and activities in detail.

Sub-criterion 8.4.d—Registration with the CRA is optional, not mandatory.

Sub-criterion 8.4.e—ITA registered charities are required to know intermediaries that provide services on its behalf, and to ensure that charity funds are used only for charitable activities. As such, there is an obligation to know enough about beneficiaries to meet this obligation. NPOs can be held liable for acts by associated NPOs if the court finds that there is an agency relationship between the two, which provides an additional incentive for NPOs to know associate NPOs. Records of registered charities must be sufficient for the CRA to verify that the charity's resources have been used in accordance with its activities.

Sub-criterion 8.4.f—Comprehensive record-keeping obligations apply both for ITA registered charities and other types of NPOs based on the provisions of provincial or federal legislation.

Criterion 8.5— As part of their annual information return charities must provide a breakdown of financial information related to revenue and expenditures. This includes information on the total expenditures for charitable activities, management and administration, and gift to qualified donees. Charities must also report ongoing and new charitable programs. Where audits reveal financial irregularities, the CRA may apply a range of sanctions set out in the ITA. The CRA is granted a wide range of powers to monitor registered charities for compliance with the filing obligations under the ITA and to apply sanctions, including financial penalties and suspensions, or revocation of registration.

Criterion 8.6— *Sub-criterion 8.6.a*—For registered charities, the registration system under the ITA is supported by the Charities Registration (Security Information) Act which allows the Minister of Public Safety and Emergency Preparedness to take into account criminal and security intelligence reports on registered charities or those applying for registration. The CSIS and also the RCMP and CBSA contribute information to these criminal and security intelligence report. The CRA has entered into MOUs with the CSIS and RCMP to facilitate the process. Any suspicion that a specific charity is linked to terrorism may result in registration being denied or revoked.

Sub-criterion 8.6.b—For ITA registered charities, the CRA may share certain information about registered charities with the public, including foreign counterparts, online through the CRA's website, or upon request. Information that is publicly accessible, includes governing documents, the name of directors or trustees, annual information returns and financial statements.

Sub-criterion 8.6.c—For non-publicly available information, the ITA allows but does not oblige the CRA to disclose to FINTRAC as well as the RCMP and CSIS information about charities suspected of being involved in FT. Equally, the Security of Canada Information Sharing Act (SCISA) permits the CRA to share any taxpayer information relevant to a terrorism offense (under part II of the CC) or threats to the security of Canada (under the CSIS Act) with competent authorities, including any information that the CRA may have on the broader sector of NPOs. FINTRAC is required under the PCMLTFA to disclose information to the CRA with regards to registered charities. Additional information sharing powers are available under the Security of Canada Information Sharing Act whenever there is a threat to Canada's national security. For NPOs other than registered charities regular investigative and information-gathering powers under the criminal procedure code are available to obtain records and information, they are required to maintain under provincial or federal NPO legislation.

Criterion 8.7— The CRA may share certain information about registered charities with foreign counterparts, including governing documents, the names of directors or trustees, annual information returns, and financial statements. Additional information may be shared by the CRA with foreign tax authorities. If required, information on registered charities or NPOs may also be shared by FINTRAC and the RCMP as described under R.40 or based on formal MLA. In sum, Canada is found to have appropriate points of contact and procedures in place to respond to international request for information sharing regarding particular NPOs.

Weighting and Conclusion:

Canada is compliant with R.8.

Recommendation 9 – Financial institution secrecy laws

In its 2008 MER, Canada was rated C with R.4, and neither the relevant laws nor the applicable FATF R. have subsequently changed. The MER assessors' only concern was that data protection law implementation was subject to excessively strict interpretations that might prevent LEAs accessing information in the course of investigations.

Criterion 9.1— Various constitutional and legal provisions impose confidentiality obligations over personal information and individuals' privacy. In particular, s.8 of the Canadian Charter of Rights and Freedoms (which forms part of Canada's Constitution) provides that everyone has the right to be secure against unreasonable search and seizure. According to the Supreme Court of Canada, the purpose of s.8 is to protect a reasonable expectation of privacy. Accordingly, those who act on behalf of a government, including LEAs and supervisors, must carry out their duties in a fair and reasonable way. Canada also has two privacy laws: the Privacy Act covers the personal information-handling practices of federal government departments and agencies; and the PIPEDA is the main federal private-sector privacy law.

PIPEDA, s.5 notably contains specific obligations concerning organizations' collection, dissemination and use of customers' personal information. Every province and territory has its own public-sector

legislation and the relevant provincial act applies to provincial government agencies (in lieu of the Privacy Act). Some provinces also have private-sector privacy legislation. Alberta, British Columbia and Québec notably have legislation that have been declared "substantially similar" to the PIPEDA and apply to private-sector businesses that collect, use and disclose personal information while carrying out business within these provinces. Finally, several federal and provincial sector-specific laws also include provisions dealing with the protection of personal information: The federal Bank Act, in particular, contains provisions regulating the use and disclosure of personal financial information by FRFIs (ss.606 and 636 (1)); and most provinces also have laws governing credit unions that require the confidentiality of information related to members' transactions.

Various provisions also govern the authorities' access to information: of the PIPEDA, s.7(3)(d), in particular, provides that an organization may, without the individual's knowledge or consent or judicial authorization, disclose personal information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention. The "substantially similar" laws in Alberta, British Columbia and Quebec contain broadly equivalent provisions. The PCMLTFA also contains a number of provisions that enable FINTRAC to access information (ss.62-63) and the Bank Act (ss.643-644) and equivalent provisions governing other FRFIs gives OSFI powers to access all records of FRFIs.

As regards sharing of information between competent authorities, implementation of the Privacy Act, which obliges federal government departments and agencies to respect privacy rights, does not seem to have caused AML/CFT problems. The PCMLTFA (ss.55, 55.1, 56 and 65(1) and (2)) empowers FINTRAC to disclose information to a range of law enforcement and other competent authorities within Canada in specified circumstances. Similarly, the PCMLTFA, s.65.1(1)(a) allows FINTRAC to make agreements with foreign counterparts to exchange compliance information. The Bank Act, s 636(2) also enables OSFI to disclose information to other governmental agencies.

Weighting and Conclusion:

Canada is compliant with R.9.

Recommendation 10 – Customer due diligence

In the 2008 MER, Canada was rated NC with R.5. There were numerous deficiencies, and also the CDD requirement did not cover all FIs as defined by the FATF. Subsequently, both the PCMLTFA and PCMLTFR were amended to include measures covering the circumstances in which CDD must take place. Further PCMLTFR amendments, effective from February 2014, addressed most of the remaining deficiencies.

The 2008 MER noted that the requirement to conduct CDD excluded financial leasing, factoring and finance companies. The Sixth FUR (2014) concluded that the set of sectors not covered by the AML/CFT regime and not yet properly risk assessed was not a major deficiency. Since then, Canada's NIRA assessed the ML/TF vulnerabilities of factoring, finance and financial leasing companies as medium risk, while pointing out that these entities were very small players. Sectors not covered by

the AML/CFT regime are continually evaluated to identify trends indicating a higher ML/TF risk rating. Their current exclusion from the scope of the AML/CTF regime is an ongoing minor deficiency.

Criterion 10.1— In its 2008 MER, Canada explained that, while there was no explicit prohibition on opening anonymous accounts, the basic CDD requirements on all new account holders effectively prohibited anonymous accounts. This also applied to accounts in obviously fictitious names. The legal position remains unchanged: The PCMLTFA, s.6.1, requires REs to verify identity in prescribed circumstances and s.64 of the PCMLTFR sets out the measures to be taken for ascertaining identity. However, the 2008 assessors were concerned about the absence of detailed rules or guidance for FIs' use of numbered accounts, including compliance officers having access to related CDD information. Subsequently, OSFI Guideline B-8 addressed this latter point, covering the provision of account numbering or coding services that effectively shield the identity of the client for legitimate business reasons. Thus, FRFIs should ensure that they had appropriately ascertained the identity of the client and that the firm's Chief AML Officer could access this information. Consequently, this deficiency has been partially addressed through an adequate control mechanism, for FRFIs only, albeit not by enforceable means. This is a relatively minor matter.

When CDD is Required

Criterion 10.2— PCMLTFR ss.54, 54.1, 55, 56, 57, 59(1), 59(2) and 59(3) of the require FIs to ascertain the identity of their clients when establishing business relations. Similarly, all REs must ascertain the identity of every client with whom they conduct an occasional large cash transaction of CAD 10 000 or more. Two or more such transactions that total over CAD 10 000, conducted within a period of 24 hours, are deemed a single transaction. CDD is required for both cross-border and domestic wire transfers exceeding CAD 1 000.

Pursuant to PCMLTFR s.53.1(1) FIs must) take reasonable measures to verify the identity of every natural person or entity who conducts, or attempts to conduct, a transaction that should be reported to FINTRAC (i.e. where there is suspicion of ML or TF). This obligation applies (s.62(5)) even when it would not otherwise have been necessary to verify identity. Also, FIs must reconfirm (s.63 (1.1) of the PCMLTFR) the client's identity where doubts have arisen about the information collected. However, this measure applies only to natural persons, not to legal persons or arrangements.

The limited application of this last measure remains a deficiency under 10.2(e).

Required CDD Measures for all Customers

Criterion 10.3— PCMLTFA, s.6.1 of the requires REs to verify the identity of a person or entity in prescribed circumstances and in accordance with the Regulations. PCMLTFR ss.64 to 66 detail the measures that REs must take to ascertain the identity of a prescribed individual, corporation and "entity other than a corporation.[107]" For individuals, acceptable identification documents include a

[107] This is not defined in the Regulations, but would include any kind of unincorporated business or legal arrangement.

birth certificate, driver's license, passport, or other similar document. For corporations, the corporation's existence is confirmed, and the names and addresses of its directors ascertained, by reference to its certificate of corporate status. However, other methods are acceptable, e.g. a record that it is required to file annually under applicable provincial securities legislation, or any other record that validates its existence as a corporation. The existence of an entity other than a corporation must be confirmed by reference to a partnership agreement, articles of association, or other similar record that ascertains its existence. These legal provisions meet the FATF standard.

Criterion 10.4— The "Third Party Determination" provisions of the PCMLTFR require FIs to determine whether their customers are acting on behalf of another person or entity. Where an account is to be used by or on behalf of a third party, the FI must collect CDD information on that third party and establish the nature of the relationship between third party and account holder.

Criterion 10.5— PCMLTFR s.11.1(1) requires FIs, at the time the entity's existence is confirmed, to obtain the following information:

For corporations, the name of all directors of the corporation and the name and address of all persons who own or control, directly or indirectly, 25% or more of the shares of the corporation;

For trusts, the names and addresses of all trustees and all known beneficiaries and settlors of the trust;

For entities other than corporations or trusts (typically, a partnership fund or unincorporated association or organization), the name and address of all persons who own, directly or indirectly, 25% or more of the shares of the entity; and

In all cases, information establishing the ownership, control, and structure of the entity.

Under the PCMLTFR, s.11.1(2), REs further need to "take reasonable measures to confirm the accuracy of the information obtained" on beneficial ownership. This requirement implies the need to use reliable sources to obtain the requisite information and the FATF standard[108] allows identification data to be obtained "from a public register, from the customer, or from other reliable sources." Also, OSFI Guideline B-8 usefully indicates that "reasonable measures" to identify ultimate beneficial owners could include not only requesting relevant information from the entity concerned, but also consulting a credible public or other database or a combination of both. This Guideline also makes clear that the measures applied should be "commensurate with the level of assessed risk."

No specific legal provisions cover beneficial ownership of personal accounts. However, the PCMLTFR, in effect, establish beneficial ownership of personal accounts: in particular, s.9 requires REs to determine whether personal accounts are being used on behalf of a third party and, for personal accounts in joint names, all authorized signatories are subject to CDD measures.

[108] FATF (2013), Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems, p. 147, www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Criterion 10.6— PCMLTFR, s.52.1, requires every person or entity that forms a business relationship under the Regulations to keep a record of the purpose and intended nature of that business relationship. OSFI Guideline B-8 amplifies this requirement, requiring a FRFI to be satisfied that the information collected demonstrates that it knows the client.

Criterion 10.7— PCMLTFR ss.54.3 (financial entities), 56.3 (life insurance sector), 57.2 (securities dealers), 59.01 (MSBs), and 61.1 (departments or agencies of the government or provinces that sell or redeem money orders) require all covered REs to conduct ongoing monitoring of their business relationships. Section 1(2) defines this to mean monitoring on a periodic basis, according to assessed risk, by a person or entity of their business relationships with clients for the purpose of (i) detecting transactions that must be reported to FINTRAC; (ii) keeping client identification information up to date; (iii) reassessing levels of risk associated with clients' transactions and activities; and (iv) determining whether transactions or activities are consistent with the information.

Where higher risks are identified, PCMLTFR, ss.71.1(a)-(c)) require "prescribed special measures" to be taken, which include enhanced measures to keep client identification and beneficial ownership information up to date and also to monitor business relationships in order to detect suspicious transactions. The Regulations do not explicitly cover scrutiny of the source of funds.

Specific CDD Measures Required for Legal Persons and Legal Arrangements

Criterion 10.8— The PCMLTFR requirements for FIs to understand the nature of the customer's business and its ownership and control structure cover legal persons or legal arrangements.

Criterion 10.9— See c.10.3 above, which covers identification and verification of legal persons and arrangements. The PCMLTFR (ss.14(b), 14.1(b), 15(1)(c), 20, 23(1)(b), 30(b) and 49(b)) require the collection of information on power to bind the legal person or arrangement in relation to an account or transaction. However, the Regulations do not cover gathering the names of relevant persons having a senior management position in the legal person or arrangement. Where an RE is unable to obtain information about the ownership, control and structure of a trust or other legal arrangement, the PCMLTFR (s.11.1(4)(a)) require reasonable measures to be taken to ascertain the identity of the most senior managing officer of the entity concerned.

The Regulations (s.65(1)) require confirmation of a corporation's existence, and its name and address, by reference to its certificate of corporate status or other acceptable official record. The existence of an entity other than a corporation must be confirmed by referring to a partnership agreement, articles of association or other similar record. There is no specific requirement, in this case, to obtain the address of the registered office or principal place of business, if different. Consequently, for non-corporate legal persons and for legal arrangements such as trusts, the standard is only partially met. Partnership agreements, etc., are unlikely to confirm details of address and principal place of business. Similarly, while trust documents usually contain sufficient information to satisfy the account-holding FI as to name, legal form, and proof of existence; such documents usually do not provide additional information about the registered address or principal business of the trust.

In addition, trust companies are required when acting as trustee of a trust (ss.55 (a)-(c)) to (i) of the PCMLTFR) to ascertain the identity of every person who is the settlor of an inter vivos trust: (ii) confirm the existence of, and ascertain the name and address of, every corporation that is the settlor of an institutional trust; and (iii) confirm the existence of every entity, other than a corporation, that is the settlor of an institutional trust. Under the Regulations (s.55 (d)), where an entity is authorized to act as a co-trustee of any trust, the trust company must (i) confirm the existence of the entity and ascertain its name and address; and (ii) ascertain the identity of all persons—up to three—who are authorized to give instructions with respect to the entity's activities as co-trustee. Finally, under the Regulations (s.55 (e)), trust companies must ascertain the identity of each person who is authorized to act as co-trustee of any trust. However, as natural persons who are trustees are not REs under the PCMLTFA, they are not subject to CDD obligations.

PCMLTFR ss 11 (a)-(b) require trust companies, for inter vivos trusts, to (i) keep a record that sets out the name and address of each of the beneficiaries that are known at the time that the trust company becomes a trustee for the trust; (ii) if the beneficiary is a natural person, record their date of birth and the nature of their principal business or their occupation; and (iii) if the beneficiary is an entity, the nature of their principal business.

Criterion 10.10— The legal requirements for obtaining information on beneficial owners of customers that are legal persons are set out under c.10.5 above.

REs must confirm the existence of a corporation or non-corporate legal entity at the opening of an account or when conducting certain transactions. At the same time, they must obtain information about the entity's beneficial ownership and confirm its accuracy. Beneficial ownership refers to the identity of the individuals who ultimately control the corporation or entity, which extends beyond another corporation or another entity. The PCMLTFR requirements for corporations and other entities refer to "persons." PCMLTFA, s.2 defines "person" to mean an individual, which therefore requires the natural person to be identified. If the RE has doubts about whether the person with the controlling ownership interest is the beneficial owner, then it is deemed to have been unable to obtain the information referred to under PCMLTFR, s.11.1(1) or to have been unable to confirm that information in accordance with PCMLTFR, s.11.1(2). In this case, the RE is required, under PCMLTFR s.11.1(4), to: take reasonable measures to ascertain the identity of the most senior managing officer of the entity; treat that entity as high risk for the purpose of PCMLTFA, s.9.6(3) and apply the prescribed special measures set out in PMCLTFR, s.71.1. Where no individual ultimately owns or controls 25% or more of an entity, directly or indirectly, REs must nevertheless record the measures they took, and the information they obtained, in order to reach that conclusion. Also, REs must comply with PCMLTFR, s.11.1(1)(d), which requires that information "establishing the ownership, control and structure of the entity" be obtained.

Criterion 10.11— The legal requirements for collecting information on the identity of beneficial owners of customers that are legal arrangements are set out under c.10.5 and 10.9 above. It is unclear, in the case of trusts, what identification requirements apply to protectors. Beneficiaries of trusts are covered by the ongoing monitoring provisions of s. 1(2) of the Regulations, which require that client identification information and information be kept up to date.

CDD for Beneficiaries of Life Insurance Policies

Criterion 10.12— All provincial *Insurance Acts* require life insurance companies to conduct CDD on (and keep a record of) the beneficiaries of life insurance policies, so this requirement applies to insurance companies nationally. There is no specific requirement to verify the identity of the beneficiary at the time of pay-out.

Criterion 10.13— As life insurance companies are covered under the PCMLTFA, they must risk assess all their clients and business relationships, products and services, and any other relevant risk factors (which include the beneficiary of a life insurance policy). In cases of high risk, life insurance companies must apply enhanced measures (prescribed special measures—s.71.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*).

Timing of Verification

Criterion 10.14— PCMLTFR, ss.64(2), 65(2) and 66(2)) specify the timeframe for verifying the identity of individuals, corporate and non-corporate entities. With certain exceptions, the legal obligation is to verify identity either at the time of the transaction or before any transaction other than an initial deposit is carried out. There are two main exceptions: (i) in relation to trust company activities, identity may be verified within 15 days of the trust company becoming the trustee; (ii) in relation to life insurance transactions and government or provincial departments or agencies handling money orders, identity may be verified within 30 days of the client information record being created. These exceptions are not justified according to what is reasonably practicable or necessary to facilitate the normal conduct of business, nor is there any condition about managing the ML/TF risks of delaying identity verification.

Criterion 10.15— PCMLTFR, s.1(2) defines "business relationship" to commence on account opening or when a client conducts specified transactions that would require their identity to be ascertained. Consequently, it is not possible for a customer to utilize a business relationship prior to verification.

Existing Customers

Criterion 10.16— see c.10.7. These ongoing monitoring obligations apply to all clients, whether or not they were clients at the date of new CDD obligations coming into force. Consequently, the ongoing monitoring process covers clients whose identity had not previously been ascertained. REs are required to take a risk-based approach to keeping information on client identification, beneficial ownership and purpose and nature of intended business relationship up to date.

Risk-Based Approach

Criterion 10.17— PCMLTFR, s.71.1 details the "prescribed special measures" to be taken in cases of high risk. This includes, for example, cases where beneficial ownership information cannot be obtained or confirmed. These special measures comprise taking enhanced measures to (i) ascertain the identity of a person or confirm the existence of an entity; (ii) keep client identification

information up to date (including beneficial ownership information); (iii) monitor business relationships for the purpose of detecting suspicious transactions; and (iv) determining whether transactions or activities are consistent with the information. In addition, Appendix 1 to FINTRAC Guideline 4 provides a checklist of products or services that should be considered high-risk.

Criterion 10.18— No reduced or simplified CDD measures are in place. Instead, the PCMLTFR gives exemptions from the client identification and record-keeping requirements in specific circumstances assessed as low risk by the authorities. These exemptions are mainly contained in s. 9 (accounts used by, or on behalf of, a third party) and s.62 (mainly concerning life insurance business). Furthermore, PCMLTFR, ss.19 and 56 create a form of exemption by requiring that life insurers only conduct CDD in relation to the purchase of an immediate or deferred annuity or a life insurance policy for which the client may pay CAD 10 000 or more over the duration of the annuity or policy. However, these exemptions do not apply where there is a suspicion of ML or TF.

Failure to Satisfactorily Complete CDD

Criterion 10.19— The PCMLTFA, s.9.2, provides that no RE shall open an account for a client if it cannot establish the identity of the client in accordance with the prescribed measures. Consequently, an FI that failed to conduct CDD, when obliged to do so, would be in breach of the Act and could be fined. There is no explicit prohibition on REs commencing a business relationship or performing a transaction when they are unable to comply with CDD measures if the identity of an individual cannot be ascertained or the existence of an entity confirmed when they open an account, the FI cannot open the account. This also means that no transaction, other than an initial deposit, can be carried out. Also, if the RE suspects that the transaction is related to a ML or TF offense, it must file an STR with FINTRAC. Under PCMLTFA, s.7, if the RE has reasonable grounds to suspect that the client conducts or attempts to conduct a transaction that is related to the commission or the attempted commission of an ML or TF offense, even if the client cannot be identified or his/her identity cannot be properly verified, the RE must file a STR. This requirement is amplified in FINTRAC guidance.

CDD and Tipping Off

Criterion 10.20— PCMLTFR, s.53.1 (2) specifies that the identity verification obligation does not apply where the RE believes that complying with that obligation would inform the customer that the transaction is being reported as suspicious. PCMLTFA s. 7 requires an STR to be filed in these circumstances.

Weighting and Conclusion

A number of relatively minor deficiencies have been identified.

Canada is largely compliant with R.10.

Recommendation 11 – Record-keeping

In the 2008 MER, Canada was rated LC with R.10. Two deficiencies were noted. First, the record-keeping requirement did not cover all FIs as defined by the FATF (notably financial leasing, factoring and finance companies). Second, FIs must ensure that all records required to be kept under the PCMLTFA could be provided within 30 days, which did not meet the requirement to make CDD records available on a timely basis. The FATF standard has not since changed, the requirement being to make records available "swiftly".

Criteria 11.1 and 11.2— The PCMLTFRs.69 detail the obligation to keep records for a period of at least five years following completion of the transaction or termination of the business relationship.

The PCMLTFR outlines, for each type of covered entity, detailed record-keeping rules for CDD, account files and business correspondence. The Regulations do not specifically require retention of any internal analysis of client business that might lead to an STR. However, covered entities would need to keep this information to substantiate that they were not in contravention of PIPEDA and that the disclosure without consent would have been warranted. The Privacy Commissioner could request this type of information under PIPEDA, s.18 as part of a compliance audit. In addition, OSFI requires FRFIs to keep such information.

Criterion 11.3— There is no clear legal obligation that transaction records be sufficient to permit reconstruction of individual transactions. However, the Regulations do specify in detail the contents of each piece of information that must be held in various records.

Criterion 11.4— The PCMLTFR s.70 requires REs to provide records upon request of FINTRAC within 30 days. This does not meet the "swiftly" standard.

Weighting and Conclusion

The deficiencies noted in the 2008 MER remain.

Canada is largely compliant with R.11.

Recommendation 12 – Politically exposed persons

In the 2008 MER, Canada was rated NC with R.6. There were no relevant legislative or other enforceable requirements in place.

Significant changes have been introduced since then. Requirements for FIs in relation to Politically Exposed Foreign Persons (PEFPs) were introduced in June 2008 through amendments to the PCMLTFA and PCMLTFR, specifying the enhanced customer identification and due-diligence requirements for such clients.

Subsequently, as part of a package of amendments to the PCMLTFA introduced in 2014, the coverage of the Act was extended to include Politically Exposed Domestic Persons (PEDP) and heads of international organizations. The bill was enacted on 19 June 2014; however, implementing

regulations are required before the PEP provisions will come into force. These regulations, announced on 4 July 2015, will come into force one year after registration of the regulations. They will require REs to determine, under prescribed circumstances, whether a client is a PEFP, a PEDP, a head of an international organization, or a close associate or prescribed family member of any such person.

Criterion 12.1— The PCMLTFR ss.54.2, 56.1, 57.1, 59(5) require REs to take reasonable measures to determine a person's status as a PEFP. FINTRAC Guidance 6G explains the PEP determination and OSFI Guideline B-8 is also relevant.

FINTRAC Guidance (s.8.1) makes clear that reasonable measures must be taken in relation to both new and existing accounts, as well as certain electronic funds transfers (EFT). Also, those measures include asking the client or consulting a credible commercially and/or publicly available database. OSFI Guideline B-8 also details what would constitute reasonable measures to make a PEFP determination.

PCMLTFA s. 9.3.2 requires REs, when dealing with a PEFP, to obtain the approval of senior management in the prescribed circumstances and take prescribed measures. For existing accounts, PCMLTFR, s. 67.1 (b) requires FIs and securities dealers to obtain the approval of senior management to keep a PEFP account open. FINTRAC Guidance 6G explains when to obtain the approval of senior management.

The Regulations (s. 67.2) also require REs to take reasonable measures to establish the PEFP's source of funds. FINTRAC Guidance 6G explains that reasonable measures include asking the client and OSFI Guideline B-8 gives a number of examples of acceptable sources of funds. Source of wealth is not mentioned in the Regulations; however, Guideline B-8 states that FRFIs should satisfy themselves that the amount of clients' accumulated funds or wealth appears consistent with the information provided.

The Regulations (s. 67.1 (1)(c)) require FIs and securities dealers to conduct enhanced ongoing transaction monitoring of PEFP and their family members' accounts. However, no similar legal requirement applies to other REs in relation to PEFPs, although FINTRAC Guidance 6G does specify enhanced ongoing monitoring of PEFP account activities. OSFI Guideline B-8 states that enhanced ongoing transaction monitoring may involve manual or automated processes, or a combination, depending on resources and needs and gives some examples of what this could comprise.

Criterion 12.2— OSFI Guideline B-8 explains that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, whether by screening or flagging large transactions or in any other way. Further, even if FRFIs know they are dealing with a domestic PEP, until new regulations come into effect, they have no legal obligation to apply enhanced measures to PEDPs as they do to PEFP accounts.

Nevertheless, this OSFI guidance states that, where a FRFI is aware that a client is a domestic PEP, it should assess any effect on the overall assessed risk of the client. If that risk is elevated, the FRFI should apply appropriate enhanced due-diligence measures.

Criterion 12.3— Currently, PCMLTFA, s.9.3 includes family members of PEFPs and PCMLTFR, (s.1.1) states that the prescribed family members of a PEFP are included in the definition of a PEFP. Until the necessary implementing regulations take effect, close associates of any kind of PEP are not covered in law or regulations.

Criterion 12.4— No provisions in law or regulations relate to beneficiaries of life insurance policies who may be PEPs.

Weighting and Conclusion

Canada is non-compliant with R.12.

Recommendation 13 – Correspondent banking

In the 2008 MER, Canada was rated PC with R.7. Deficiencies were noted in relation to: assessment of a respondent institution's AML/CFT controls; assessment of the quality of supervision of respondent institutions; and inadequate CDD for payable-through accounts.

Criterion 13.1— The PCMLTFR (s.15.1 (2)) cover correspondent banking relationships, requiring FIs to collect a variety of information and documents on the respondent institution. That information includes: the primary business line of the respondent institution; the anticipated correspondent banking account activity of the foreign FI, including the products or services to be used; and the measures taken to ascertain whether there are any civil or criminal penalties that have been imposed on the respondent institution in respect of AML/CFT requirements and the results of those measures. The Regulations contain no specific requirements about determining either the reputation of the respondent institution or the quality of supervision to which it is subject. The PCMLTFR (s.15.1(3)) require the taking of reasonable measures to ascertain whether the respondent institution has in place AML/CFT policies and procedures, including procedures for approval for the opening of new accounts. There is, however, no requirement to assess the quality of a respondent institution's AML/CFT controls. PCMLTFA s. 9.4 (1) requires senior management approval to be obtained for establishing new correspondent relationships. The Regulations (s.15.1(2)(f)) specify the collection of a copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity.

Criterion 13.2— The PCMLTFR (s. 55.2) stipulate that where the customer of the respondent institution has direct access to the services provided under the correspondent banking relationship (the 'payable-through account' scenario), the FI shall take reasonable measures to ascertain whether (i) the respondent institution has met the customer identification requirements of the Regulations; and (ii) the respondent institution has agreed to provide relevant customer identification data upon request.

Criterion 13.3— PCMLTFA, s.9.4 (2) prohibits correspondent banking relationships with a shell bank. In addition, the PCMLTFR (s. 15.1 (2) (h) require FIs to obtain a statement from the

respondent institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.

Weighting and Conclusion

Deficiencies remain under c. 13.1.

Canada is largely compliant with R.13.

Recommendation 14 – Money or value transfer services

In its 2008 MER, Canada was rated NC with SR VI. The main deficiencies were: lack of a registration regime for money services businesses (MSBs); no requirement for MSBs to maintain a list of their agents; and the sanction regime available to FINTRAC and applicable to MSBs was deemed not effective, proportionate and dissuasive. Subsequently, Canada has made significant progress, and the FATF standard has been strengthened to require countries to take action to identify unlicensed or unregistered MSBs and apply proportionate and dissuasive sanctions to them.

Criterion 14.1— PCMLTFA, s.11.1 stipulates that any entity or person covered by s.5(h) of the Act, (persons and entities engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's checks or other similar negotiable instruments) and those referred to in s.5(l) of the Act (those that sell money orders to the public), must be registered with FINTRAC.

Criterion 14.2— Under its mandate (PCMLTFA, s. 40(e)) to ensure compliance with part 1 of the Act, FINTRAC has a process for identifying MSBs that carry out activities without registration. This includes searching advertisements and other open sources as well as through on-site visits. Additionally, MVTS whose registration status is revoked are still tracked to ensure that they are not conducting business illegally.

The PCMLTF Administrative Monetary Penalties (AMP) Regulations describe the classification of different offenses under the PCMLTFA and the Regulations. Failure to register is classified as a serious violation. These Regulations classify violations as minor, serious, and very serious, each with a varying range of monetary penalties, up to CAD 500 000. In addition to criminal sanctions and monetary penalties for non-compliance, FINTRAC uses other means to encourage compliance. Monetary penalties are only considered after giving an entity or person a chance to correct deficiencies. If a very serious violation has been committed, a fine is greater than CAD 250 000, or if there is repeat significant non-compliance, FINTRAC considers publicly naming that entity or person, using its powers under s.73.22 of the PCMLTFA.

Criterion 14.3— PCMLTFA s. 40 (e) gives FINTRAC the mandate to ensure compliance with the Act. FINTRAC uses its powers under the PCMLTFA (ss. 62, 63 and 63.1) to examine records and inquire into the business and affairs of REs to monitor MVTS providers for AML/CFT compliance.

Criterion 14.4— PCMLTFA, ss.11.12(1) and (2) require that a list of agents, mandataries or branches engaged in MSB services on behalf of the applicant be submitted upon registration of the MSB with FINTRAC. S. 11.13 of the Act stipulates that a registered MVTS must notify FINTRAC of any change to the information provided in the application or of any newly obtained information within 30 days of the MVTS becoming aware of the change or obtaining the new information. This includes information about the MVTS's agents.

This criterion is also met through the legal obligation described under c. 14.1 above.

Criterion 14.5— The PCMLTFR (s.71(1)(d)) require MVTS, who have agents or other persons authorized to act on their behalf, to develop and maintain a written ongoing compliance training program for those agents or persons. S. 71(1)(e) also requires MVTS to institute and document a review of their agents' policies and procedures, risk assessment and the training program for the purpose of testing effectiveness. Such reviews must be carried out every two years.

Weighting and Conclusion

Canada is compliant with R.14.

Recommendation 15 – New technologies

In the 2008 MER, Canada was rated NC with former R.8 due to the lack of legislative or other enforceable obligations addressing the risks of new technological developments. Since then, some 40 legislative amendments to the PCMLTFA were tabled in Parliament (e.g. measures to subject new types of entities to the PCMLTFA, including online casinos, foreign MSBs and businesses that deal in virtual currencies such as Bitcoin). Canada is currently developing regulatory amendments to cover pre-paid payment products (e.g. prepaid cards) in the AML/CTF regime. The NRA examined the ML/TF vulnerabilities of 27 economic sectors and financial products, including new and emerging technologies, both in terms of products (e.g. virtual currency and pre-paid access), and sectors (e.g. telephone and online services in the banking and securities sectors).

Criterion 15.1— REs must conduct a risk assessment that includes client and business relationships, products and delivery channels, and geographic location of activities of the RE and the client(s), and any other relevant factors (PCMLTFR. s.71(1)(c)). While the requirements capture the need to assess ML/TF risks related to products and delivery mechanisms, there is no explicit legal or regulatory obligation to similarly risk assess the development of new products and business practices, nor is there any such obligation relating to the use of new or developing technologies for new and pre-existing products. However, Canada issued regulatory amendments for public comment in July 2015 clarifying that REs must consider, in their risk assessment, any new developments in, or the impact of new technologies on, the RE's clients, business relationships, products or delivery channels or the geographic location of their activities. A risk assessment review must be conducted every two years by an internal or external auditor, or by the entity (s.71(1)(e) of the Regulations). This ensures that risk assessments are regularly evaluated to capture risks, which may include new technologies. FINTRAC Guideline 4 specifies that new technology developments (e.g. electronic cash,

stored value, payroll cards, electronic banking, etc.) must be included in a company's risk assessment.

Criterion 15.2— While there is a regulatory expectation in FINTRAC's risk-based approach guidance[109] which states that REs should reassess their risk if there are changes due to new technologies or other developments, there are no explicit requirements in law or regulation that FIs undertake risk assessments prior to the launch or use of such products, practices and technologies.

Weighting and Conclusion:

Canada is non-compliant with R.15.

Recommendation 16 – Wire transfers

In the 2008 MER, Canada was rated NC with SR VII, which had simply not been implemented. Canada made some progress since then. The requirements have also been very substantially expanded in R.16 (i.e. inclusion of beneficiary information in wire transfers and additional obligations on intermediary and beneficiary FIs and MSBs).

Ordering Financial Institutions

Criterion 16.1— PCMLTFA, s.9.5 requires FIs to include with the transfer, when sending an international EFT, the name, address, and account number or other reference number, if any, of the client who requested it. The Act has no equivalent provision about including beneficiary name, account number or unique transaction reference number in this 'ordering FI' scenario. However, Schedule 2, Part K, of the PCMLTFR, which covers outgoing SWIFT payment instructions report information, does stipulate that, for single transactions of CAD 10 000 or more, the beneficiary client's name, address and account number (if applicable) should be included. There are no enforceable provisions requiring FIs to include beneficiary information in EFTs below CAD 10 000 (either as a single transaction, or multiple transactions within a 24-hour period).

Criterion 16.2— PCMLTFA, s.9.5 is not limited to single transfers—it, therefore, also applies in cases where numerous individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries.

Criterion 16.3— There is no 'de minimis' threshold for the requirements of c.16.1.

Criterion 16.4— Originator information would be verified through CDD obligations (see R.10). In addition, s. 53.1 of the Regulations states that the identity of every person that conducts a suspicious transaction must be ascertained, unless it was previously ascertained, or unless the FI believes that doing so would inform the individual an STR was being submitted.

Criterion 16.5— The Act's s.9.5 requirements cover both domestic and international EFTs.

[109] FINTRAC (2015), Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorist Financing, www.fintrac-canafe.gc.ca/publications/rba/rba-eng.pdf.

Criterion 16.6— Canada does not permit simplified originator information to be provided.

Criterion 16.7— The PCMLTFR (ss. 14 (m) and 30 (e)) require FIs and MSBs to keep a record of the name, address and account number, or transaction reference of the ordering client for all EFTs of CAD 1 000 or more. In addition, a record must be kept of the name and account number of the recipient of the EFT, as well as the amount and currency of the transaction.

Criterion 16.8— There is no explicit prohibition on executing wire transfers where CC, ss.16.1 to 16.7 above cannot be met. However, if an RE is unable to comply with the relevant legal requirements, it cannot proceed with a wire transfer without breaking the law and being subject to AMPs.

Intermediary Financial Institutions

Criteria 16.9 to 16.12— The PCMLTFA and regulations use the terms "send/transfer" and "receive" to apply obligations to intermediaries, which are, therefore, subject to the same requirements that apply to ordering and beneficiary institutions. Thus, the implications of possible data loss and of straight-through processing are not captured, as they should be to meet the standard.

Beneficiary Financial Institutions

Criterion 16.13— PCMLTFA, s.9.5(b) requires FIs to take reasonable measures to ensure that any transfer received by a client includes information on the name, address, and account number or other reference number, if any, of the client who requested the transfer. These requirements apply equally to all EFTs, regardless of where they are situated in the payment chain. Where an FI is transmitting a transfer received from another FI, it is, therefore, required to ensure that complete originator information is included. There are no legal requirements relating to beneficiary information.

OSFI Guideline B-8 states that FRFIs that act as intermediary banks should develop and implement reasonable policies and procedures for monitoring payment message data subsequent to processing. Such measures should facilitate the detection of instances where required message fields are completed but the information is unclear, or where there is meaningless data in message fields. The Guideline cites a few examples of reasonable measures that could be taken.

Criteria 16.14 and 16.15— There are no specific obligations on beneficiary FIs involved in cross-border EFTs.

Money or Value Transfer Service Operators

Criterion 16.16— All obligations identified in CC, ss.16.1–16.9 above apply to MSBs and their agents.

Criterion 16.17— There are no specific legal requirements for MTVS providers either to review ordering and beneficiary information to decide whether to file an STR or to ensure that an STR is filed in any country affected and transaction information made available to the FIU.

Implementation of Targeted Financial Sanctions

Criterion 16.18— See the assessment of R.6 and R.7. The processing of EFTs, in terms of FIs taking freezing action and complying with prohibitions from conducting transactions with designated persons and entities, is adequately covered in law.

Weighting and Conclusion

The legal obligations applicable to ordering FIs and MSBs are broadly satisfactory, but there remain some weaknesses.

Canada is partially compliant with R.16.

Recommendation 17 – Reliance on third parties

In the 2008 MER, Canada was rated NC with R.9. In the only two scenarios where reliance on a third party or introduced business was legally allowed without an agreement or arrangement, the measures in place were insufficient to meet the FATF standard. In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector used introduced business mechanisms as a business practice. However, no specific requirements, as set out in R.9, applied to these scenarios. Only minor changes have subsequently been introduced.

Criterion 17.1— The PCMLTFR (ss. 64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities, to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person.

More specific legal provisions apply to both the life insurance industry and securities dealers. A life insurance company, broker, or agent is not required to ascertain the identity of a person where that person's identity has previously been ascertained by another life insurance company, broker, or agent in connection with the same transaction or series of transactions that includes the original transaction. Similarly, a securities dealer, when opening an account for the sale of mutual funds, is not required to ascertain identity where another securities dealer has already done so in respect of the sale of mutual funds for which the account has been opened. The PCMLTFR (s.56(2) and s.62(1)(b)) refer.

Apart from the specific situations set out above, all requirements under the PCMLTFR continue to apply to the FI that has the relationship with the customer.

The PCMLTFR (s.64.1) state that, when REs use an agent or a mandatary to meet their client identification obligations, they must enter into a written agreement or arrangement with the agent or mandatary. In addition, the RE must obtain from the agent or mandatary the customer information that was obtained under the agreement or arrangement. The agent or mandatary can be any individual or entity, provided these two conditions regarding written agreement and obtaining customer information are met. Where the client is not physically present at the opening of an account, establishment of a trust or conducting of a transaction, the agent or mandatary has the same

two options, outlined in ss.64(1) and 64(1.1), that an RE does when dealing with a client who is not physically present.

In the first option, the agent or mandatary must obtain the individual's name, address, and date of birth. Then, they must confirm that one of the following has ascertained the identity of the individual by referring to an original identification document:

- a financial entity, life insurance company, or securities dealer affiliated with them;
- an entity affiliated with them and whose activities outside Canada are similar to those of a financial entity, life insurance company, or securities dealer; or
- another financial entity that is a member of their financial services cooperative association or credit union central association of which they also are a member.

To use this option, the agent or mandatary must verify that the individual's name, address and date of birth correspond with the information kept in the records of that other entity. The second option requires the use of a combination of two of the identification methods set out in Part A of Schedule 7 of the PCMLTFR.

Where agents or mandataries with written agreements are concerned, the relying entity must obtain customer information supplied under the agreement. However, life insurance companies/brokers/agents or securities dealers are not required to obtain from the relied-upon institution the necessary CDD information.

Similarly, life insurance companies/brokers/agents or securities dealers are not required to satisfy themselves that copies of CDD information will be made available to them by the third party on request without delay.

There is no explicit obligation, either for relying entities with agents and mandataries or for life insurance companies/brokers/agents or securities dealers, to satisfy themselves that the FI relied on is regulated and supervised or monitored for compliance with CDD and record-keeping obligations in line with R.10 and R.11.

Criterion 17.2— The PCMLTFA and PCMLTFR do not require life insurance companies/brokers/agents or securities dealers to assess which countries are high risk for third party reliance. The authorities state that reliance may only be placed on life insurance companies/brokers/agents or on securities dealers that are subject to the PCLMTFA, and FINTRAC's oversight. If so, the scenario outlined in Criterion 17.2 would not arise.

While ss.56(2) and 62(1) (b) of the PCMLTFR do not actually preclude the possibility of reliance being placed on third parties outside Canada, with no account taken of the level of country risk, an RE can only rely on third parties outside Canada if they are affiliated with them. Canada issued

regulatory amendments for public comment in July 2015 that included an amendment with respect to Group-Wide Compliance Programs that would require REs to take into consideration as part of their compliance programs the risks resulting from the activities of their affiliates.

Criterion 17.3— The PCMLTFR (ss.64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person. PCMLTFA, ss9.7 and 9.8 require foreign branches and subsidiaries, subject to there being no conflict with local laws, to develop and apply policies to keep records, verify identity, have a compliance program, and exchange information for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. Thus, group-wide ML/TF standards should apply, providing appropriate safeguards.

Where there is a conflict with, or prohibition by, local laws, the RE must keep a record of that fact, with reasons, and notify both FINTRAC and its principal federal or provincial regulator within a reasonable time (PCMLTFA, s.9.7(4)).

Weighting and Conclusion

A number of deficiencies remain, even though that reliance on third parties appears to be of limited practical application.

Canada is partially compliant with R.17.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 2008 MER, Canada was rated LC with R.15 due to minor deficiencies and NC with R.22 due to the lack of legal obligation to ensure that foreign branches and subsidiaries applied AML/CFT measures consistent with home country standards, and obligation to pay particular attention to branches and subsidiaries in countries, which did not, or insufficiently, applied the FATF Recommendations. The current FATF standards are broadly unchanged, although R.18 specifies in more detail what should be done to manage ML/TF risk where host country requirements are less strict than those of the home country. Significant changes came into force in Canada in June 2015.

Criterion 18.1— PCMLTFA s. 9.6 requires FIs to establish and implement a compliance program to ensure compliance with the Act. The program must include the development and application of policies and procedures for the FI to assess, in the course of their activities, the risk of an ML or TF offense. The PCMLTFR (ss. 71 (1)(a) and (b)) specify that: a person must be appointed to be responsible for implementation of the program; and the program must include developing and applying written compliance policies and procedures that are kept up-to-date and approved by a senior officer.

OSFI Guideline B-8 stipulates that FRFIs must have a Chief Anti-Money Laundering officer (CAMLO) responsible for implementation of the enterprise AML/ATF program, who should be one person positioned centrally at an appropriate senior corporate level of the FRFI. Separately, OSFI Guideline E-13 requires that FRFIs must have a Chief Compliance officer with a clearly defined and

documented mandate, unfettered access and, for functional purposes, a direct reporting line to the Board.

Neither the PCMLTFA nor PCMLTFR contain any specific obligations regarding FIs' screening procedures when hiring employees. Similarly, there are no measures in place in sector legislation at the federal or provincial level. OSFI Guideline E-17 details OSFI's expectations in respect of screening new directors and senior officers of FRFIs at the time of hiring. However, this applies only to a defined set of "Responsible Persons," not to all employees.

The PCMLTFR (s. 71(1)(d)) require REs that have employees, agents or other persons authorized to act on their behalf to develop and maintain a written ongoing training program for those individuals. In addition, OSFI Guideline B-8 advises FRFIs to ensure that written AML/ATF training programs are developed and maintained. Appropriate training should be considered for the Board, Senior Management, employees, agents and any other persons who may be responsible for control activity, outcomes or oversight, or who are authorized to act on the Company's behalf, pursuant to the PCMLTFR.

The PCMLTFR (s.71 (1) (e)) oblige all REs to institute and document a review of their policies and procedures, the risk assessment and the training program for the purpose of testing effectiveness. That review must be carried out every two years by an internal or external auditor of the RE, or by the RE itself, if it has no auditor. OSFI Guideline B-8 amplifies the requirement in a number of ways and also sets out an expected standard of self-assessment of controls applicable to FRFIs.

Criterion 18.2— Measures which came into effect in June 2015 expanded section 9.7 of the PCMLTFA to cover foreign branches as well as subsidiaries. The effect was to require FIs, securities dealers and life insurance companies to implement policies and procedures for CDD, record-keeping and compliance programs that are consistent with Canadian requirements and apply across a financial group.

A new s.9.8(1) of the Act introduced requirements for REs to have policies and procedures in place for how they will share information with affiliates for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. This provision is sufficiently widely drawn to cover the kind of customer, account and transaction information stipulated in the FATF standard. There are no prohibitions in either the PCMLTFA or PIPEDA on sharing of information, including STRs, within financial groups, domestically or cross-border.

The new law did not cover safeguards on the confidentiality and use of information exchanged. However, the necessary safeguards already exist under PIPEDA (s.5 and Schedule 1), which apply equally to client information received from a branch or subsidiary under the PCMLTFA.

Criterion 18.3— Under newly amended s.9.7(4) of the PCMLTFA, when local laws would prohibit a foreign branch or foreign subsidiary from implementing policies that are consistent with Canadian AML/ATF requirements, the RE must advise FINTRAC and their principal regulator. (In the case of FRFIs, this is OSFI; for provincially regulated FIs, the relevant provincial supervisor).

Weighting and Conclusion

There is a remaining deficiency regarding the internal controls aspect of R.18.

Canada is largely compliant with R.18.

Recommendation 19 – Higher-risk countries

In the 2008 MER, Canada was rated PC with R.21, because there were no general enforceable requirement for FIs to give special attention to transactions or business relationships connected with persons from higher-risk countries, no measures advising of other countries with AML/CFT weaknesses, and no requirement to examine the background and purpose of transactions and to document findings. The FATF standard remains broadly the same, but there have been major changes in Canada since 2008.

Criterion 19.1 and 19.2— Part 1.1 of the PCMLTFA, which entered into force in June 2014, introduced two new authorities for the Minister of Finance: (i) the authority to issue directives requiring REs to apply necessary measures to safeguard the integrity of Canada's financial system in respect of transactions with designated foreign jurisdictions and entities. The measures contemplated included CDD, monitoring and reporting of any financial transaction to FINTRAC; (ii) the authority to recommend that the Governor-in-Council issue regulations limiting or prohibiting REs from entering into financial transactions with designated foreign jurisdictions and entities. These authorities enable Canada to take targeted, legally enforceable, graduated and proportionate financial countermeasures against jurisdictions or foreign entities with insufficient or ineffective AML/ATF controls. These measures can be taken in response to a call by an international organization, such as the FATF, or unilaterally. The Minister has not issued any countermeasures under Part 1.1; however, OSFI and FINTRAC have regularly drawn the attention of FRFIs and REs to the FATF calls on members, and have issued regular guidance in Notices and Advisories following each FATF meeting. OSFI has issued prudential supervisory measures against FRFIs it believes have not implemented FATF expectations (PCMLTA (s.11.42) and PCMLTFR (s.71.1)).

Criterion 19.3— Risk assessments on jurisdictions with AML/ATF weaknesses are conducted through the IFAC Under s.11.42(3) of the Act, the Minister's decision to issue a Directive may require the Director of FINTRAC to inform all REs. Additional guidance is provided through FINTRAC advisories and OSFI notices, available online, encouraging enhanced CDD with respect to clients and beneficiaries involved in transactions with high-risk jurisdictions.

Weighting and Conclusion:

Canada is compliant with R.19.

Recommendation 20 – Reporting of suspicious transaction

In the 2008 MER, Canada was rated LC with R.13 and SR. IV because some FIs (e.g. financial leasing, factoring and finance companies) were not covered by the obligation to report and there was no requirement to report attempted transactions. Some improvements have been made since then.

Criterion 20.1— PCMLTFA, s.7 requires REs to report to FINTRAC every financial transaction that occurs, or that is attempted, in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML or TF offense. The scope of the PCMLTFA still excludes certain sectors (financial leasing, finance and factoring companies), but this represents an ongoing minor deficiency. ML is defined by reference to CC, s.462.31(1), which, in turn, is defined in CC, s.462.31(1) to mean any offense that may be prosecuted as an indictable offense under this or any other Act of Parliament, other than an indictable offense prescribed by regulation. As described under c.3.2, ML now applies to a range of offenses in each FATF designated category of predicate offenses, including tax evasion.

Suspicious transactions must be reported "within 30 days" of detection of a fact that constitutes reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of an ML offense or a TF offense. (PCMLTF Suspicious Transaction Reporting Regulations, s.9(2)).This does not meet the standard of reporting "promptly."

Criterion 20.2— Attempted transactions are now covered by the reporting requirement.

Weighting and Conclusion

The reporting requirement covers several, but not all elements, of the standard.

Canada is partially compliant with R.20.

Recommendation 21 – Tipping-off and confidentiality

In the 2008 MER, Canada was rated C with R.14.

Criterion 21.1— The PCMLTFA (s.10) states that no criminal or civil proceedings lie against a person or an entity for making an STR in good faith or for providing FINTRAC with information about suspicions of ML or TF activities. However, the requirement does not explicitly extend to reporting related to ML predicate offenses.

Criterion 21.2— PCMLTFA s.8 specifies that no person or entity can disclose that they have made an STR, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. The law does not, however, cover a situation where a person or entity is in the process of filing a STR but has not yet done so. Neither does the legal obligation explicitly extend to reporting related to ML predicate offenses.

Weighting and Conclusion

The tipping off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses.

Canada is largely compliant with R.21.

Designated Non-Financial Businesses and Professions (DNFBPs)

Since the 2008 MER, Canada has extended the AML/CFT requirements to BC Notaries and DPMS. The following DNFBPs are now subject to AML/CFT obligations: land-based casinos, accountants (defined as chartered accountant, certified general accountant, certified management accountant)[110] and accounting firms, British Columbia Notaries Public and Notary Corporations (hereinafter referred to as BC Notaries), real estate brokers or sales representatives, dealers in precious metals and stones (hereinafter DPMS) and certain trust companies, which fall under PCMLTFA, s.5 (e). Legal counsel and legal firms are covered as obliged AML/CFT entities, pursuant to PCMLTR, s.33.3, but, on 13 February 2015,[111] the Supreme Court of Canada concluded that the AML/CFT provisions are inoperative, as they are unconstitutional, for lawyers and law firms in Canada. Canada extended the AML/CFT regime to real estate developers when, under certain conditions, they sell to the public real estate (PCMLTFR, s.39.5). Notaries in provinces other than Québec and British Columbia are restricted to certifying affidavits under oath, and document certification. These notaries do not conduct any financial transactions and the transfer of property is done exclusively through lawyers in these provinces (see 2008 MER, para. 150). TCSPs are not a distinct category under the PCMLTFA and PCMLTFR. The definition of casino (PCMLTFR, s.1(1)), which excludes registered charities authorized to perform business temporarily, provides an unclear exemption.[112]

All gambling is illegal,[113] unless specifically exempted under CC, s.207. Several provinces (British Columbia, Quebec, Manitoba Nova Scotia, Prince Edward Island, New Brunswick and Newfoundland) have introduced online gambling through an extensive interpretation of the notion of "lottery scheme" allowed to them under CC, s.207(4)(c), which includes games operated through a computer. When these provinces introduced internet gambling, FINTRAC sent them a letter to inform them that

[110] PCMLTFR, Section 1. (2).

[111] The Supreme Court of Canada on 13 February 2015 has concluded that the search provisions of the Act infringe Section 8 of the Canadian Charter of Rights and Freedoms, while the information gathering and retention provisions, in combination with the search provisions, infringe Section 7 of the Charter Canada (Attorney General) v. Federation of Law Societies of Canada, 2015 SCC 7.

[112] There is no definition of "charitable purposes" and the notion of "temporary" business, does not give an exact timeframe, making unclear the reference to "not more than two consecutive days at a time," without fixing any further limit per week or per year. The exemption involving registered charities is to avoid duplication in the AML/CFT regime, as the Provincial Authority or its designate are RE of FINTRAC. Nevertheless, taking into account the possible operational models of casinos operating in Canada, the current definition of casino and the resulting AML/CFT requirements lack clarity in addressing the respective AML/CFT responsibilities of the different persons or entities that could be simultaneously involved in the business of the same casino (Crown corporations or regulators branches involved in the conduct and management of lotteries schemes, charitable organizations, First Nation organizations, casino's service providers).

[113] CC, Section 206 (1).

they were considered subject to AML/CFT obligations. Subsequently, these casinos started sending to FINTRAC Casino Disbursement Reports (for example, FINTRAC has received 988 such reports in the last 24 months). Nevertheless, the amendment to the definition of casinos that makes reference to online gambling operators is not yet entered into force.[114]

There are also land-based gaming and on line gambling[115] sites actually operating within Quebec, whose legal status is unclear which are not supervised by the province and which are not subject to AML/CFT obligations. These activities are authorized by the Kahnawake Gaming Commission operating on the basis of an asserted jurisdiction by the Mohawks over their territory. They are considered illegal by the authorities. Offshore gambling sites are deemed to be illegal as each casino must be licensed by a Canadian province. The authorities clarified that these activities are a matter for law enforcement to oversee.

Cruise ships that offer gambling facilities in Canadian waters are not obliged entities for AML/CFT purposes. (See 2008 MER, para. 1186-1187). Lottery schemes cannot be operated within five nautical miles of a Canadian port at which the ship calls (s.207.1 of the CC). Of note, there are no Canadian cruise ships. The exemption of cruise ship casinos is based on a proven low risk.

Trust and company services are provided by trust companies, legal counsels, legal firms and accountants—the PCMLTFA therefore does not identify TCSPs separately. Twenty-two trust companies (covered by a provincial Act, falling under of PCMLTFA, s.5(e)) are subject to AML/CFT obligations, but lawyers and accountants are not, despite the high vulnerability rating highlighted in the NRA.[116]

Recommendation 22 – DNFBPs: Customer due diligence

In the 2008 MER, Canada was rated NC with these requirements due to deficiencies in the scope of DNFBPs covered and in CDD and record-keeping requirements. Since then, Canada has extended the scope of the AML/CFT requirements to BC Notaries and DPMS and addressed some deficiencies in CDD requirements applicable to DNFBPs.[117]

Criterion 22.1— Scope issue: Internet casinos, TCSPs are not covered and the relevant provisions are inoperative with respect to legal counsels, legal firms and Quebec notaries (PCMLTFR, ss.33.3,

[114] Steps are being taken in this respect. Bill C-31 introduced legislative amendments to PCMLTFA s.5 k 1, which will come into force once the regulations are finalized, aimed at establishing AML/CFT obligations for online gambling conducted and managed by the provinces and covering those lottery schemes other than bingo and the sale of lottery tickets that are conducted and managed by provinces in accordance with CC, s.207(1)(a). These amendments will also extend the notion of relevant business to include other electronic devices similar to slot machines (such as video lottery terminals, currently excluded from the AML/CFT regime) but establishing a relevant threshold of "more than 50 machines per establishment" (PCMLTFA, s.5(k)(ii)).

[115] Online gaming operators that are licensed by the Commission must be hosted at Mohawk Internet Technologies, a data centre, located within the Mohawk Territory of Kahnawake.

[116] NRA, p.32.

[117] In particular, introducing the obligation to collect information on the purpose and intended nature of the business relationship and ongoing due diligence, extending the circumstances in which CDD is required, providing for enhanced measures in higher risk scenarios, excluding the exemption regime in case of suspicion.

33.4, 33.5, 59.4, 59.41, 59.4). As regards accountants and BC notaries, not all the relevant activities under the criterion are taken into account.

DNFBPs[118] are not required to obtain, take reasonable measures to confirm, and keep records of the information about the beneficial ownership of legal persons and legal arrangements, nor as to understand the ownership and control structure of the latter. DNFBPs are only required to confirm the existence of and ascertain the name and address of every corporation or other entity on whose behalf a transaction is being undertaken, and in the case of a corporation the names of its directors.[119] The rule of "third party determination" (PCMLTFR, s.8) is limited to individuals and is not applied to all relevant circumstances when CDD is required under the criterion. DNFBPs are not explicitly required to establish that the person purporting to act on behalf of the customer is so authorized. There are additional deficiencies for each relevant category. Casinos can perform a large variety of financial services, including wire transfers (see 2008 MER, para. 138). The following measures for ascertaining identity are carried out in line with the following threshold: on account opening (no threshold), when dealing with EFTs (CAD 1 000) and, dealing with foreign exchange or extension of credit (CAD 3 000).[120] The CAD 10 000 thresholds for ascertaining identity for cash financial transactions and casinos disbursement[121] are higher than the FATF standard. Not all the range of non-cash occasional transactions are covered: in particular, the purchase of chips through checks, credit, and debit cards, as well as prepaid cards are not captured. The redemption of "tickets" under PCMLTFR, s.42(1)(a) is not included, even if some kind of tickets (TITO tickets)[122] have been detected by FINTRAC in typologies of ML. There are no enforceable provisions requiring casinos to include beneficiary information in wire transfers, and no obligation for all REs to ascertain the identity of authorized signers (PCMLTFR, ss.54(1)(a) and 62(1)(a)). As regards, accountants and BC Notaries, not all the relevant activities under the criterion are included. In particular, no requirement is provided in relation to activities related to organization of contributions for the creation, operation and management of companies, legal persons and arrangements, and the scope of "purchasing or selling" securities, properties and assets is more limited than the notion of "management" included under the criterion. The definition of accountant (PCMLTFR, s.1(1) does not include "Chartered Professional Accountant."[123] In a real estate transaction, when the purchaser and the vendor are represented by a different real estate broker, each party to the transaction is identified by their own real estate broker. Real estate agents, in case of unrepresented party are required to take reasonable measures only to ascertain the identity of the party (PCMLTFR, s.59.2 (2, 3, and 4)), rather than applying reasonable risk-based CDD measures to the party that is not their client. DPMS are covered as required by the standards when they engage in the purchase or sale of

[118] With the exception of legal counsel and legal firms for which however the provisions are inoperative (Section 11.1 (1) of the PCMLTFR.
[119] PMCLTFR 59.1(b) & (c), 59.2(1)(b) &(c), 59.3 (b) & (c), 59.5 (b) & (c), 60 (e) &(f)
[120] PCMLTFR, Sections 60(a), 60(b)(iv), 60(b)(iii), 60(b)(ii)
[121] PCMLTFR, Sections 53 and 60(b)(i).
[122] Ticket In Ticket Out (TITO) "tickets" are also an increasingly popular casino value instrument used in many Canadian casinos (FINTRAC, ML Typologies and Trends in Canadian Casino, Nov. 2009, p.8).
[123] The unified new professional designation replaces the former three (Chartered Accountants, Certified General Accountants and Certified Management Accountants), and it is currently completed in several provinces (Quebec, New Brunswick, Saskatchewan, Newfoundland and Labrador). Further work is underway and expected to be included in forthcoming regulatory amendments.

precious metals, precious stones or jewellery in an amount of CAD 10 000 or more in a single transaction, other than those pertaining to manufacturing jewellery, extracting precious metals or precious stones from a mine, or cutting, or polishing precious stones..

Criterion 22.2— Scope issue: see 22.1. The circumstances under which relevant DNFBPs have to keep records do not fully match the list of activities required under R.10 (see 22.1). Furthermore, a non-account business relationship is established when transactions are performed in respect of which obliged entities are required to ascertain the identity of the person, rather than being based on a mere element of duration. The said definition entails that, apart from the case of suspicion, the record keeping requirements on a business relationship arise only when the prescribed thresholds for the transactions are reached. The deficiencies identified in R.11 apply also to DNFBPs.

Criteria 22.3, 22.4 and 22.5— There are no requirements for DNFBPs to comply with specific provisions covering PEPs, new technologies and reliance on third parties.

Weighting and Conclusion:

Canada is non-compliant with R.22.

Recommendation 23 – DNFBPs: Other measures

In its 2008 MER, Canada was rated NC with these requirements, due to the limited scope of DNFBPs included as well as to deficiencies with the underlying recommendations and to concern about the effectiveness of the STR regime in these sectors. Canada has since extended the scope of DNFBPs to some extent (See R.22), included attempted transactions in the STR regime and empowered the Department of Finance to take financial countermeasures with respect to higher-risk countries.

Criterion 23.1— PCMLTFA, s.7 (transaction where reasonable grounds to suspect) does not apply to all relevant categories of DNFBPs, nor to all relevant activities of accountants and BC Notaries as described under R.22.[124] The analysis in relation to R.20 above equally applies to reporting DNFPBs. There are no key substantive differences between the reporting regime for FIs and DNFBPs. FINTRAC Guidelines no. 2 (Suspicious Transactions) includes industry-specific indicators.

Criterion 23.2— Scope issue: see 23.1. Accountants, accounting firms, legal counsels and legal firms, BC Notaries, real estate agents and developers, land-based casinos, DPMS are all required to establish and implement a compliance program (PCMLTFA, s.9.6 (1); PCMLTFR, s.71(1)). While compliance procedures must be approved by a senior officer, PCMLTFA, ss.9.6 and PCMLTFR, s.71(1)(a) do not stipulate that the designation of the compliance officer shall be at the management level. DNFBPs, other than land-based casinos, are not required to have adequate screening procedures to ensure high standards when hiring employees. Also, there is no specific requirement that review of the compliance regime be performed by an independent audit function, as it can also be carried out through a procedure of self-assessment (PCMLTFR, s.71(1)(e)).

[124] Under PCMLTA, Section 5, Part 1 of the Act (including the STRs obligations) applies while carrying out the activities described under the regulations.

Criterion 23.3— Scope issue: see 23.1. See R.19 for a description of this requirement.

Criterion 23.4— Scope issue: see 23.1. The requirements for DNFBPs are the same as those applied to FIs under R.21.

Weighting and Conclusion:

Canada is non-compliant with R.23.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Canada was rated NC with former R.33 based on concerns over a lack of transparency for legal entities, the availability of bearer shares without adequate safeguards against misuse, and a lack of powers by the authorities to ensure the existence of adequate, accurate and timely beneficial ownership information for legal entities. Since 2008, the obligations for FIs to obtain information on the identity of beneficial owners and the CRA's ability to disseminate information on legal entities to the RCMP have been strengthened.

Canada's corporate legal framework consists of federal, provincial and territorial laws: (i) Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). Federally incorporated entities are entitled to operate throughout Canada but in addition to registration at the federal level, are also subject to registration with the province or territory in which they carry out business. (ii) Each of the thirteen territories and provinces regulates the types of legal entities that can be established at the local level. Eight provinces and territories have enacted specific laws that provide for the establishment of corporations and NPOs. Prince Edward Island, Newfoundland and Labrador, Alberta, Manitoba, Quebec, and New Brunswick do not have specific NPO legislation in place but regulate NPOs through the relevant provincial company law.

Legal entities incorporated at the provincial or territorial level enjoy business name protection only in the province or territory where they are incorporated. To operate in another province in Canada, they have to register with that province but there is no guarantee that they will be able to use their corporate name (e.g. a business entity with the same name may already be operating in that province). Federal, provincial and territorial corporate entities may carry out business internationally if the foreign country recognizes the type of corporate entity.

In addition to legal entities, all provinces provide for the establishment of general and limited partnerships pursuant to common law rules; and all provinces, but Yukon, Prince Edward Island and Nunavut have passed statutes to provide for the establishment of limited liability partnerships. Partnerships are not subject to registration as part of the establishment process, but most provinces and territories require registration of businesses before a partnership may operate there. Business registration obligations under provincial and territorial laws also apply to foreign entities wishing to carry out business in Canada.

Criterion 24.1— *Federal legal persons:* Innovation, Science and Economic Development Canada (ISED), formerly Industry Canada, provides a comprehensive overview and comparison on its internet homepage of the various legal entities available and their forms and basic features. All legal entities established at the federal level are subject to registration. Given that corporations are by far the most utilized type of legal entity in Canada, particular emphasis is put on information pertaining to federal corporations under CBCA and their incorporation and registration process, which can be initiated online or by sending all required documents to the competent registrar via email, fax, or mail. [125] ISED also offers a search tool, which makes some basic information of federal companies publicly available. The search function also indicates the legislation the corporation is incorporated under, which in turn clarifies basic regulating powers. *Provincial legal persons:* Similar information and services are provided through the homepages of all provincial governments except that of New Brunswick. The relevant web links are easy to find through ISED's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity or to register a corporation. *Partnerships and foreign entities:* Partnerships and foreign entities operating in any of Canada's provinces or territories are subject to registration at the provincial level. The Canada Business Network maintains a homepage that provides links to the various provincial and territorial business registries.

Criterion 24.2— The NRA identified privately held corporations as being highly vulnerable to misuse for ML/TF purposes. The conclusion was reached based on the understanding that such corporations can easily be established and be used to conceal beneficial ownership. The risk assessment determines the inherent risks involved with legal persons based on factors such as the products and services offered by legal entities, the types of persons that may establish or control a legal person, the possible geographic reach of a Canadian legal entity, and taking into account FINTRAC statistics on typologies involving legal entities in Canada.

Basic Information

Criterion 24.3— Both federal and provincial corporations, NPOs with legal personality and cooperatives are established through incorporation by the relevant incorporating department or agency. *Federal legal persons:* On the federal level, ISED, as part of the incorporation and annual filing process, collects and publishes information comprising the corporation's name, type, status, corporation number, registered office address in Canada, name and address of all directors, and governing legislation. The regulating powers for federal corporations are set out in the legislation or in the corporation's articles, which are approved by the Director appointed under the relevant Act. *Provincial legal persons:* Company information including the corporate name, type, status, registered office in Canada, and name and address of directors is collected through the same process as on the federal level, which is through annual filing procedures. *Partnerships and foreign entities:* Business registration requirements vary between the different provinces and territories, but usually require the provision of the name, registered office, mailing address, place of business in the province/territory, the date and jurisdiction of incorporation (for extraterritorial companies) or type

[125] www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.

of partnership, the name and address of directors or partners and a copy of the partnership contract or the incorporation certificate or other proof of existence. Partnerships not carrying out any business in Canada are not required to register as part of the establishment process.

Criterion 24.4— Record-keeping obligations extend to the corporation's articles and by-laws and any amendments thereof, of minutes of shareholder meetings and resolutions, share registers, accounting records, and minutes of director meetings and resolutions. Pursuant to CBCA, s.50, companies must also keep a share register that indicates the names and address of each shareholder, the number and class of shares held, as well as the date and particulars of issuance and transfer for each share. Similar provisions are set out in provincial legislation. Federal as well as provincial companies are required to keep records of basic information either in a location in Canada or at a place outside Canada, provided the records are available for inspection by means of computer technology at the registered office or another place in Canada and the corporation provides the technical assistance needed to inspect such records (CBCA, s.20). There is no legal requirement to inform the incorporating department or agency, or where applicable, the company register of the location at which such records are being kept.

Criterion 24.5— Under CBCA, s.19 (4) federal corporations are required to inform the Director appointed under the CBCA within 15 days of any change of address of the registered office. Changes in legal form, name or status as well as amendments to the articles of incorporation take effect only after they have been filed with the Director. More or less the same updating requirements are especially provided for under provincial legislation, except in Quebec and Nova Scotia.[126] In Nova Scotia, the updating requirement applies but changes to the registered office have to be filed within 28 days and there is only a general obligation to notify the Registrar "from time to time" of any changes among its directors, officers, or managers. Directors, shareholders and creditors have access to these documents and are permitted at all times to check their accuracy. However, no formal mechanism is in place to ensure that shareholder registers are accurate. For partnerships and extraterritorial corporations, some provinces and territories impose an annual filing obligation, others require renewal of the license and updating of relevant information on a multi-year basis.

Beneficial Ownership Information

Criterion 24.6— Canada uses existing information to determine a legal entity's beneficial ownership, if and as needed, including as follows:

(i) FIs providing financial services to legal entities, partnerships or foreign companies. Since 2014, obligations under the PCMLTFA for FIs to obtain ownership information of customers or beneficiaries that are legal entities have been strengthened. Prior to 2014 FIs identified beneficial owners of legal entities mostly based on a declaration of the customer. For those companies established prior to 2014, it is, thus, questionable whether this measure did indeed result in the availability of accurate and updated beneficial ownership information. Ongoing CDD obligation under the PCMLTFA have resulted in BO information becoming available for a number of companies that opened bank accounts in Canada prior to 2014, but most FIs interviewed by the assessors

[126] For example Section 2 Ontario Corporations Information Act; Article 20 Alberta Business Corporation Act; Article 19 Nova Scotia Companies Act.

indicated that the ongoing CDD process has not yet been completed for all legal entities. For some DNFBPs as outlined in R.22, certain limited CDD obligations apply as discussed under R.22 but those do not amount to a comprehensive requirement to identify and take reasonable measures to verify beneficial ownership information and the obligations also are inoperative with regards to lawyers.

(ii) The federal and provincial company registries record some basic information as discussed above, but do not generally collect information on beneficial owners. Verification mechanisms for registered information are not in place. The CRA as part of its general obligations, collects information on legal entities that file tax returns. As indicated in the 2008 MER, however, this information generally does not comprise beneficial ownership information. Furthermore, not all legal entities in Canada file tax returns with the CRA; and

(iii) Legal entities themselves are required to collect certain information on holders of shares but no mechanisms are in place to ensure that the registered information is accurate.

(iv) For public companies listed on the stock exchange, disclosure requirements exist for shareholders with direct or indirect control over more than 10% of the company's voting rights.

As outlined under R.9 and 31, LEAs have adequate powers to obtain information from FIs, DNFBPs and any other types of companies and the CRA. However, the process of linking a specific FI with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. In sum, while some of the information collection mechanisms have been strengthened since 2008, deficiencies with regards to the collection and availability of full and updated beneficial ownership information remain and timely access by law enforcement authorities to such information is not guaranteed in all cases.

Criterion 24.7— As indicated under criterion 24.6, FIs are required to collect and update beneficial ownership information. The registries, the CRA and legal entities themselves are not required to ensure that accurate and updated beneficial ownership information is collected.

Criterion 24.8— Companies on both federal and provincial levels are obliged to grant the Director under the relevant Act access to certain information, including in relation to company share registers (Article 21 CBCA). There is no legal obligation on corporations or partnerships to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or for authorizing a DNFBP in Canada to provide such information to the authorities.

Criterion 24.9— Legal entities are required to maintain accounting records for six years, but not from the date of dissolution, but of the financial year to which they relate. In addition, pursuant to s.69 of the PCMLFTR FIs/some DNFBPs holding information on legal entities must keep that information for five years from termination of the business relationship or completion of the transaction. The Director retains corporate records submitted under the CBCA for a period of six years, except for articles and certificates which are kept indefinitely. In addition, s.225 of the CBCA requires a person who has been granted custody of the documents or records of a dissolved corporation to produce those records for six years following the date of its dissolution or such

shorter period as ordered by a court. Non-financial documents or records must be kept by the corporation until the corporation is dissolved; and then for another six years or less period as ordered by a court. The CRA, in partnership with the National Archivist of Canada, retains documents obtained or created by the CRA for various periods of time depending on the nature of the information. In relation to questions of beneficial ownership, the relevant retention periods are five to ten years, in some instances indefinitely.

Other Requirements

Criterion 24.10— Some basic company information is publicly available on various federal and provincial government websites and is therefore available to the authorities in a timely fashion. For information that is not publicly available, a wide range of law enforcement powers are available to obtain beneficial ownership information, including search warrants, using informants, surveillance techniques, wiretaps and production orders, and public sources (e.g.: law enforcement databases, city databases, corporate companies, civil proceedings, bankruptcy records, divorce records, civil judgments, land titles and purchase, building permits, credit bureau, insurance companies, liquor and gambling licenses, death records, inheritance, shipping registers, federal aviation, trash searches, automobile dealerships) and private source information searches. To be able to compel an FI to produce records pertaining to the control or ownership structure of a legal entity or legal arrangement, LEAs must first establish the link between a legal entity and a specific FI. Several tools are available to this effect (e.g.: grid search request to all D-SIBs to establish if they count the target person amongst their customers, VIRs to FINTRAC, requests to Equifax, mortgage and loan checks , consultations of NEPS to obtain an economic profile of an individual or private or public company). Investigative techniques may also be used (e.g. informants, witnesses, wiretaps). The RCMP may also request information from the CRA once charges have been laid in a criminal case, and on the basis of a judicial authorization. Prior to the prosecution stage, a tax order under the CC can be obtained for the RCMP to receive tax information from the CRA on a specific entity. Since 2014, the CRA may also share information with the RCMP on its own motion in cases where the CRA considers that there are reasonable grounds to believe that the information in its possession would provide evidence of listed serious offenses, including ML, bribery, drug trafficking and TF. In relation to tax crimes, the CRA CID may also obtain information. The relevant Director under each corporate statute—in the case of the CBCA the Director of Corporations Canada— also has the authority to inspect a corporation's records. Once it is established that a specific RE maintains a business relationship with a legal entity, LEAs may obtain a court order and deploy the measures available under criminal procedures to obtain, compel the production of, or seize relevant information—including beneficial ownership information—from any person, as discussed under R.31.

Criterion 24.11— Bearer shares are permitted both under the CBCA and several provincial company laws (for companies limited by shares).[127] While the CBCA generally requires the issuance of shares to be in registered form, the CBCA also makes provision for the issuance of certain types of shares in bearer form. In the absence of an express prohibition, the CBCA, therefore, still leaves some

[127] Quebec, Prince Edward Island, North-Western Territories and Nunavut allow for the issuance of registered shares only.

room for the issuance of bearer shares and no safeguards are in place to ensure that such shares are not being misused for ML or TF purposes.

Criterion 24.12— The CBCA requires corporations to keep shareholder registers in relation to registered shares, whereby the term "holder" of a security is defined as "a person in possession of a security issued or endorsed to that person." Under Part XIII of the CBCA, the holder of a share is permitted to vote at a meeting using someone else to represent them. The CBCA permits a registered shareholder to authorize another person to vote on their behalf. The proxy form itself lists the registered shareholder and the name of the "proxyholder" or person acting on their behalf. The proxy is recorded at the shareholder meeting, which provides transparency in respect of the identity of these individuals. However, the outlined arrangement still allows for nominee shareholding arrangements if the relevant shares are not voted. CBCA, s.147 permits, for example, securities brokers, FIs, trustees, or any nominees of such persons or entities to hold securities on behalf of another person who is not the registered holder but beneficial owner of that security. Similar provisions are found in provincial legislation such as, for example, Alberta Business Corporations Act, s.153 and Quebec's Business Corporations Act, s.2. Corporate directors are not permitted under the CBCA and provincial statutes. Nominee director arrangements in form of one natural person formally acting as director on behalf of another person may, however, still exist. Nominees (whether shareholders or directors) are not required to be licensed, or disclose their status, or to maintain information on or disclose the identity of their nominator. However, under the PCMLFTR, legal entities when opening a bank account, are required to provide details on the natural person that owns or controls a legal entity, which would include the nominating shareholder or director. For publicly listed companies, the risk of abuse of nominee shares is properly mitigated based on rigid reporting obligations for change of shares in excess of 10%. In sum, for companies other than those listed on the stock exchange, there are insufficient mechanisms in place to ensure that nominee shareholders are not misused for ML or TF purposes.

Criterion 24.13— Under the CBCA and provincial company laws violation of a company's disclosure, filing or record-keeping obligations may be fined with up to CAD 5 000 and/or imprisonment for up to six months in case of a violation by a natural person acting on behalf of the company. FIs and those DNFBPs covered under the law are subject to criminal (imprisonment for up to six months and/or a fine of up to CAD 50 000) as well as administrative sanctions if they fail to comply with their identification obligations with regards to legal entities (PCMLTFA, ss.73.1 and 74). In addition, officers, directors and employees of FIs and DNFBPs may be subject to sanctions regardless of whether the FI or DNFBP itself was prosecuted or convicted, as discussed under R.35. In summary, the statutory sanctions available are proportionate and dissuasive.

Criterion 24.14— Some basic information in the federal and provincial company registers is publicly available and can be directly accessed by foreign authorities. For other information, the powers and mechanisms described under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 apply.

Criterion 24.15— Information on the quality of assistance received from other countries in the context of MLA and in response to ownership information requests is kept by the International Assistance Group (IAG) at the Department of Justice. The IAG maintains a copy of the requests made,

the follow-up that takes place with regards to each request, and keeps copies of all documents and information provided in response to the request. When forwarding the relevant information to the requesting agency, the IAG inquires with that agency, whether the request should be considered fulfilled. The authorities stated that the information collected by IAG suggests that the assistance received is generally adequate, although the result vary according to the particular component of basic/beneficial ownership sought.

Weighting and Conclusion

Serious gaps remain under criterion 6 with respect to the availability of beneficial ownership information for legal entities and partnerships.

Canada is partially compliant with R.24.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Canada was rated PC with former R.34 as the obligations to obtain, verify, and retain beneficial ownership information was considered to be inadequate. Since then, changes have been introduced to the PCMLTFR to strengthen FI obligations with regards to the identification and verification of beneficial ownership information for legal arrangements (whether created in Canada or elsewhere). In addition, the CRA's power to disseminate tax information to LEAs have been enhanced, taxpayer information can be shared at the discretion of the CRA if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC s. 462.31. However, it is not clear for how many of the millions of trusts estimated to exist under Canadian law beneficial ownership information is available and access to such information is in any case difficult to obtain as there is no requirement for trustees to be licensed or registered.

Canada allows for the establishment of common law trusts as well as civil law fiducie (in Quebec). There is no general registration requirement for trusts, and trustees may but do not have to be licensed individuals or entities under the PCMLTFA. No specific statutes regulate the operation of foreign trusts in Canada, or require the registration of such foreign trusts.

Criterion 25.1— In the case of professional trustees, the customer due-diligence obligations vary depending on the trustee's profession: TCSPs are not subject to the general identification and verification obligations under the PCMLTFA as outlined under R.22. The CDD obligations applied to accountants have limitations as discussed in R.22. The requirements for lawyers are inoperative as a result of a Supreme Court decision. Trustees other than professional trustees are not subject to any statutory customer due diligence or record-keeping obligations.

Criterion 25.2— TCSPs are not covered under the scope of the PCMLFTR. Accountants are subject to basic ongoing CDD measures that do not amount to a comprehensive obligation to obtain and take reasonable measure to verify the identity of beneficial owners. Other trustees are not subject to comprehensive CDD or record-keeping requirements, as indicated under criterion 1.

Criterion 25.3— There is no obligation on trustees to disclose their status without being prompted, but under the PCMLFTR, FIs are required to determine whether a customer is acting on behalf of someone else, to establish the control and ownership structure of legal entities they are providing services to, and to obtain the names and addresses of all trustees, known beneficiaries and settlors.

Criterion 25.4— There is no prohibition under Canadian law for trustees to provide trust-related information to competent authorities, except in the case of lawyers where legal privilege may prevent authorities from accessing such information.

Criterion 25.5— Where there are suspicions of a crime, LEAs may deploy a wide range of investigative measures to obtain, compel the production of, or seize relevant information from any trustee, whether subject to the PCMLFTR or not. The extent to which the information available would include beneficial ownership information and information on the trust assets is unclear, as apart from the PCMLFTR, no legal requirements to maintain such information exist. Furthermore, linking a specific FI or DNFBP with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. With regards to FIs and accountants and trust companies acting as trustees, LEAs may also obtain information available to FINTRAC in its capacity as FIU through a request for voluntary information records. FINTRACs powers to access such information are, however, limited as outlined under criterion 29.2. In situations where a trust owes taxes and is required to file income tax returns, the CRA also has access to certain trust information, including the name and type of the trust and certain financial information on the trust. Information available to the CRA typically includes beneficiary, but not beneficial ownership information. The CRA may share taxpayer information upon request by LEAs either based on a court order or after criminal charges have been laid; or upon its own initiative if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC, s462.31.

Criterion 25.6— The authorities may exchange information on trusts with foreign counterparts based on the procedures outlined under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 and 11. LEAs have wide powers to exchange information with foreign counterpart. FINTRAC as well as the CRA may also share information with foreign counterparts as part of their respective functions. Investigative measures to obtain beneficial ownership can be taken upon foreign request.

Criterion 25.7— Under the PCMLFTR, failure to comply with the identification, verification or record-keeping requirements is subject to a range of criminal and administrative sanctions (see write-up under R.35 for more details). Trustees other than accountants are not subject to the AML/CFT framework. Violations of the principles of a trustees' breach of fiduciary duties may give rise to claims by the beneficiary and legal liability of the trustee based on these claims. However, in the absence of a specific obligation to collect and maintain beneficial ownership or general trust information there are also no sanctions available to authorities for a failure of the trustee to do so.

Criterion 25.8— For accountants, a the PCMLFTR sanctions may be applied by supervisory authorities as discussed under criterion 27.4. For other trustees, however, no sanctions are in place in the case of a failure to grant competent authorities timely access to trust related information.

Weighting and Conclusion:

Canada is non-compliant with R.25.

Recommendation 26 – Regulation and supervision of financial institutions

In the 2008 MER, Canada was rated PC with former R.23 due to the exclusion from the AML/CFT regime of certain sectors without proper risk assessments, an unequal level of supervision of AML/CFT compliance, lack of a registration regime for MSBs and concerns around fit and proper screening requirements. Canada made significant progress since then.

Criterion 26.1— FINTRAC is the AML/CFT supervisor for all REs subject to the PCMLTFA. It is assisted in the regulation and supervision of FIs by other federal and provincial regulators that are responsible for prudential and conduct supervision. However, ultimate responsibility for supervision and sanctioning under the PCMLTFA remains with FINTRAC. It is estimated that 80% of Canada's financial sector market is controlled by FRFIs. FRFIs are under the supervision of OSFI and include six large conglomerates (DSIBs) that hold a substantial share of the financial sector and other financial entities such as banks, insurance companies, cooperative credit and retail associations, trust companies and loan companies. OSFI's powers are mandated under the OSFI Act and governing legislation for the various financial sectors such as the *Bank Act*, *Trust and Loan Companies Act, Insurance Companies Act* and *Cooperative Credit Associations Act*. Non-FRFIs (e.g. credit unions) are regulated and supervised by provincial regulators under provincial statute.

AML/CFT supervisory functions are concentrated in FINTRAC and have not been delegated to primary regulators in Canada. At the federal level, OSFI and FINTRAC concurrently assess FRFI's for compliance with AML/CFT compliance obligations and are moving to a joint examination process (see further details below). At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other supervisors and has signed 17 MOUs with supervisors in relation to non-FRFIs. FINTRAC is authorized to share information with primary regulators at national and provincial levels relating to AML/CFT to monitor compliance with the PCMLTFA, and such regulators are also authorized to share information with FINTRAC.

Market Entry

Criterion 26.2— Federal and provincial authorities are the primary regulators of FIs with responsibility for prudential and conduct supervision including the licensing and registration of market entrants. FINTRAC is responsible for the registration and supervision of MSBs (along with AMF for MSBs operating in Quebec).

Market entry rules for FRFIs are set out in the relevant federal governing legislation and the process is entirely under the control and direction of OSFI. The Minister of Finance is responsible for approving Letters Patent creating domestic FRFIs, and for authorizing foreign banks and life insurance companies to operate branches in Canada by means of Ministerial Orders. OSFI is responsible for managing the process leading up to Ministerial actions. Authorized banking is

regulated both at the federal and provincial levels and it is not possible for the process to permit the creation or authorization of shell banks.

The following table sets out the licensing or registration requirements in Canada.

Reporting Entities	Primary Regulator	Licensed/Registered	Legislation
Banks	Federal-OSFI	Licensed. Domestic banks are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign banks receive certificates to operate by one or more branches in Canada.	Bank Act
Cooperative Credit and Retail Associations [128]	Federal-OSFI for Cooperative Retail Associations; Provincial-Cooperative Credit Associations	Same as domestic banks	Cooperative Credit Associations Act
Credit Unions and *caisses populaires*	Provincial authorities	Registration	Legislation includes Credit Unions Act; Financial Institutions Act; Credit Union Incorporation Act; Credit Unions and *Caisses Populaires* Act; Deposit Insurance Act; An act respecting financial services cooperatives; An Act respecting the Mouvement Desjardins
Life Insurance Companies	Federal-OSFI Provincial authorities	Licensed [129] Either licensed or registered	Insurance Companies Act Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act; Life Insurance Act; Registered Insurance Brokers Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services(Quebec); Saskatchewan Insurance Act

[128] OSFI's oversight of Cooperative Credit Associations, commonly referred to as credit union centrals, is limited and quite different from its oversight of banks and other FRFIs. Cooperative Credit Associations are organized and operated based on cooperative principles. With the exception of the Credit Union Central of Canada ('CUCC'), the Cooperative Credit Associations are provincially incorporated, and regulated and supervised at the provincial level. The CUCC, which is federally incorporated, functions as the national trade association for the Canadian credit union system and does not provide any financial services. Cooperative Retail Associations are federally incorporated and supervised by OSFI in the same way as for banks and other FRFIs.

[129] Domestic life insurance companies under OSFI's jurisdiction are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign life insurance companies only operation under the federal legislation and receive Ministerial Orders permitting one or more branches in Canada.

Reporting Entities	Primary Regulator	Licensed/Registered	Legislation
Life Insurance Brokers and Agents	Provincial authorities	Licensed or registered	Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act; Life Insurance Act; Registered Insurance Brokers Act; Saskatchewan Insurance Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services (Quebec)
Trust and Loan Companies	Federal-OSFI Provincial authorities	Licensed Licensed or registered	Trust and Loan Companies Act Legislation includes Loan and Trust Corporations Act; Financial Institutions Act; Corporations Act; Trust and Loan Companies Act; Trust and Loan Companies Act; Deposit Insurance Act; An act respecting trust companies and savings companies (Quebec)
Investment Dealers	IIROC Provincial authorities	Registration Licensed (Northwest Territories) or registered	IIROC Dealer Member Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Mutual Fund Dealers	Mutual Funds Dealers Association Provincial authorities	Registered Licensed (Northwest Territories) or registered	MFDA Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Investment Counsel and Portfolio Management Firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Other securities firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Money Service Businesses	FINTRAC *Autorité des marchés financiers* (Québec)	Registration Licensed	PCMLTFA and PCMLTF Registration Regulations Money-Services Business Act

Criterion 26.3— Federal and provincial regulators are responsible for carrying out fit-and-proper tests on persons concerned in the management or ownership of FIs in Canada. The measures are used to prevent criminals or their associates from holding a significant or controlling interest in an FI in Canada.

OSFI conducts fit-and-proper tests on FRFIs at the application stage to assess the fit-and-proper status of applicants, their principals (beneficial owners), senior management and Boards of Directors. Fit-and-proper tests are conducted under the Bank Act (ss.27, 526 and 675), Trust and Loan Companies Act (s.26), Cooperative Credit Associations Act (s.27) and Insurance Companies Act (ss.27 and 712). OSFI requires that applicants provide details of whether applicants have been the subject of any criminal proceedings or administrative sanction and it conducts security screening.

OSFI has the authority to apply fit-and-proper tests during the lifetime of a FRFI but only applies this authority directly to changes of ownership and/or shareholding. To address changes in directors or senior managers, OSFI has issued Guideline E-17 "Background Checks on Directors and Senior Managers of Federally Regulated Entities" in that regard. These requirements are applied throughout the life of FRFIs. After an FRFI is licensed, fit-and-proper testing on new senior officers and Directors is conducted by the FRFI rather than by the regulator. However, OSFI continues to apply fit-and-proper checks on new shareholders. OSFI assesses FRFIs' compliance with the Guideline and has issued prudential findings on background checks conducted by FRFIs on responsible persons. Since 2014, FRFIs are required to notify OSFI of plans to appoint or replace senior managers or directors.[130]

Persons and entities operating and controlling MSBs are required to register with FINTRAC under the PCMLTF Registration Regulations. FINTRAC conducts criminal record checks when assessing applications for registration as MSBs and it can refuse or revoke registrations where a person has been convicted of certain criminal offenses.

Provincial regulators apply fit-and-proper controls to assess the suitability of persons who control, own or are beneficial owners of provincially regulated FIs. General fit-and-proper requirements apply in the securities and insurance sectors. For example, the Investment Industry Regulatory Organization of Canada (IIROC) evaluates whether an individual appears to be "fit and proper" for approval/registration and /or whether the individual's approval is otherwise not in the public interest. Included in the criteria are the evaluation of an individual's integrity and criminal record. Provincial securities regulators apply similar criteria. In addition, MSBs located in Quebec are subjected to a "fit-and-proper" test by the *Autorité des marches financiers* (AMF) under the *Money Services Business Act* (Quebec).

Provincial regulators have not adopted fitness and probity requirements for persons owning or controlling financial entities after market entry to the same extent as what is achieved at federal level.

Risk-Based Approach to Supervision and Monitoring

Criterion 26.4— OSFI and provincial regulators are responsible for prudential and conduct supervision of Core Principle institutions in Canada under the OSFI Act, provincial legislation and other governing legislation. OSFI applies an AML/CFT assessment program as part of the Core Principles-based prudential supervision of FRFIs. All FRFIs are supervised by OSFI on a consolidated

[130] OSFI issued an Advisory on Changes to the Membership of the Board or Senior Management.

or group basis, as required by the Core Principles. Canada underwent an IMF FSAP in 2013 and OSFI was found to comply with the implementation of the Core Principles in the banking and insurance sectors and was rated LC.

FINTRAC is responsible for the supervision of all REs for AML/CFT compliance under the PCMLTFA, including Core Principles institutions supervised by OSFI and provincial prudential regulators. OSFI and FINTRAC have a coordinated approach to supervision of Core Principles institutions that are FRFIs. FINTRAC consults and coordinates with other federal and provincial prudential supervisors and has signed 17 MOUs with regulators to exchange compliance related information.

Both OSFI and provincial regulators adopt a risk-based approach to identify firms that have a higher risk of AML/CFT activities. In 2013, OSFI and FINTRAC adopted a concurrent approach to conduct AML/CFT examinations in the FRFI sector. Non-Core Principles institutions are supervised by FINTRAC for compliance with the PCMLTFA. FINTRAC also receives information from provincial regulators arising from their prudential/conduct supervisory activities that may be relevant to AML/CFT compliance. MSBs are registered and supervised by FINTRAC (and AMF in Quebec) for compliance with the PCMLTFA.

Criterion 26.5— AML/CFT supervision is conducted in Canada on a risk-sensitive basis. A shorter version of the NRA identifying the inherent ML/TF risks in Canada has recently been published and the findings are being incorporated into supervisors' compliance activities. Supervisors have their own operational risk assessment models and they use a range of programs, activities and tools to supervise and monitor compliance with AML/CFT requirements. There has been an increase in the frequency and intensity of on-site and offsite supervision of FIs in recent years. There has also been an increase in resources at FINTRAC to carry out compliance activities since the last MER.

FINTRAC has developed an AML/CFT Supervisory Program that is risk-based to ensure that REs are complying with their obligations under the PCMLTFA. It uses an enhanced risk-assessment model to assign risk ratings to REs that allows the allocation of resources according to higher-risk areas. Its risk model relies on information such as media information, ML/TF intelligence, financial transaction reporting behaviour, information received from law enforcement and regulatory partners that have MOUs with FINTRAC. It is updated regularly using information it collects through intelligence and examinations and is adjusted following on-site and off-site examinations. The risk assessment carried out on FRFIs is done in collaboration with OSFI.

FINTRAC's Supervisory Program is influenced and guided by a number of factors including the risk rating of the RE using the enhanced risk-assessment model and using other tools such as the examination selection strategy. FINTRAC focuses its supervisory activities on a risk-based approach using higher-intensity activities for higher-risk REs and using other lower-intensity activities for medium- and lower-risk entities. FINTRAC's primary tool to supervise for AML/CFT compliance is its examinations strategy that is well developed. The examination strategy developed by FINTRAC prioritized activities aimed at REs that have been found to be non-compliant previously and those with high-risk ratings. It also focuses on key industry players with large market shares, which are examined regularly, given the inherent risks that are associated with their size and respective

business models and the consequences of non-compliance. FINTRAC also has a range of offsite mechanisms to conduct supervision of FIs including compliance assessment reports (CAR), desk-based reviews, monitoring of financial transactions, observation letters, compliance enforcement meetings, IT tools, voluntary self-disclosures of non-compliance and other awareness/assistance tools. CARs are used to segment REs within a sector, with results being used to initiate desk and on-site exams.

OSFI applies a risk-based approach to AML/CFT supervision. It has an AML/CFT risk assessment separate from its prudential risk assessment model for FRFIs and directs its assessment program at Canada's largest banks and insurance companies and other FRFIs considered at highest risk of ML and TF. OSFI's risk assessment methodology focuses on the vulnerabilities of FRFIs to ML and TF, looking at factors such as size, geographical spread, products, services and distribution channels and quality of risk management generally. It assigns a risk profile on each institution considering the risk factors and the quality of its risk management. OSFI's risk assessment results in a classification of FRFIs into categories of high, medium and low risk based on a combination of inherent risk, coupled with broader prudential views on the quality of risk management. OSFI supervises FRFIs on a group-wide basis and it conducts examinations of FRFI's on a cyclical basis depending on an FRFI's risk ratings and when information is received from prudential supervisors and other regulators including FINTRAC. OSFI also monitors major events or developments impacting the management or operations of FRFIs that informs both the content of AML/CFT assessments and also the assessment planning cycle.

FINTRAC and OSFI have agreed a concurrent approach to AML/CFT supervision of FRFIs allowing for concurrent examinations in addition to individual examinations that both supervisors can conduct of FRFIs. Both OSFI and FINTRAC exchange information that is relevant to FRFI's compliance with AML/CFT obligations. FINTRAC and provincial regulators also exchange information and FINTRAC can conduct AML/CFT follow-up activities with provincially regulated REs when AML/CFT issues are reported to it. Other supervisors also adopt risk assessments and supervision that are related to AML/CFT. For example, IIROC uses a risk assessment model for IIROC-regulated firms to determine priority focus and can apply an AML examination module by IIROC that is judged to present an AML/CFT risk. The primary responsibility for AML/CFT supervision remains with FINTRAC and any supervisory activity conducted by other supervisors' supplements, but does not replace, FINTRAC's responsibility to ensure compliance with the PCMLTFA and Regulations made thereunder.

Criterion 26.6— FINTRAC reviews its risk model on an ongoing basis and recently reviewed its sectoral analysis. FINTRAC also reviews its understanding of ML/TF risks for individual REs through reviewing the institution's compliance history, reporting behaviour and risk factors. In its ongoing review of the risk assessment, FINTRAC regularly monitors and assesses actionable intelligence, ML/TF risks and trigger events. OSFI reviews its AML/CFT risk profiles of FRFIs periodically. Risk assessments are applied to DSIBs on a continuous basis, reflecting their dominance of the FRFI sector and their very high-risk level. On-site assessments of DSIBs are conducted on a regular basis and DSIBs may be subject to more intensive supervision (staging) where deficiencies have been identified. The review of the risk profiling of other high-risk FRFIs is updated at less frequent

intervals, due to their less complex risk profiles. Provincial regulators are also kept apprised of ML/TF risks by FINTRAC and through the recently published NRA.

Weighting and Conclusion

Further fitness and probity controls are required.

Canada is largely compliant with R.26.

Recommendation 27 – Powers of supervisors

In the 2008 MER, Canada was rated LC with these requirements, notably because FINTRAC had no power to impose AMPs on REs. This has been remedied in December 2008.

Criterion 27.1— FINTRAC has authority to ensure compliance by all REs with parts 1 and 1.1 of the PCMLTFA (s.40). OSFI and provincial supervisors also have supervisory powers over REs under their own supervisory remit under federal and provincial legislation: e.g. the OSFI Act indicates the Superintendent's powers and duties in relation to the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act and the supervisory powers of the Superintendent are uniform under these Acts.

Criterion 27.2— FINTRAC has the authority to conduct inspections of FIs under the PCMLTFA. It can carry out on-site examinations of REs under PCMLTFA, s.62(1). Such examinations can be routine (with notice) but FINTRAC also has the authority to conduct unannounced examinations of REs under the PCMLTFA. OSFI has no mandate under PCMLTFA, but it supervises FRFIs under the OSFI Act and FRFIs' governing legislation (e.g. Bank Act) to determine whether they are in sound financial condition, are managed safely and are complying with their governing statute law. IIROC and provincial regulators conduct audits of registered firms to ensure compliance with Canadian securities laws.

Criterion 27.3— FINTRAC is authorized under the PCMLTFA to compel production of any information relevant to monitoring compliance with AML/ATF requirements. It can enter any premises (except a dwelling house) to access any document, computer system and to reproduce any document "at any reasonable time" (PCMLTFA, ss.62(1) and (2)). FINTRAC also has the authority to require REs to provide any information that FINTRAC needs for compliance purposes (s.62). There is a 30-day period given to deliver the information (PCMLTFR, s.70). OSFI has general powers to compel information from REs under OSFI Act, s.6 and federal governing legislation. While not mandated under the PCMLTFA, other regulators have the power to compel information under provincial or governing legislation to protect the public and market integrity. FINTRAC can exchange information on compliance with Parts 1 and 1.1 of the PCMLTFA with federal and provincial agencies that regulate entities.

Criterion 27.4— FINTRAC and OSFI have a range of supervisory tools to sanction REs for non-compliance. These tools include supervisory letters, action plans for FRFIs, staging by OSFI, compliance agreements, revocation of registration of MSBs by FINTRAC, revocation of FRFIs'

licenses by the AG of Canada[131] and criminal penalties. The PCMLTFA AMP Regulations provide FINTRAC with the power to apply AMPs to any FI and DNFBPs subject to the AML/CTF regime for non-compliance with the PCMLTFA. Provincial regulators, IIROC and MFDA have the power under their own governing legislation to conduct investigations and undertake enforcement action where necessary to protect the public and market integrity. They have the power to restrict, suspend and cancel registration. Further information is provided under the analysis of R.35.

Weighting and Conclusion:

Canada is compliant with R.27.

Recommendation 28 – Regulation and supervision of DNFBPs

In the 2008 MER, Canada was rated NC with these requirements (pages 229–243) notably because of deficiencies in the scope of the DNFBPs covered and not subject to FINTRAC supervision, and the sanction regime and resources available to FINTRAC were considered inadequate. Since then, the scope of DNFBPs under the supervision of FINTRAC has been extended to BC Notaries and DPMS, and FINTRAC was granted the power to impose sanctions under the PCMLTF AMP Regulations.

Casinos

Criterion 28.1— *a)* Gambling activities are illegal in Canada, except if conducted and managed by the province or pursuant to a license issued by the province on the basis of CC, ss.207(1)(a) to (g), and three different models are in place (charity, commercial casinos, First Nation casinos, as described in the 2008 MER pages 214–215). Internet gambling are not subject to AML/CFT obligations, as the amendment to the definition of casino under PCMLTFA[132] is not yet into force, as well as ship-based casinos (the latter is a very minor issue, considering that, according to the authorities, no Canadian cruise ship are currently being operated, and lottery schemes cannot be operated within 5 nautical miles of the Canadian shore). Several provinces have introduced internet gambling (British Columbia, Quebec, Manitoba, Nova Scotia, Prince Edward Island, New Brunswick, and Newfoundland). Under the provincial legislation, also lottery schemes performed through Internet are required to be licensed.

b) All provinces and territories have regulation on terms and conditions for obtaining the license and a regulatory authority empowered to administer the relevant provincial legislation. Due-diligence requirements of the applicants (casino operator, key persons associated with the applicants and executive members) are part of the licensing process, where financial, business information, information referring to criminal proceedings, and reputational elements are required and subject to a review conducted by the competent provincial regulatory authorities. The licensing provisions make reference to due-diligence procedure related to an extensive notion of "associates" of the applicant, and when the applicant is a company or a partnership controls are extended to partners, directors, as well as to any subject who directly or indirectly control the applicant or has a beneficial

[131] This authority is subject to a number of conditions as set out in federal governing legislation.
[132] In particular, PCMLTFA, Section 5, k, (i).

interest in the applicant. Notice of changes in directors, officers, associated of the registrants are submitted to the approval of the competent regulatory authority. Notification of charges and convictions of the licensee, as well as of its officers, shareholders, owners are required. In respect of charities that require a license to conduct casino events eligibility requirements must be met both where a charitable model has been adopted[133] and where a corporation model is in place.[134] Charitable events may be licensed also by First Nations Authority under the agreement with the relevant provincial legislator (Manitoba, Saskatchewan),[135] where the authority to issue license to charitable gaming has been delegated by the competent provincial authorities in favour of First Nations commissions. Under the Agreements (Part 10.1) the parties agree that the terms and conditions that apply to licenses off and on reserve are essentially the same. Audits are performed in order to ensure that the operators comply with the terms and conditions of the license.

Under the relevant provincial legislation, the same provisions apply also to lottery schemes performed through Internet.

The table below summarizes the list of casino's regulators identified under the provincial gaming legislation and the relevant legislation. Licensing authorities do not have express AML/CFT responsibility to qualify as competent authorities.

Province	Regulator	Provincial Legislation
Alberta	Alberta Gaming &Liquor Commission	Gaming and Liquor Act
British Columbia	Gaming Policy and Enforcement Branch	Gaming Control Act
Manitoba	Liquor and Gaming Authority of Manitoba First Nations Gaming Commissions at reserve charitable gaming within the municipality or on reserve	Liquor and Gaming Control Act
New Brunswick	Gaming Control Branch-Department of Public Safety	Gaming Control Act
Nova Scotia	Nova Scotia Alcohol and Gaming Division	Gaming Control Act

[133] Pursuant to Section 20.(1) of the Gaming and Liquor Regulation in Alberta charitable or religious organisation in order to qualify for the license must satisfy the board that the proceeds generated from the gaming activities must be used for charitable and religious activities. In this context, the volunteers of charities are allowed to work in key positions at the casino events only if licensed, thus being subject to criminal record checks. The Commission must ensure that the licensed organisation comply with the relevant legislation.
[134] Where Lottery Corporations are empowered to conduct and manage gaming on behalf of the provincial government, group or organization can be licensed to hold a gaming event by the competent regulator. In British Columbia background investigations may be conducted also in respect of the eligible organisation, its directors, officers employees or associated (Section 80 (1) (g) (vi) of the Gaming Control Act. Audit of the licensee are performed conducted by the Charitable Gaming Audit Team of the Gaming Policy and Enforcement Branch.
[135] In Saskatchewan the Provincial regulatory authority, SLGA, owns and manage the slot machines at six casinos operated by the Saskatchewan Indian Gaming Authority, a non-profit corporation licensed by SLGA, while the Indigenous Gaming Regulator has a delegated authority under 207 (1) (b) of the CC to issue charitable gaming licenses on designated reserves.

Province	Regulator	Provincial Legislation
Ontario	Alcohol and Gaming Commission of Ontario	Gaming Control Act Alcohol and Gaming Regulation and Public Protection Act
Quebec	*Régie des alcools des courses et des jeux*	Act Respecting Lotteries, Publicity Contest and Amusement Machines An Act respecting the *Société des lotteries du Québec.*
Saskatchewan	Saskatchewan Liquor and Gaming Authority IGR responsible for licensing and regulating charitable gaming on First Nations, operating through a Licensing Agreement with SLGA (2007).	The Alcohol and Gaming Regulation Act
Yukon	Professional Licensing & Regulatory Affairs Branch	Lottery Licensing Act Sec 2 (Eligibility) and Sec 10 (Regulations) of the Lottery Licensing Act
Newfoundland and Labrador	Department of Government Services and Lands, Trades Practices and Licensing Division (no specific provisions)	Lottery schemes-General rules
Prince Edward Island	PEI Lotteries Commission /Department of Community and Cultural Affairs for casinos charities	Lotteries Commission Act
Northwest territories	Consumer Affairs, Department of Municipal and Community Affairs	Lotteries Act Lottery Regulations
Nunavut	Department of Community and Government Services	The Lotteries Act and Regulations

c) FINTRAC is the only competent supervisory authority for compliance of casinos with AML/CFT requirements. It has signed the MOUs with the following regulators: Alcohol and Gaming Commission of Ontario (AGCO); British Columbia Gaming Policy Enforcement Branch (GPEB); Alcohol and Gaming Division of Service Nova Scotia; Saskatchewan Liquor and Gaming Authority (SLGA). Online gambling is not covered by the definition of casino currently into force under PCMLTFA.

DNFBPs Other than Casinos

Criterion 28.2— FINTRAC is the designated competent authority under PCMLTFA and PCMLTFR for the AML/CFT supervision of all DNFBPs. FINTRAC supervises 26,000 DNFBPs in total, including casinos (discussed under 28.1), trust and loan companies, accountants, dealers in precious metals and stones, BC Notaries, and real estate agents and developers. As described under R.22 lawyers and Quebec notaries, trust and company service providers that are not included among the trust and loan companies are not monitored for AML/CFT purposes.

Criterion 28.3— All the categories of DNFBPs that fall into the scope of AML/CFT regime are monitored by FINTRAC for compliance with AML/CFT requirements. Apart from real estate dealers under certain condition, the AML requirements have not been extended to other categories in addition to those provided for in the FATF standards.

Criterion 28.4— *a)* FINTRAC powers to monitor and ensure compliance are the same for FIs and DNFBPs (PCMLTFA s. 62). For details, see R.27.

b) The powers to prevent criminals or their associates from being accredited, or from owning, controlling or managing a DNFBPs other than casinos are more limited. No specific measure is in place for DPMS. Referring to accountants the current process of creating a unified new professional designation, the Chartered Professional Accountant, replacing the former three (Chartered Accountants, Certified General Accountants and Certified Management Accountants), is at different stages in the various provinces. The provincial associations are in charge of ensuring high professional standards also through investigation of complaints and enforcement actions. In the admission to membership disclosure of investigations and disciplinary proceedings is required and consent must be provided permitting the Registrar to access the relevant information.[136] Members are also required to promptly inform CPA after having being convicted of criminal offenses.[137] Allegations for a wide set of crimes, included ML, financial frauds, TF, entail a rebuttable presumption of failing to maintain good reputation of the profession.[138] Accounting firms (partnerships, limited liability partnerships and professional corporations) are required to disclose investigations involving any partners[139] or shareholders and consent shall be provided permitting the Registrar to access information regarding such investigation. Any change in partners, shareholder must be notified and failure to provide such disclosure are considered breach of memberships obligations. Regarding BC Notaries, under the Notaries Act of BC, the Society of Notaries Public of BC is empowered to maintain standards of professional conduct. The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favour of the RCMP must be provided. Under the Notary Act also Notary Corporation (Notary Act, ss.57 and 58(f) of) are subject to a permit and the procedure imply controls on the voting shares members (that must be members of the Society in good standing, thus having passed the screening procedures described above related to disclosure of criminal records) as well as the non-voting members (who can be only members of the Society or relatives). The Society is empowered to impose fines, as well as take disciplinary action and revoke the permits (Notary Act, s.35). In respect of real estate agents, as shown in the attached each province has suitability requirements for licensee that apply as individual,[140] which in most cases entail the provision of Certified Criminal Records Checks. Nevertheless, in some cases the relevant provisions make reference both as a condition of refusal to issuing and to suspending or cancelling a license to the notion of "public interest,"[141] which, despite the authorities, consider broad to include a large number of factors, seems to be too vague and left to the discretion of the competent regulatory authorities. The integrity requirements in respect of

[136] Section 2 of Reg. 4-1 of CPA Ontario.
[137] Rule 102. 1 of the Rules of professional conduct CPA Ontario.
[138] Rule 201.2 of 1 of the Rules of professional conduct CPA Ontario.
[139] Regulations 4-6, Section 11, CPA Ontario.
[140] No specific integrity requirement under the Real Estate Agents Licensing Act. The convictions of offenses against the CC shall be related to qualifications, functions or duties of the agent/sales persons (Section 18, (k) and are cause for suspension or cancellation of license.
[141] Manitoba, Section 11(1) of the Real Estate Brokers Act, New Brunswick, Section 10 (2) of the Real Estate Act; Prince Edward Islands, Section 4 (3) of the Real Estate Trading Act.

corporations and partnerships are not always expressly extended to partners, directors, officers.[142] Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority.[143] Furthermore, the relevant legislation is essentially orientated in a perspective of consumer's protection so that in some cases the condition for refusal of the license are previous convictions of indictable offense "broker-related,"[144] as well as the notification of licensee makes reference to convictions involving a limited set of offenses.[145] Moreover, as the presence of criminal records is not necessarily a bar to registration, a case-by-case approach is taken by the regulatory authority. Provincial legislation establishes an express exemption regime in favour of lawyers, trust companies[146] and in some cases accountants from the requirement for license in respect of real estate services provided in the course of their practice.

DNFBPS Category	Designated Competent Authority	Relevant Legislation	Market Entry Safeguards
Real Estate	**Regulatory Authority**	**Provincial Legislation**	
Alberta	Real Estate Council of Alberta	Real Estate Act, in particular Part 2, s. 17, Real estate Act Rules (20 (1) for individuals, ss 30 and 34 for real estate brokerage. s. 10.3 of Real Estate Regulations	All the provinces have suitability requirements for licensee that apply as individual. The integrity requirements in respect of corporations and partnerships are not always expressly extended to partners, directors, officers. Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority
British Columbia	Real Estate Council of British Columbia	Real Estate Services Act ss 3 (1) and 10	
New Brunswick	New Brunswick Financial and Consumer Services Commission Division	New Brunswick Real Estate Act ss 3 and 4.2	
Newfoundland and Labrador	The Financial Service Regulation Division	Real Estate Trading Act, s. 7	
Manitoba	Manitoba Securities Commission for licensing	The Real Estate Brokers Act and The Mortgage Brokers Act	
Nova Scotia	Nova Scotia Real Estate Commission	Real Estate Trading Act ss.4, 12	
Ontario	Real Estate Council of Ontario	Real Estate and Business Brokers Act s. 9.1, 10 (19)	

[142] In Saskatchewan, for example, under Section 26.1 (b) of the Real Estate Act the integrity requirements are limited to officers and directors. The same requirement is established in Nova Scotia under 12 (1) (b) of the Real Estate Trading Act.
[143] Only change in officials and partners in New Brunswick, Section 15 (1) (b) and (c) of Real Estate Act partners in Prince Edward Island Section 14 of Real Estate Trading Act.
[144] Quebec, Section 37 of the Real Estate Brokerage Act.
[145] New Brunswick, Section 15 (2) of the Real Estate Act (frauds, theft or misrepresentation).
[146] See, for example in British Columbia, Real Estate Service Act, Section 3, (3) lett. e) and f) the exemption regime in favour of FI that has a trust business authorization under the Financial Institutions Act and practicing lawyers.

DNFBPS Category	Designated Competent Authority	Relevant Legislation	Market Entry Safeguards
Prince Edward Island	Office of the Attorney General, Consumer and Corporate and Insurance Services	Real Estate Trading Act, ss.4 (3), 8 (2) b); 14	
Quebec	*Organisme d'autoréglementation du courtage immobilier du Québec*	*Loi sur le courtage immobilier* ss.4, 6, 37	
Saskatchewan	Real Estate Commission	The Real Estate Act s. 18 (1) and 26 (1)	
Yukon Territories	Professional Licensing and Regulatory Affairs	Real Estate Agents Act, ss.6, 7	
Northwest Territories	Municipal and Community Affairs-Superintendent of Real Estate	Real Estate Agents Licensing Act, ss.2, 1; 8 (1); 18	
Nunavut	Consumer Affairs	Real Estate Agents Licensing Act	
Accountants and Accounting Firms	Chartered Professional Accountant, the Certified Management Accountant, the Certified General Accountant and provincial associations	conducts (as),	As regards admission to Membership see, for example, Certified Management Accountants of Ontario (Regulation 4-1); CMA Regulations of Alberta (s. 2 (2), where it is stated that each applicant for registration shall provide evidence on conviction of a criminal offense.
DPMS	**No designated competent authority**	-	**No measure in place**
BC Notaries	The Society of Notaries Public	the Notary Act	The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favour of the RCMP. Notary Corporation (ss 57 and 58 f the Notary Act) are subject to a permit and the procedure imply controls on the voting shares members (that must be in good standing) as well as the non-voting members (who can be only members of the Society or relatives)

c) There are civil and criminal sanctions[147] available for failure to comply with AML/CFT obligations for DNFBPs as described under R.35, as well as the public notice of AMPs imposed. The AMP regime allows administrative sanctions to be applied to REs although the maximum threshold raises doubts about the dissuasiveness and/or proportionality of sanctions for serious violations or repeat offenders. However, there is a range of measures available to supervisors to ensure compliance that are both proportionate and dissuasive.

All DNFBPs

Criterion 28.5— FINTRAC has further developed its risk model that lead to a risk classification (low, medium, high) of activity sectors and entities and the frequency and intensity of supervision is a function of FINTRAC's risk assessment. FINTRAC has started to integrate the results of inherent NRA for 2015/2016. The risk model takes into account numerous sources of information in order to assess the risk factor of specific REs. Further details on how the risk profile affects the scope and frequency of controls are provided under IO.3.

Weighting and Conclusion

AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. Online gambling, ship-based casinos, trust and company service providers that are not included among the trust and loan companies are not subject to AML/CFT obligations and not monitored for AML/CFT purposes. The entry standards and fit-and-proper requirements are absent in DPMS and TCSPs, while for the real estate brokerage they are not in line with the standards. Taking into account the deficiencies identified in the scope of DNFBPs and subsequent coverage of AML/CFT supervision and in the fit-and-proper requirements for DPMS, TCSPs and for the real estate brokerage

Canada is partially compliant with R.28.

Recommendation 29 - Financial intelligence units

In its third MER, Canada was rated PC with former R.26 (see paragraphs 364–418) notably due to the fact that the FIU (i) had insufficient access to intelligence information from administrative and other authorities, and (ii) was not allowed to gather additional information from REs. The first deficiency has since been addressed. The FATF standard was strengthened by new requirements which focus on the FIU's strategic and operational analysis functions, and the FIU's powers to disseminate information upon request and request additional information from REs.

Criterion 29.1— In 2000, Canada established an administrative FIU—Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which is a national centre for receiving, analysing and disseminating information in order to assist in the detection, prevention, and deterrence of ML, associated predicate offenses and TF activities: PCMLTFA, s.40. The definition of an ML offense

[147] Sections 73.1 to 73.24 of PCMLTFA.

under the PCMLTFA is based on the definition of the offenses established in the CC, which includes information related to associated predicate offense.[148]

Criterion 29.2— FINTRAC serves as a national agency authorized to receive STRs and other systematic reporting required by the PCMLTFA or the PCMLTF regulations, including Terrorist Property Reports, Large Cash Transaction Reports (of CAD 10 000 or more), SWIFT and Non-SWIFT Electronic Funds Transfer Reports (of CAD 10 000 or more), Casino Disbursement Reports (of CAD 10 000 or more), physical cross-border currency or monetary instruments reports and seizures reports and any financial transaction, or any financial transaction specified in PCMLTFA. In addition, FINTRAC is authorized to receive voluntary information records (VIRs), i.e. information provided voluntarily by LEAs[149] or government institutions or agencies, any foreign agency that has powers and duties similar to those of the Centre (i.e. FINTRAC), or by the public about suspicions of ML or TF activities.[150]

Criterion 29.3— *a)* FINTRAC may request the person or entity that filed a STR to correct or complete its report when there are quality issues such as errors or missing information, but not in other instances where this would be needed to perform its functions properly. According to the authorities, Canada's constitutional framework prohibits FINTRAC from requesting additional information from REs. This deficiency was highlighted in Canada's Third MER, and Canada's Sixth Follow-up Report concluded that, despite the information-sharing mechanism put in place by FINTRAC since its last evaluation, the deficiency has not been adequately addressed.

b) PCMLTFA, ss.54 (1) (a) to (c), states that FINTRAC may collect information stored in a database maintained, for purposes related to law enforcement or national security, by the federal government, a provincial government, the government of a foreign state or an international organization, if an agreement to collect such information has been concluded. FINTRAC has direct or indirect access to a wide range of law enforcement information, as the Canadian Police Information Centre (CPIC), the Public Safety Portal (PSP), CBSA's cross-border currency reports and seizure reports databases, RCMP's National Security systems and *Sûreté du Québec*'s criminal information and the Canada Anti-fraud Centre of the RCMP databases, as well as to the CSIS database. However, FINTRAC still has insufficient access to the information collected and/or maintained by–or on behalf of–administrative and other authorities, such as CRA databases.

Criterion 29.4— *a)* FINTRAC must analyse and assess the reports and information received and/or collected under PCMLTFA, ss.54(1)(a) and (b), namely, STRs, Large Cash Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, physical cross-border currency or monetary instruments reports and seizures reports, information provided voluntarily by LEAs and

[148] See subsection 462.31(1) of the criminal code where "designated offence" means "a primary designated offence or a secondary designated offence" under section 487.04 of the CC.
[149] FINTRAC receives information provided voluntarily by CSIS, CBSA, CRA–Criminal Investigation Directorate–and the RCMP, as well as provincial and municipal police.
[150] VIRs are the mechanism used by LEAs and other partners of FINTRAC to send information to and advise FINTRAC of investigative priorities without creating an obligation on FINTRAC to respond so as to respect the principle of independence of the FIU. The majority of VIRs that FINTRAC receives focus on priority investigations. VIRs are often the starting point of FINTRAC's analysis (however, FINTRAC always maintains its ability to proactively develop cases).

other regime partners (i.e. the VIRs), queries from, foreign FIUs, as well as information collected from several databases or open source information (s. 54(1) (c) PCMLTFA).

b) FINTRAC is also required to conduct research into trends and developments in the area of ML and TF activities and to undertake strategic analysis (s. 58(1)(b) PCMLTFA). It does so by leveraging a range of open and classified sources of information. It publishes Typologies and Trends Reports[151] on a broad array of issues. From 2010 to 2015, it produced 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors (both covered and non-covered by the PCMLTFA). These reports provide feedback to REs, respond to Canada's intelligence priorities and build the evidence base for new policy development. FINTRAC has also participated to the working out of Canada's first formal NRA.

Criterion 29.5— FINTRAC is able to disseminate "designated information,"[152] either spontaneously or in response to a VIR, to the appropriate police force,[153] the CRA, CBSA, Communications Security Establishment, Provincial Securities Regulators (as of 23 June 2015) and CSIS, through secure and protected channels (ss.55(3)(a) to (g) and 55.1(1)(a) to (d) PCMLTA). It is also able to disseminate information upon request to LEAs with a court order issued in the course of court proceedings in respect of an ML, TF, or another offense (PCMLTFA, s.59(1). This process has not been used in recent years, as LEAs obtain sufficient information from FINTRAC in response to their VIRs. FINTRAC's AML/CFT supervisory unit and FIU unit are able to exchange information in the exercise of their respective functions. As indicated under R.30, some competent authorities, such as Environment Canada or Competition Bureau, cannot request information from the FIU.

Criterion 29.6— Information held by FINTRAC is securely protected and is disseminated in accordance with the PCMLTFA (s.40(c)). FINTRAC has internal procedures (FINTRAC's Privacy framework) governing the security and confidentiality of information, the respect of the confidentiality and security rules by its staff members and limiting access to information, including access to the IT system, to those who have a need to know in order to effectively perform their duties.

Criterion 29.7— FINTRAC was established as an independent agency that acts at arm's length and is independent from LEAs and other entities to which it is authorized to disclose information under ss.55(3), 55.1(1) or 56.1(1) or (2) (PCMLTFA, s.40(a)).

[151] Mass Marketing Fraud: Money Laundering Methods and Techniques (January 2015), Money laundering trends and typologies in the Canadian securities sector (April 2013), Money Laundering and Terrorist Financing Trends in FINTRAC Cases Disclosed Between 2007 and 2011 (April 2012), Trends in Canadian Suspicious Transaction Reporting (STR) (April and October 2011), Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (July 2010), Money Laundering Typologies and Trends in Canadian Casinos (November 2009), Money Laundering and Terrorist Financing Typologies and Trends in Canadian Banking (May 2009).
[152] The terms "designated information" cover a range of information, including the name and criminal records of a person or entity involved in the reported transaction, the amounts involved, etc.
[153] The appropriate police force means the police force that has jurisdiction in relation to the ML offense. This includes federal, provincial and municipal police forces, as they receive their power from the province.

a) The Director of FINTRAC is appointed by the Governor in Council for a reappointed term of no more than five year with a maximum term of ten years, and has supervision over and direction of the Centre regarding the fulfilment of its mission (internal organization, decisions taken, etc.) and in administrative matters (staff and budget).

b) FINTRAC is able to make arrangements or engage independently with other domestic competent authorities. Agreements or arrangements with foreign counterparts on the exchange of information are entered either into by the Minister or by the Centre with the approval of the Minister (PCMLTFA, s.56 (2)).

c) FINTRAC is not located within an existing structure of another authority: the FIU is an independent agency under the responsibility of the Minister with legally established and distinct core functions (PCMLTFA, ss.42 and 54).

d) The Minister is responsible for FINTRAC (PCMLTFA, s.42(1)) and the director of FINTRAC is the chief executive officer of the Centre, has supervision over and direction of its work and employees and may exercise any power and perform any duty or function of the Centre (PCMLTFA, s.45(1)).

Criterion 29.8— FINTRAC has been a member of the Egmont Group since 2002.

Weighting and Conclusion

FINTRAC has limited access to some information.

Canada is partially compliant with R.29.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 2008 MER, Canada was rated LC with former R.27 due to an effectiveness issue. Minor changes have since been made. There are also significant changes in the standard.

Criterion 30.1— LEAs are designated with the responsibility for investigating ML, predicate offenses and TF. There is one national police force (the RCMP) and two provincial LEAs (respectively, in Ontario and Quebec). The RCMP is a federal, provincial, and municipal policing body. All Canadian police forces are potential recipients of FINTRAC disclosures under the PCMLTFA and can investigate ML/TF offenses.

Most predicate offenses are investigated by provincial and municipal police forces, including the RCMP when they are acting as provincial police (except Ontario and Quebec). Serious or proceeds-generating crime investigations can be done by the RCMP either exclusively or in parallel with provincial or municipal forces.

The RCMP has the primary law enforcement responsibility to investigate both terrorism and TF. The Terrorist Financing Team of the RCMP's Federal Policing Criminal Operations (FPCO) is responsible for, inter alia, monitoring and coordinating major ongoing investigational projects related to

terrorist organizations on financial and procurement infrastructures.

Criterion 30.2— All national, provincial and municipal police forces are authorized, under the CC, as "peace officers" to conduct parallel financial investigations related to their criminal investigations. They may refer the ML/TF case to other police units for investigation, regardless of where the predicate offense occurred.

Criterion 30.3— All police forces are empowered to identify, trace, seize, and restrain property that is, or may subject to forfeiture, or is suspected of being proceeds of crime. They are empowered with a wide range of measures under the CC (see Criterion 4.2).

Criterion 30.4— Other agencies, including the CRA (Income Tax Act), Competition Bureau (Competition Act, ss.11-21) and Environment Canada (Environmental Protection Act 1999), have the authority to conduct financial investigations related to the predicate offenses that they respectively specialize in. In addition, law enforcement agencies in Canada have the authority under Common Law to investigate crime and criminal offenses such as ML. They may seek judicial authority to seize and freeze assets. For the CBSA, although it does not have the responsibility for pursuing financial investigations of predicate offenses included in the Immigration Refugee Protection Act (IRPA), the Customs Act and border related legislations, a referral mechanism is in place for RCMP to follow up on the financial investigations. PCMLTFA, s.18 authorizes the seizure and forfeiture of cash by CBSA. Section 36 of the same Act also authorizes the disclosure of the information to the RCMP for criminal investigations into ML or TF.

Criterion 30.5— All police forces are responsible for investigating corruption offenses (CC, ss.119-121 and Corruption of Foreign Public Officials Act, s.3). As mentioned in R.4 and above, they have the powers to identify, trace, and initiate the freezing and seizing of assets.

Weighting and Conclusion:

Canada is compliant with the R.30.

Recommendation 31 - Powers of law enforcement and investigative authorities

In its 2008 MER, Canada was rated C with former R.28. Minor changes have since been implemented in the Canadian legal framework as well as in the standard.

Criterion 31.1— *a)* CC, ss.487.014 (production order) and 487.018 (production order for financial and commercial information) empower a justice or judge to order a person other than a person under investigation to produce specified documents or data within the time to any peace or public officer. S.487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number.

b) Search warrant under CC, s.487 is available for peace and public officers to search any prescribed places for available information.

c) Law enforcement officers are authorized to take statements from voluntary witnesses under the powers conferred by the Common Law and in accordance with the Charter of Rights and Freedoms and the Canada Evidence Act. However, a witness cannot be compelled to provide a statement to police in an investigation of ML or its associated predicate offenses. For TF investigations, witnesses are bound to provide a statement in an investigative hearing under Part II.1 of the CC (Terrorism).

d) Search warrants under CC, s.487 (search and seizure of evidence) and 462.32 (search and seizure of proceeds of crime) empower investigators to search and seize evidence. The General Warrant under CC, s.487.01 further authorizes the use of any device or means to collect evidence.

Criterion 31.2— *a)* RCMP can mount undercover operations to infiltrate crime syndicates and collect evidence for prosecution. Based on the principles in common law, the police are deemed to have common law powers where such powers are reasonably necessary in order for them to execute the mandate of investigating the commission of serious offenses, and undercover operations fall into this category.

b) Law enforcement can intercept communications pursuant to an Order made under CC, s.186 without the consent of the targeted person. It applies to organized crime offenses or an offense committed for the benefit of, at the direction of, or in association with a criminal organization; or a terrorism offense. It applies to both ML and TF offenses.

c) Computer systems can only be accessed with the consent of the owner or by a search warrant / General Warrant under the CC, but the courts[154] have found that particular considerations apply to computers and the stored content therein, which may require authorities to obtain specific prior judicial authorization to search computers found within a place for which a search warrant has been issued.

d) Similar to (a) above, Canadian Police are conferred with the power to conduct controlled delivery and is subject to stringent RCMP's internal policy.

Criterion 31.3— *a)* CC, s.487.018 (production order for financial and commercial information) empower a justice or judge to order a FI or DNFBP other than a lawyer to produce specified data within the time to any peace or public officer. The s. 487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number. Search warrant under the provision of CC, s.487 is also available for peace and public officers to search any prescribed places for available information. However, the mechanism used to identify whether legal or natural persons hold or control accounts is not timely and deficient. In identifying whether a subject holds or controls accounts, law enforcement agencies will apply for a court order and serve it to the FI/DNFBP they reasonably suspect of holding such information and wait for the FI/DNFBP to respond. Each order can only be served to one specified FI/DNFBP. In urgent cases, the order can be drafted to obtain an initial response within days or otherwise it will take a longer time. The time required for such identification is considered not timely enough and the mechanism is not exhaustive to identify all accounts held with FIs/DNFBPs.

[154] (R. v. Vu, 2013 SCC 60 (CanLII))— www.canlii.org/en/ca/scc/doc/2013/2013scc60/2013scc60.html. .

LEAs may also use other informal processes, such as surveillance or FINTRAC disclosures, to identify the FIs/DNFBPs. These informal processes are sometimes lengthier and again not exhaustive to identify accounts held by the subject.

b) Warrants and production orders are normally obtained on an ex-parte basis. If the order is directed to a third party, a condition may be added specifically to prohibit the third party from revealing the fact of the warrant to the account holders. Assistance Order, under CC, s.487.02, can also be applied by the law enforcement agencies to seek assistance from a person and request that he/she refrain from disclosing the information to the suspect.

Criterion 31.4— Most law enforcement agencies can ask for information from FINTRAC by submitting VIRs. FINTRAC is able, under PCMLTA, ss.55(3)(a) to (q) and 55.1(1)(a), to disseminate "designated information" by responding to these VIRs. However, these provisions do not allow other competent authorities such as Environment Canada or Competition Bureau conducting investigations of ML and associated predicate offenses to ask for information held by the FINTRAC.

Weighting and Conclusion

LEAs generally have the powers that they need to investigate ML/TF but there are some shortcomings.

Canada is largely compliant with R.31

Recommendation 32 – Cash Couriers

In its 2008 MER, Canada was rated C for former SR IX (para 559–607).

Criterion 32.1— Canada has implemented a declaration system[155] for both incoming and outgoing physical cross-border transportation of currency and bearer negotiable instrument. A declaration is required for all physical cross-border transportation, whether by travellers or through mail, courier and rail or by any other means of transportation. The declaration obligation applies to both natural and legal persons acting on their own and behalf of a third party, and applies to the full range of currency and BNI, as defined in the Glossary to the FATF Recommendations.

Criterion 32.2— The reporting of currency and bearer-negotiable instrument of an amount of CAD 10 000 or more must be made in writing on the appropriate form and must be signed and submitted to a CBSA officer.[156] The reporting requirements of the PCMLTFA are met once the completed report is reviewed and accepted.

Criterion 32.3— This criterion is not applicable in the context of Canada, as it only applies to disclosure systems.

[155] Part 2 of the *PCMLTFA.*

[156] The PCMLTFA Sec. 12(3) outlines who must report; this applies to conveyances regardless of mode (air; marine; rail; land or postal).

Criterion 32.4— Upon discovery of a false declaration of currency or BNIs, or a failure to declare, CBSA officers have the authority to request and obtain further information from the carrier with regard to the origin of the money and its intended use, as to ask for the documents supporting the legitimacy of the source of funds (Customs Act s. 11).

Criterion 32.5— Under PCMLTFA, s.18, when persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or monetary instruments and to impose an administrative fine. The officer shall, on payment of a penalty in the prescribed amount (CAD 250, CAD 2 500, or CAD 5 000, depending of the circumstances, including the particular facts and circumstances of any previous seizure(s) the individual has had under the PCMLTFA), return the seized currency or monetary instruments to the individual from whom they were seized or to the lawful owner. If the officer has reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime within the meaning of CC, s.462.3(1) or funds for use in TF activities, there are no terms of release and the funds are forfeited. Overall, the administrative sanctions could appear to be nor proportionate and nor dissuasive for undeclared or falsely declared cross-border transportation of cash over the threshold.

Criterion 32.6— CBSA forwards all Cross-border Reports submitted by importers or exporters as well as seizure reports to FINTRAC electronically. If the currency or monetary instruments have been seized under PCMLTFA, s.18, the report is sent without delay to FINTRAC, in order to undertake an analysis on seizure information.

Criterion 32.7— CBSA officers undertake customs as well as immigration matters. Under PCMLTFA s. 36, CBSA is allowed to communicate information to FINTRAC, to the appropriate police force and to the CRA. Reports and seizure reports are systematically sent to the FIU and reports are communicated to the RCMP. The RCMP has a formal MOU with CBSA and a Joint Border Strategy which stipulates the roles and responsibilities of each partner and how they will cooperate.

Criterion 32.8— When persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or bearer negotiable instrument. No terms of release are offered on funds that are suspected to be proceeds of crime within the meaning of CC, s.462.3(1) or TF (PCMLTFA, s.18(2)). When an individual fully complies with the requirement to report on currency above the threshold, but there are reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out a seizure under the CC. The CBSA is empowered to restrain currency or BNIs for a reasonable time in order to allow the RCMP to ascertain whether evidence of ML/TF may be found, but there is no clear process is in place to engage any authority in ascertaining these evidences following false declaration or undeclared cross-border transportation of cash, nor where there is a suspicion of ML/TF or predicate offenses.

Criterion 32.9— False declaration leading to seizures of currency and bearer negotiable instruments are entered and maintained into the Integrated Customs Enforcement System. These information are also sent by CBSA to FINTRAC, which incorporates them into its database. These

reports include information that must be provided in the mandatory reports.[157] Under PCMLTFA, ss.38 and 38.1, within an agreement or arrangement signed by the Minister, cross-border seizure reports where ML/TF is suspected are provided to foreign counterparts if the CBSA has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or a TF offense, or within Custom Act s. 107 in accordance with an agreement. Declaration which exceeds the prescribed threshold are not retained by CBSA, but are forwarded to FINTRAC that should be in position to disclose CBCRs to its foreign counterparts, what may complicate international cooperation between customs regarding cash couriers.

Criterion 32.10— The information collected pursuant to the declaration obligation is subject to confidentiality.[158] There are no restrictions on the amount of money that can be imported into or exported from Canada; however, once the amount has reached or exceeded the threshold it must be reported.

Criterion 32.11— When there is reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out subsequent criminal investigation and laying of charges under the CC. If the suspicion is confirmed, seizure and confiscation measures may be decided by the judicial authority under the conditions described in R.4.

Weighting and Conclusion

There are some minor deficiencies.

Canada is largely compliant with R.32.

Recommendation 33 – Statistics

In its 2008 MER, Canada was assessed as LC with former R.32 because the absence of statistical information on ML investigations and sentencing, confiscation, response times for extradition and mutual legal assistance (MLA) requests, response times for requests to OSFI by its counterparts. Some changes were introduced in the standard as well as in Canada.

Criterion 33.1— The compilation of AML/CFT related statistics are coordinated by Finance Canada and provided by all regime partners including FINTRAC, the RCMP, the PPSC and Statistics Canada at the federal and provincial level. The authorities maintain a comprehensive set of statistics that appears suitable to assist in the evaluation of the effectiveness of its AML/CTF framework. As a consequence of the NRA process, the authorities have improved the usefulness of existing data sets and developed new ones. The authorities intend to maintain the AML/CFT related statistics with a focus on periodically measuring the effectiveness of the AML/CFT regime.

[157] Including amount and type of currency or BNI, identifying information on the person transporting, mailing or shipping the currency or monetary instruments, as well as information on the person or entity on behalf of which the importation or exportation is made.
[158] PCMLTFA, article 36 and followings.

Sub-criterion 33.1 a: FINTRAC keeps statistics of STRs received and disseminated. Statistics on STRs received by regions is also available. Regarding the statistics provided on the dissemination of information by FINTRAC, it is unclear whether these disclosures derive from STRs, as required by the FCFT standard statistics related to the FIU.

Sub-criterion 33.1 b: Canada maintains acceptable statistics regarding ML/TF investigations, prosecutions and convictions. Statistical data on ML, proceeds of crime and TF investigations and prosecutions is generated at the national, federal and provincial levels. It is generated from various sources, such as Statistics Canada's Uniform Crime Reporting Survey (UCR), the RCMP Occurrence Data (a records management system), the Public Prosecution Service's iCase, its case management and timekeeping system. The RCMP has employed its Business Intelligence program to provide statistical information on ML/TF investigations that is more detailed than UCR. This information is derived from the RCMP's various Operational Record Management Systems.

Sub-criterion 33.1 c: Canada maintains statistics on assets seized, forfeited and confiscated as proceeds of crime and offense-related property (the equivalent of "instruments" or "instrumentalities" in other countries). However, there is no legal requirement for the AG to keep statistics on seizures.

Sub-criterion 33.1 d: Statistics on made and received mutual legal assistance or other international requests for cooperation are maintained by the Department of Justice Canada. These statistics are used by Justice Canada to track the timeliness of response and the nature of underlying predicate crime.

Weighting and Conclusion

Canada is compliant with R.33.

Recommendation 34 – Guidance and feedback

In its 2008 MER, Canada was rated LC with these requirements due to the lack of specific guidelines intended for sectors such as life insurance companies and intermediaries, and insufficient general feedback given outside the large FIs sector. There has been a substantial increase in guidance and feedback by Canadian authorities since the last MER.

Criterion 34.1— Canada provides guidance to industry on AML/CFT principally through regulators. FINTRAC provides guidance to both FIs and DNFBPs that is accessible on its website. A range of guidance has been published in the form of guidelines, trends and typologies reports, frequently asked questions, interpretation notices, sector specific pamphlets, brochures and information sheets on general topics such as the examination process. Guidance information is tailored to the different reporting sectors and deals with reporting, record-keeping, customer due diligence, general compliance information and questionnaires. Issues such as suspicious transaction reporting, terrorist property reporting, record-keeping, client identification, and implementing compliance

regime to comply with AML/CFT obligations. Global Affairs Canada has issued guidance for countering proliferation (CP) sanctions regimes.

OSFI has a dedicated section of its website for AML/CFT and sanctions issues and it has issued prudential guidance that includes guidance on AML/CFT. A number of other guidelines issued by OSFI are either directly or indirectly applicable to AML/CFT requirements of the FRFI sector. In addition, OSFI's Instruction Guide Designated Persons Listings and Sanction Laws sets out OSFI's expectations for FRFIs when implementing searching and freezing CP and sanctions reporting obligations under the Criminal Code, UN Regulations and other sanctions laws. Other regulators such as IIROC have issued AML guidance to IIROC Dealer members in 2010. OSFI's guidance for FRFIs focuses on prudent risk management and internal controls to address the risk of ML and TF. It includes guidance on deterring and detecting ML and TF, background checks on directors and senior management, oversight of outsourced AML/CFT functions, corporate governance and screening of designated persons under the CC and UN Regulations. While FINTRAC is the main authority responsible for issuing AML/CFT guidance, other regulators also provide guidance on AML issues[159] and consult FINTRAC for policy interpretations.

Feedback is given by FINTRAC to industry through an outreach and assistance program for REs. This includes participating in conferences, seminars, presentations and other events providing feedback on compliance with AML/CFT legislation. REs can liaise with FINTRAC and OSFI by email or an enquiries telephone line. Each RE has a designated FINTRAC Compliance Officer to contact with any queries. FINTRAC's guidance and feedback to REs, in particular MSBs, is also reported as having increased significantly. The RCMP provides guidance through lectures to various businesses throughout Canada on recognizing and reporting suspicious transactions and has given conferences and seminars on identifying, reporting, and investigating ML and materials produced by it on AML related issues.

Since 2008, Canada has provided guidance to the life insurance sector that is very similar to what is provided to other sectors. The guidance on AML/CFT provided by OSFI is applicable to all FRFIs subject to the PCMLTFA including life insurance companies. The guidance provided by FINTRAC is relevant to FIs and DNFBPs and there is sector specific guidance for the financial sector including life insurance companies and brokers and MSBs.

Weighting and Conclusion

There is more specific guidance needed in certain sectors.

Canada is largely compliant with R.34.

[159] Quebec: AMF published a notice on AML/CFT requirements of their regulated entities; Nova Scotia Credit Union Deposit Insurance Corporation, Financial Institutions Commission of British Columbia, British Columbia Gaming Policy Enforcement Branch, Deposit Insurance Corporation Ontario, Prince Edward Island Credit Union Deposit Insurance Corporation have all published guidance on their websites.

Recommendation 35 – Sanctions

In its 2008 MER, Canada was rated PC because: administrative sanctions were not available to FINTRAC; OFI used a limited range of sanctions; and effective sanctions had not been used in cases of major deficiencies. Several changes occurred since then, e.g. FINTRAC was granted the power to apply AMPs for non-compliance with the PCMLTFA.

Criterion 35.1— Civil and criminal sanctions are available in addition to remedial actions. FINTRAC is responsible for imposing AMPs for non-compliance with the PCMLTFA and its regulations.

The PCMLTFA and related legislation provide for penalties for non-compliance with AML/CFT measures. Part V of the PCMLTFA sets out penalties for non-compliance with the Act. The United Nations Act provides that, when the United Nations Security Council passes a resolution imposing sanctions, such measures automatically become part of domestic law, and sets out penalties for non-compliance with its provisions.

The PCMLTFA covers a range of criminal offenses and a series of sanctions for contraventions of the provisions of the Act. Criminal penalties for non-compliance can lead up to CAD 2 million in fines and up to five years in prison. The criminal sanctions regime applies to most of the law and regulations provisions in the PCMLTFA. LEAs can conduct investigations and lay criminal charges in cases of non-compliance with the PCMLTFA.

The PCMLTF AMP Regulations govern the imposition of administrative sanctions for non-compliance with the PCMLTFA and related regulations. They provide for penalties, classifying violations as minor, serious or very serious. The maximum penalty for a violation by a person is set at CAD 100 000 and for a RE it is CAD 500 000. The imposition of a penalty is on a per violation basis: therefore, where there are multiple violations, an entity is potentially exposed to the maximum penalty for each individual violation. The maximum AMP thresholds for serious violations raises doubts whether it is proportionate or dissuasive (notwithstanding it relates to each instance of violation), given that there may be circumstances where a single egregious breach (or a few) may occur and the cumulative threshold might not be either a proportionate or dissuasive sanction. The threshold may also not be dissuasive in circumstances of repeat offending.

There are also other non-monetary methods used by FINTRAC, in addition to the AMP procedure, to apply corrective measures or sanction REs, including issuing deficiency letters, action plans for FRFIs, compliance meetings and enquiries, public naming, revocation of registration of MSBs and non-compliance case disclosures to LEAs.

OSFI has a range of powers as set out in OSFI Act, s.6. OSFI can apply written interventions, staging (more intense/frequent supervision), put in place compliance agreements and directions of compliance, place terms and conditions on a FRFI's business operations and direct independent auditors to extend the scope of their audit and guidance, which are enforceable. The staging process, involving more intensive supervision of an FRFI, does have a dissuasive affect, as it attracts an increase in the deposit insurance premiums paid by the FRFI concerned. OSFI can also remove

directors and/or officers from office, and/or take control of an FRFI in extreme cases of non-compliance with federal legislation, including the PCMLTFA. While OSFI does have the power to impose monetary penalties for non-compliance with general prudential provisions under an FRFI's governing legislation, violations of the PCMLTFA are dealt with by FINTRAC through the AMP procedure. OSFI has regulatory guidelines for AML compliance and background checks of directors and senior managers. OSFI cannot apply AMPs for non-compliance with the PCMLTFA.

Other regulators, such as securities regulators, can impose sanctions under securities legislation in circumstances where a market intermediary fails to meet legal requirements. The measures that can be taken include terminating the intermediary's license and imposing terms and conditions that restrict the intermediary's business. Sanctions can also be imposed on members for contraventions of self-regulatory organizations' requirements, including AML and supervision requirements.

Criterion 35.2— PCMLTFA, s.78 provides that sanctions are applicable to any officer, director, or agent of the person or entity that directed, assented to, acquiesced in, or participated in its commission.

Weighting and Conclusion

The dissuasiveness and/or proportionality of some of the sanctions is unclear.

Canada is largely compliant with R.35.

Recommendation 36 – International instruments

Canada was rated LC with former R.35 and SR I in the 2008 MER, because the ML offense did not cover all designated categories of predicate offenses and contained a purposive element that was not broad enough to meet the requirements of the Conventions, and because of inadequate measures to ascertain the identity of beneficial owners.

Criterion 36.1— Canada is party to the conventions listed in the standard.[160]

Criterion 36.2— Bill C-48 amended to the CC to meet the requirements of the Merida Convention, especially by providing for the forfeiture of property used in the commission of an act of corruption and to clarify that it may be direct or indirect, and that it is not necessary that the person who commits the corrupt act receive the benefit derived from the act. Canada also addressed the deficiencies identified in 2008 (see R. 3 and 10).

Weighting and Conclusion:

Canada is compliant with R.36.

[160] Canada ratified the Vienna Convention on 5 July 1990, the Palermo Convention on 13 May 2002, and the Merida Convention on 2 October 2007, the Convention on the Suppression of Terrorist Financing Convention on 19 February 2002, and the Inter-American Convention against Terrorism. It has also signed the Council of Europe Convention on Cybercrime (2001), on 23 November 2001.

Recommendation 37 - Mutual legal assistance

In its third MER, Canada was rated LC with former R.36 and SR. V due to concerns about Canada's ability to handle MLA requests in a timely and effective manner and about the lack of adequate data that would establish effective implementation. Canada's legal framework for MLA was supplemented by Canada's new Protecting Canadians from Online Crime Act (PCOCA, in force 9 March 2015). The requirements of the (new) R.37 are more detailed.

Criterion 37.1— Canada has a sound legal framework for international cooperation. The main instruments used are the Mutual Legal Assistance in Criminal Matters Act (MLACMA); the relevant international conventions, the Extradition Act; 57 bilateral treaties on MLA in criminal matters, extradition and asset sharing; and MOUs for the other forms of assistance to exchange financial intelligence, supervisory, law enforcement or other information with counterparts. These instruments allow the country to provide rapid and wide MLA. In the absence of a treaty, Canada is able to assist in simpler measures (interviewing witnesses or providing publicly available documents), or, based in the MLACMA, to enter in specific administrative arrangements, that would provide the framework for the assistance.

Criterion 37.2— Canada uses a central authority (the Minister of Justice, assisted by the International Assistance Group—IAG) for the transmission and execution of requests. There are clear processes for the prioritization and execution of mutual legal assistance requests, and a system called "iCase" is used to manage the cases and monitor progress on requests.

Criterion 37.3— MLA is not prohibited or made subject to unduly restrictive conditions. Canada provides MLA with or without a treaty, although MLA without a treaty is less comprehensive. Requests must meet generally the "reasonable grounds to believe standard, in relation for example to MLACMA ss 12 (search warrant) and 18 (production orders). However, certain warrants (financial information, CC, s.487.018, tracing communications, and new s.487.015) may be obtained on the lower standard of "reasonable ground to suspect."

Criterion 37.4— Canada does not impose a restriction on MLA on the grounds that the offense is also considered to involve fiscal matters, nor on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs.

Criterion 37.5— MLACMA, s.22.02 (2) states that the competent authority must apply *ex parte* for a production order that was requested in behalf of a state of entity. In addition to that, the international Conventions signed, ratified and implemented by Canada include specific clauses requiring the confidentiality of MLA requests be maintained.

Criterion 37.6— Canada does not require dual criminality to execute MLA requests for non-coercive actions.

Criterion 37.7— Dual criminality is required for the enforcement of foreign orders for restraint, seizure and forfeiture or property situated in Canada. MLACMA, ss.9.3 (3) (a) and (b) and 9.4 (1) (3) (5) (a) (b) and (c) allow the Attorney General of Canada to file the order so that it can be entered as a

judgment that can be executed anywhere in Canada if the person has been charged with an offense within the jurisdiction of the requesting state, and the offense would be an indictable offense if it were committed in Canada. This applies regardless of the denomination and the category of offenses used.

Criterion 37.8— Most, but not all of the powers and investigative techniques that are at the Canadian LEAs' disposal are made available for use in response to requests for MLA. The relevant powers listed in core issue 37.1 are available to foreign authorities via an MLA request, including the compulsory taking of a witness statement (according to MLACMA, s.18). Search warrants are not possible to obtain via letters rogatory. However, the Minister may approve a request of a state or entity to have a search or a seizure, or to use any device of investigative technique (MLACMA, s.11). The competent authority who is provided with the documents of information shall apply *ex parte* for the warrant to a judge of the province in which the competent authority believes evidence may be found. Regarding the investigative techniques under core issue 37.2, undercover operations and controlled delivery are possible through direct assistance between LEAs from the foreign country and Canada. Production orders to trace specified communication, transmission data, tracking data and financial data are possible by approval of the Minister in response to a foreign request. The authorities will not grant interception of communications (either telephone, emails or messaging) solely on the basis of a foreign request (this special investigative technique is not provided for in the MLACMA and will not be provided for in bilateral agreements. According to MLACMA, s.8.1, requests made under an agreement may only relate to the measures provided for in the bilateral agreement). The only possibility to intercept communications is within a Canadian investigation in the case of organized crime, or a terrorism offense, which would require that the criminal conduct occurred, at least in part, in Canadian territory (including a conspiracy to commit an offense abroad). Foreign orders for restraint, seizure and confiscation can be directly enforced by the Attorney General before a superior court, as if it were a Canadian judicial order.

Weighting and Conclusion

The range of investigative measures available is insufficient.

Canada is largely compliant with R.37.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Canada was rated LC with R.38 in the 2008 MER due to the limited evidence of effective confiscation assistance, the rare occurrence of sharing of assets and the fact that Canada executed requests to enforce corresponding value judgments as fines. The framework remains the same.

Criterion 38.1— Canada has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate laundered property and proceeds from crime (MLACMA, ss.9.3, 9.4 and CC, ss.462.32, 462.33), and instrumentalities used in or intended for use in ML, predicate offenses or TF. There is, however, no legal basis for the confiscation of property of corresponding value. As was the case during its previous assessment, Canada still treats value-based

forfeiture judgement as fines, which has limitations and cannot be executed against the property. If the fine is not paid, it can be converted into a prison sentence. Regarding the identification of financial assets new CC, s.487.018 allows the production of financial registration data in response to requests from foreign states.

Criterion 38.2— In Canada, MLA is based on the federal power in relation to criminal law. Therefore, the enforcement of some foreign non-conviction based confiscation orders is not possible under the MLACMA because they were not issued by a "court of criminal jurisdiction." However, in cases where the accused has died or absconded before the end of the foreign criminal proceedings, the MLACMA applies because the matter would still be criminal in nature. Due to Canada's constitutional division of powers, the Government of Canada cannot respond to a request for civil forfeiture as such requests fall within the jurisdiction of Canada's provinces. However, most of the Canadian provinces have already adopted legislation on a civil confiscation regime. Even if Canada is not able to provide assistance to requests for cooperation based on NCB proceedings, non-conviction based confiscation is possible under Canadian law. Should a foreign state seek to recover assets from Canada though NCB asset forfeiture, it must hire private counsel to act on its behalf in the province where the property or asset is located.

Criterion 38.3— *a)* No particular legal basis is required in Canada for the coordination of seizure and confiscation actions. It is a matter primarily for national and foreign police authorities at the stage of seizure. Thus, via direct police-to-police contact, arrangements are made in relation to any relevant case.

b) The Seized Property Management Act sets out the mechanisms for the management and, when necessary, the disposition of property restrained, seized and forfeited. The Minister of Public Works and Government Services is responsible for the custody and management of all property seized at the federal level. The Minister may make an interlocutory sale of the property that is perishable or rapidly depreciating, or destroy property that has little or no value. Property seized in the provincial level is managed by the provincial prosecution services.

Criterion 38.4— Canada shares confiscated property on a mutual agreement basis, under the Seized Property Management Act, s.11. Canada has 19 bilateral treaties regarding the sharing and transfer of forfeited or confiscated assets and equivalent funds.

Weighting and Conclusion

The seizure and confiscation regime has a deficiency, which is the impossibility of confiscation of equivalent value.

Canada is largely compliant with R.38.

Recommendation 39 – Extradition

Canada was rated LC with R.39 in the 2008 MER, mostly because of the difficulties in establishing the delay element, due to insufficient statistical data. The legal framework remains unchanged.

Criterion 39.1— Canada is able to execute extradition requests in relation to ML/TF without undue delay. Statistics provided to this assessment have shown that at least 40% of the requests are executed on a timely basis, what shows that the existing legal framework allows for extraditions without delay.

a) Both ML and TF are extraditable offenses (Extradition Act, ss.3(1) (a) and (b) of the combined with CC, ss.83.02, 83.03, 83.04 and 462.31).

b) Canada has a case management system (iCase) and clear processes in place for timely execution of extradition including prioritization of urgent cases. The Extradition Act sets out timelines for specific steps to ensure minimal delays, and requires judges to set an early date for the extradition hearing when the person has been provisionally arrested (s.21(1)(b)(3).

c) Canada does not place unreasonable or unduly conditions on the execution of extradition requests.

Criterion 39.2— Nationality does not constitute grounds for refusal to extradite under the Extradition Act, ss.44, 46, and 47 of the, but the Charter of Fundamental Rights and Freedoms gives Canadian citizens the right to remain in Canada. The Supreme Court decided in *U.S. v. Cotroni* that extradition is a reasonable limitation of the right to remain in Canada, and the decision whether to prosecute or not in Canada and allow the authorities in another country to seek extradition is made following consultations between the appropriate authorities in the two countries when various factors, including nationality, are considered in weighing the interests of the two countries in the prosecution. Historically, the result of most of these assessments has been to favour extradition, but when it is not, the Canadian citizen can be prosecuted in Canada.

Criterion 39.3— Dual criminality is required for extradition. It is not relevant whether the extraditable conduct is named, defined or characterized by the extradition partner in the same way as it is in Canada (Extradition Act, s.3(2)).

Criterion 39.4— Direct transmission of an extradition request to Canada's IAG or via Interpol is possible unless a treaty provides otherwise. Requests for provisional arrest may be made via Interpol by virtually all of Canada's extradition partners. The extradition process is simplified when the person consents to commit and surrender. Canada does not grant extradition based solely on a foreign warrant for arrest, such as in an Interpol Red Notice, or a foreign judgment, or in the absence of a treaty, based on reciprocity. There must be an assessment of the evidence, which takes place in the course of the judicial phase, which is followed by the Ministerial phase of the extradition proceedings.

Weighting and Conclusion:

Canada is compliant with R.39.

Recommendation 40 – Other forms of international cooperation

In the 2008 MER, Canada was rated LC with these requirements (para. 1551–1612). The main deficiency raised was related to FINTRAC as a supervisory authority.[161]

General Principles

Criterion 40.1— Canada's competent authorities can broadly provide international cooperation spontaneously or upon request related to ML/TF[162]. Referring to FINTRAC as FIU, PCMLTFA allows the Centre to disclose information to a foreign FIU spontaneously and makes reference to a disclosure of designated information "*in response to a request*."

Criterion 40.2— *a)* Competent authorities have the legal basis to provide international cooperation (see criterion 40.1).

b) Nothing prevents competent authorities from using the most efficient means to cooperate.

c) FINTRAC as a FIU and as a supervisor, OSFI, CBSA, and RCMP use clear and secure gateways, mechanism or channels for the transmission and execution of requests.

d) FINTRAC as an FIU has put in place processes for prioritizing and executing requests and answers in five business days if the Centre has transaction information in its database and FINTRAC as a supervisory authority processes the request and provides a response in a matter of days. In regard to TF, RCMP prioritize, assign and respond to such requests in the most efficient and effective manner on a National Level. It has not been established that LEA and supervisor authorities have clear procedures for the prioritization and timely execution of bilateral requests.

e) Competent authorities have clear processes for safeguarding the information received. FINTRAC policies and procedures for the safeguard of information apply to both the FIU and the supervisory side of FINTRAC. All supervisory information received by OSFI is subject to the same standard of confidentiality as domestic information (OSFI Act, s.22). RCMP has policies for handling requests and sharing or exchanging criminal intelligence and information with foreign partners and agencies (RCMP Operational manual Chapter 44.1s).

Criterion 40.3— Under the Privacy Act, competent authorities need bilateral or multilateral arrangements to cooperate with foreign counterparts where a disclosure of personal information about an individual is involved. FINTRAC as a FIU, RCMP and CBSA have signed a comprehensive network of MOUs and letters of agreement with foreign counterparts, but FINTRAC as a supervisory authority has entered into two MOUs so far. The Canadian authorities indicated that these bilateral agreements were signed mostly in a timely way. Examples of MOUs signed promptly have been

[161] *FINTRAC* as a supervisory authority had the legal capacity to exchange information with foreign counterparts but had not put the arrangements and agreements in place.
[162] FINTRAC as a FIU: *PCMLTFA*, section56; FINTRAC as a supervisory authority: *PCMLTFA*, section.65.1; RCMP: *Privacy Act and Memoranda of understanding or Letters of agreements*; CBSA: *PCMLTFA*, art.38 and 38.1 and *Custom Act*; OSFI: OSFI Act, section 22.

provided to the assessors. The OSFI Act does not require that the Superintendent enter into a MOU with a foreign counterpart in order to be able to cooperate.

Criterion 40.4— FINTRAC provides feedback upon requests to its foreign counterparts on the use and usefulness of the information obtained (PCMLTFA, ss.56.2 and 65.1(3)). Canadian authorities indicated that FINTRAC generally provides feedback to its foreign counterparts on the usefulness of the information obtained within five to seven days. There is no restriction on OSFI's ability to provide feedback. There is no general impediments, which prevents Canada's LEAs from providing feedback regarding assistance received.

Criterion 40.5— Competent authorities do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance on any of the four grounds listed in this criterion.

Criterion 40.6— Competent authorities have controls and safeguards to ensure that information exchanged is used for the intended purpose for, and by the authorities, for whom the information was provided.[163]

Criterion 40.7— Competent authorities are required to maintain appropriate confidentiality for any request for cooperation and the information exchanged, consistent with data protection obligations

Criterion 40.8— FINTRAC as an FIU, may conduct inquiries on behalf of foreign counterparts, by accessing its databases (all report types, federal and provincial databases maintained for purposes related to law enforcement information or national security, and publicly available information), under PCMLTFA, s.56.1(2.1). FINTRAC as a supervisory authority can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2), but only two MOUs have been signed so far. The RCMP can use a number of criminal intelligence and police databases to conduct inquiries on behalf of foreign counterparts, under sharing protocols that aim at protecting the right to privacy of the individuals mentioned in the databases.

Exchange of Information Between FIUs

Criterion 40.9— FINTRAC exchanges information with foreign FIUs in accordance with the Egmont Group principles or under the terms of the relevant MOU, regardless of the type of its counterpart FIU. The legal basis for providing cooperation is in PCMLTFA, s.56(1), which stipulates that the Centre exchanges information if it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or TF offense, or an offense that is "*substantially similar to either offense.*"

Criterion 40.10— FINTRAC provides feedback on the usefulness of information obtained, when feedback is specifically requested by foreign FIUs (PCMLTFA, s.56), and whenever possible as well as on the outcome of the analysis conducted, based on the information provided.

[163] *Privacy Act*—FINTRAC as a FIU: PCMLTFA, para 56 (3) and MOUs template; FINTRAC as a supervisory authority: PCMLTFA, s.65.1 (1) (b) and MOUs template; RCMP: Operational manual on information sharing; OSFI: OSFI Act, s.22.

Criterion 40.11— FINTRAC have the power to exchange:

a) The information held in its database (c. 40.8), which does not cover the scope of the information required to be accessible or obtainable directly or indirectly under R.29, as it does not include additional information from REs.

b) The information FINTRAC has the power to obtain or access directly or indirectly at the domestic level (c. 40.8), subject to the principle of reciprocity.

Exchange of Information Between Financial Supervisors

Criterion 40.12— PCMLTFA, allows FINTRAC to enter into information sharing arrangements or agreements under new s.65(2) with any agency in a foreign state that has responsibility for verifying AML/CFT. OSFI has broad authority to share supervisory information with domestic and foreign regulators or supervisors of FIs, including SROs.

Criterion 40.13— FINTRAC, as the AML/CTF supervisor for entities covered by the PCMLTFA, has the authority to share with foreign supervisors compliance-related information that FINTRAC has in its direct possession about the compliance of persons and entities. The information that FINTRAC may exchange with foreign supervisors is defined by "FINTRAC supervisory MOU Template." Canadian authorities indicated that FINTRAC can exchange information domestically available, including information held by FIs. As regards OSFI, under the OSFI Act a broad exemption is provided under s.22(2) in favour of the exchange of supervisory information with any government agency or body that regulates or supervises FIs.

Criterion 40.14— *a)* FINTRAC and OSFI do not require legislation to exchange regulatory information, and that they currently exchange such information. Examples were given by FINTRAC of cross-border cooperation with other regulators.

b) OSFI, under OSFI Act, s.22 can exchange supervisory information with foreign government agency or body that regulates or supervises FIs which meets this Criterion.

c) PCMLTFA, subsection 65.1 enables FINTRAC to exchange supervisory information with other supervisors about the compliance of persons and entities, record-keeping and reports. Through its supervisory examinations and compliance assessment reports, FINTRAC normally obtains information on REs' internal AML/CFT procedures and policies, CDD, customer files and sample accounts and transaction information. FINTRAC is able to exchange this information with other supervisors. However, this possibility is limited to exchanges with counterparts who are MOU partners.

Criterion 40.15— FINTRAC can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2).

Criterion 40.16— FINTRAC can enter into agreements or arrangement with other supervisors to exchange information pursuant to the PCMLTF.[164] Under such agreements or arrangements, there is an obligation to keep such information confidential and not further disclose the information. FINTRAC's tactical MOU sets out the requirements for use and release and confidentiality of information exchanged between financial supervisors. It is provided in the tactical MOU that information that has been exchanged will not be disclosed without the express consent of the requested authority. It is also provided that if an authority has a legal obligation to disclose information, it will notify and seek the consent of the other authority. OSFI can exchange information with other supervisors on the basis that such information satisfies the requirements of the Act and will be kept confidential.

Exchange of Information Between Law Enforcement Authorities (LEAs)

Criterion 40.17— Under article 44.1 of the RCMP Operational Manual on "Sharing of information with Foreign Law Enforcement," RCMP and other Canadian LEAs are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, associated predicate offenses or TF, including the identification and the tracing of proceeds and instrumentalities of crime. Nevertheless, CBSA does not retain CBCRs, which have to be obtained through international cooperation between FIUs, what could complicate their access by CBSA's foreign counterparts. PS works with other countries on national security, border strategies and countering crime, including ML and TF. PS also participates in a number of fora and initiatives to foster its international cooperation, including violent extremism and foreign fighters.

Criterion 40.18— Canadian LEAs can use the legislative powers available under the CC[165] and other Acts[166] including investigative techniques available in accordance with domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. However, it appears than the range of powers and investigative techniques that can be used by LEA to conduct enquiries and obtain information on behalf of foreign counterparts are very limited.[167] Both the PPOC and ML offense definitions allow that the offense need not to have occurred in Canada "so long as the act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence." Canada extensively cooperates with foreign law enforcement counterparts based on multilateral agreements in the context of Interpol and on bilateral MOUs.

Criterion 40.19— Canadian LEAs are able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangement to enable such joint investigations on the basis of RCMP Act (and the RCMP Operational policy Chapter 15 provides guidance on joint forces operation). Joint Forces Operations (JFO) involve one or more

[164] PCMLTFA, s.40 (c). PCMLTFA, s.65.1 (1) (b) also provides a limit on how the information can be used by both parties to a supervisory MOU. MOU Supervisory Template, Section 6 on Permitted Uses and Release of Exchanged Information, and Section 7 on Confidentiality are also relevant.
[165] CC, s.462.31 allows police to perform reverse sting operations to obtain information on ML cases and CC, s.462.32 to seize POC.
[166] Mutual Legal Assistance in Criminal Matters Act, RCMP Act and Canada Evidence Act.
[167] The only provisions which can be used allows police to perform reverse sting operations to obtain information on ML cases and to seize POC (CC, ss.462.31 and 462.32).

police/enforcement agencies working with the RCMP on a continuing basis over a definite period. A JFO should be considered in major multi-jurisdictional cases that are in support of national priorities and must be consistent with the mandated responsibility of the particular resource.

Exchange of Information Between Non-Counterparts

Criterion 40.20— Under PCMLTFA, FINTRAC as a FIU and a supervisor may enter into an agreement or arrangement, in writing, with an institution or agency of a foreign state that "*has powers and duties, similar to those of the Centre,*" which seems to exclude diagonal cooperation. Nevertheless, Canadian authorities indicate than when FINTRAC receives a request from a non-counterpart, the Centre address it either through its domestic partners or through the foreign FIU or supervisor. RCMP operational manual 44.1 outlines that sharing information will be managed on a case-by-case basis and there is no element that prevents RCMP to exchange information indirectly. OSFI has a broad ability to share information diagonally based on the wording of the OSFI Act, s.22. The "any government agency that regulates or supervises FIs" wording does not seem to limit disclosure to prudential regulators. However, OSFI would have to determine on a case-by-case basis whether such agency "regulates or supervises FIs." OSFI has shared information with foreign FIUs where they are also AML/CFT supervisors.

Weighting and Conclusion

There is room for improvement in regard to non-MLA international cooperation.

Canada is largely compliant with R.40.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• Lawyers, legal firms and Quebec notaries are not legally required to take enhanced measures to manage and mitigate risks identified in the NRA.
2. National cooperation and coordination	C	• The Recommendation is fully met.
3. Money laundering offence	C	• The Recommendation is fully met.
4. Confiscation and provisional measures	LC	• The legal provisions do not allow for the confiscation of property equivalent in value to POC.
5. Terrorist financing offence	LC	• CC, s. 83.03 does not criminalize the collection or provision of funds with the intention to finance an individual terrorist or terrorist organization.
6. Targeted financial sanctions related to terrorism & TF	LC	• Persons in Canada are not prohibited from providing financial services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person. • No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC and RIUNRST.
7. Targeted financial sanctions related to proliferation	LC	• No mechanisms for monitoring and ensuring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. • Little information provided to the public on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.
8. Non-profit organisations	C	• The Recommendation is fully met .
9. Financial institution secrecy laws	C	• The Recommendation is fully met.
10. Customer due diligence	LC	• Exclusion of financial leasing, factoring and finance companies from scope of AML/CTF regime. • Minor deficiency of existence of numbered accounts whose use is governed only by regulatory guidance. • Minor deficiency of limited application, to natural persons only, of requirements to reconfirm identity where doubts arise about the information collected. • No explicit legal requirements to check source of funds. • No requirement to identify the beneficiary of a life insurance payout. • Minor deficiency of exceptions to the timing requirements for verifying identity are not clearly justified in terms of what is reasonably practicable or necessary to facilitate the normal

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		conduct of business. • Minor deficiency of the lack of a requirement to obtain the address and principal place of business of non-corporate legal persons and legal arrangements such as trusts.
11. Record keeping	LC	• The legal obligation requiring REs to provide records to FINTRAC within 30 days does not constitute "swiftly", as the standard specifies.
12. Politically exposed persons	NC	• Only one element of the FATF standard is currently largely met, although new legislation covering domestic PEPs will come into force in July 2016.
13. Correspondent banking	LC	• No requirement for a FI to assess the quality of AML/CFT supervision to which its respondent institutions are subject.
14. Money or value transfer services	C	• The Recommendation is fully met.
15. New technologies	NC	• No explicit legal or regulatory obligation to risk assess new products, technologies and business practices, before or after their launch.
16. Wire transfers	PC	• No specific requirements for intermediary and beneficiary FIs to identify cross-border EFTs that contain inadequate originator information, and take appropriate follow-up action. These are significant deficiencies.
17. Reliance on third parties	PC	• No explicit requirements on life insurance entities and securities dealers in relation to either necessary CDD information to be provided by the relied-upon entity or supervision of that entity's compliance with CDD and record-keeping obligations. • No requirements on life insurance entities or securities dealers to assess which countries are high risk for third party reliance.
18. Internal controls and foreign branches and subsidiaries	LC	• No specific legal requirements in relation to screening procedures when hiring employees.
19. Higher-risk countries	C	• The Recommendation is fully met.
20. Reporting of suspicious transaction	PC	• Minor deficiency that financial leasing, finance and factoring companies are not required to report suspicious activity to FINTRAC. • Lack of a prompt timeframe for making reports.
21. Tipping off and confidentiality	LC	• The tipping off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
22. DNFBPs: Customer due diligence	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • On line gambling, TCSPs that are not trust companies are not obliged entities. • No requirement on beneficial owner, PEP, new technologies, reliance on third parties. With the exception of a limited set of transactions the fixed threshold (CAD 10,000) of cash financial transactions and casinos disbursement exceeds that provided in the Recommendation. • The circumstances in which accountants and BC notaries are required to perform CDD are not in line with the FATF requirement.
23. DNFBPs: Other measures	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • TSCPs that are not trust and loan companies and on line gambling are not subject to the AML/CFT obligations; the circumstances under which accountants and BC notaries are required to comply with STRs are too limitative. • Further deficiencies identified under R.20 for DNFBPs that are subject to the requirements.
24. Transparency and beneficial ownership of legal persons	PC	• No appropriate mechanism to ensure that updated and accurate beneficial ownership information is collected for all legal entities in Canada, whether established under provincial or federal legislation. • Timely access by competent authorities to all beneficial ownership information is not warranted, in particular in cases where such information is held by a smaller or provincial FI, or a DNFBP. • Insufficient risk mitigating measures in place to address the ML/TF risk posed by bearer shares and nominee shareholder arrangements. • No obligation for legal entities to notify the registry of the location at which company records are held. • In some provinces, there is no legal obligation to update registered information within a designated timeframe. • No legal obligation on legal entities to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or to authorize a DNFBP in Canada to provide such information to the authorities.
25. Transparency and beneficial ownership of legal arrangements	NC	• No obligation for trustees to obtain and hold adequate, accurate and current beneficial ownership information for all legal arrangements in Canada, whether established under provincial or federal legislation, or basic information on other regulated agents or and service providers to the trust. • Professional trustees, including lawyers, are not required to maintain beneficial ownership information for at least five

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		years. • Insufficient mechanism in place to facilitate timely access by competent authorities to all beneficial ownership information and any trust assets held or managed by the FI or DNFBP. • No requirement for trustees to proactively disclose their status to FIs and DNFBPs when forming a business relationship or carrying out a financial transaction for the trust. • Proportionate and dissuasive sanctions for a failure by the trustee to perform his duties are not available in most cases.
26. Regulation and supervision of financial institutions	LC	• There are further fitness and probity controls needed for persons owning or controlling financial entities after market entry at provincial level.
27. Powers of supervisors	C	• The Recommendation is fully met.
28. Regulation and supervision of DNFBPs	PC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • Online gambling, cruise ship casinos, TSCPs not included among trust and loan companies are not subject to AML/CFT obligations and thus not monitored for AML/CFT purposes. • The entry standards and fit and proper requirements are absent in DPMS and TCSPs than trust companies, and they are not in line with the standards for real estate brokerage.
29. Financial intelligence units	PC	• FINTRAC is not empowered to request further information to REs. • FINTRAC has a limited or incomplete access to some administrative information (e.g. fiscal information), • FINTRAC is not able to disseminate upon request information to some authorities (e.g. Environment Canada, Competition Bureau)
30. Responsibilities of law enforcement and investigative authorities	C	• The Recommendation is fully met.
31. Powers of law enforcement and investigative authorities	LC	• No mechanism in place to timely identify whether a natural or legal person holds / controls accounts • No power to compel a witness to give statement in ML investigation • Only LEAs can ask for designated information from FINTRAC
32. Cash couriers	LC	• Administrative sanctions are not proportionate, nor dissuasive. • It has not been established that a clear process was in place to analyse or investigate cross-border seizures. • Cross-border currency reports are not retained by CBSA and can only be exchanged with foreign Customs authorities through FIUs' international cooperation.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
33. Statistics	C	• The Recommendation is fully met.
34. Guidance and feedback	LC	• There is more specific guidance needed in certain sectors such as DNFBPs to ensure that they are aware of their AML/CFT obligations, the risks of ML/TF and ways to mitigate those risks. There is also further feedback required arising out of the submitting of STRs.
35. Sanctions	LC	• The maximum threshold of administrative sanctions raises doubts about the dissuasiveness of sanctions for serious violations or repeat offenders.
36. International instruments	C	• This Recommendation is fully met.
37. Mutual legal assistance	LC	• The MLACMA does not allow for the interception of communications (either telephone or messaging) based solely on a foreign request, what hampers foreign investigations.
38. Mutual legal assistance: freezing and confiscation	LC	• Canada cannot respond to requests for the seizure and confiscation of property of corresponding value.
39. Extradition	C	• The Recommendation is fully met.
40. Other forms of international cooperation	LC	• The impediments raised in R.29 for FINTRAC, notably the fact that the FIU is not empowered to request further information from REs and the fact that some RE are not requested to fulfil STRs, impacts negatively the international cooperation with its counterparts. • LEAs are not able to use a large range of powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts.

TABLE OF ACRONYMS

AMF	*Autorité des Marchés Financiers*
AML/CFT	Anti-money laundering and combating the financing of terrorism
APG	Asia/Pacific Group on Money Laundering
BC	British Columbia
CBCR	Cross-border currency report
CBSA	Canada Border Services Agency
CDR	Casino Disbursement Report
CDSA	Controlled Drugs and Substances Act
CRA	Canada Revenue Agency
CRA-CID	Canada Revenue Agency—Criminal Investigations Directorate
CSIS	Canadian Security Intelligence Service
DAR	Detailed Assessment Report
DOJ	Department of Justice
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
DNFBP	Designated Non-Financial Businesses and Professions
D-SIB	Domestic Systematically Important Bank
EFTR	Electronic Funds Transfer Report
FATF	Financial Action Task Force
FI	Financial institution
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial intelligence unit
FRFI	Federally Regulated Financial Institution
GAC	Global Affairs Canada
IAG	International Assistance Group
ICC	Interdepartmental Coordinating Committee on Listings
IMF	International Monetary Fund
IO	Immediate Outcome
IPOC	Integrated Proceeds of Crime Initiative

ISEDC	Innovation, Science and Economic Development Canada (former Industry Canada)
LCTR	Large Cash Transaction Report
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
MSB	Money service business
ML	Money laundering
MLA	Mutual legal assistance
NPO	Non-profit organisation
NRA	National risk assessment
OCG	Organised criminal group
OPC	Office of the Privacy Commissioner
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PCMLTFR	Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
PEFP	Politically exposed foreign persons
PEP	Politically exposed person
PF	Proliferation financing
PIPEDA	Personal Information Protection and Electronic Documents Act
POC	Proceeds of crime
PPSC	Public Prosecution Service of Canada
PS	Public Safety Canada (former Public Safety and Emergency Preparedness)
PSPC	Public Services and Procurement Canada (former Public Works and Government Services Canada)
RBA	Risk-based approach
RCMP	Royal Canadian Mounted Police
RE	Reporting entity
RIUNRST	Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism
STR	Suspicious transaction report
TCSP	Trust and company service provider
TF	Terrorist financing
TFS	Targeted financial sanction

UNSCR	United Nations Security Council Resolution
UNAQTR	United Nations Al-Qaida and Taliban Regulation
US	United States of America
VIR	Voluntary Information Record

www.fatf-gafi.org | www.apgml.org

September 2016

Anti-money laundering and counter-terrorist financing measures - Canada
Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Canada as at the time of the on-site visit on 3-20 November 2015. The report analyses the level of effectiveness of Canada's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.

Appendix 6

FINTRAC – *Indicators of Money Laundering in Financial Transactions Related to Real Estate*

Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

OPERATIONAL BRIEF:

Indicators of Money Laundering in Financial Transactions Related *to* REAL ESTATE

Canada

Appendix 6

OPERATIONAL BRIEF:

Indicators of Money Laundering in Financial Transactions Related *to* REAL ESTATE

Operational Briefs are intended to provide clarification and guidance on issues that impact the ability of reporting entities to maintain a strong compliance regime. More specifically, these products are focused on risk and vulnerabilities associated with exploitation for money laundering and terrorist activity financing, and on meeting reporting obligations with respect to suspicious transaction reports.

1. PURPOSE

This Operational Brief provides indicators that are intended to assist reporting entities involved in real estate transactions to meet their obligations to report suspicious transactions or attempted suspicious transactions that are related to the commission or attempted commission of a money laundering or terrorist activity financing offence. Included are real estate brokers, agents[1] and developers, as well as other types of reporting entities such as banks, securities dealers, trust/loan companies, life insurance companies/ brokers/agents, credit unions, "Caisses Populaires", British Columbia notaries, and accountants that are also involved in financial transactions related to real estate.

2. HIGHLIGHTS

- Reporting entities dealing with real estate related transactions are vulnerable to exploitation for money laundering purposes, either wittingly or unwittingly.
- Suspicious transaction reports submitted to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) describe indicators of suspected money laundering through real estate financial transactions that mirror those reported internationally.
- Minimal filings of suspicious transaction reports regarding real estate transactions indicate a clear need for operational guidance to all relevant reporting entities.
- FINTRAC provides indicators of money laundering in real estate in order to support all relevant reporting entities in meeting their obligations to report on suspicious financial transactions or attempted financial transactions.
- These indicators will be used by FINTRAC, along with other sources of information, to assess compliance with reporting obligations.

1 In the province of Quebec, the term used is "courtiers immobiliers" reflecting a unique set of requirements as set out in the Quebec Real Estate Broker Act and By-law and Regulation. For more details please see guidance provided by the Organisme d'autoréglementation du courtage immobilier du Québec (OACIQ) at https://www.oaciq.com/en/pages/by-laws-and-regulations

3. BACKGROUND

3.1 Canadian Real Estate: A Large and Susceptible Market

The Canadian real estate industry is extensive, consisting of approximately 100,000 brokers and sales representatives working through many real estate boards and associations across the country. In addition, a large number of developers and builders also sell real estate. The actual size of the real estate market is difficult to determine precisely, but as an order of magnitude, Canadian Mortgage and Housing (CMHC) statistics indicate that in a 10-year period, over $9 trillion of mortgage credits were negotiated[2] and up to approximately 5 million sales took place through Multiple Listing Services (MLS)[3]. In contrast, FINTRAC received, during approximately the same 10-year period (2003 to 2013), 127 suspicious transaction reports nationally by real estate brokers, agents or developers, and 152 by other types of reporting entities also involved in real estate transactions, such as banks, securities dealers, trust/loan companies, etc.

The exploitation of real estate by criminals for money laundering purposes is well recognized internationally and underscores the importance of quality reporting on relevant suspicious transactions. Many countries are increasing their efforts to implement counter measures following the Financial Action Task Force (FATF)'s work on this topic indicating that the real estate sector is highly susceptible for many reasons: for example, easy price manipulation and a variety of complex options for selling/purchasing/financing with anonymity[4]. Although illicit funds seem to be laundered primarily through residential homes, corporate properties also play a role[5]. FINTRAC, through its compliance examinations, has observed deficiencies in most aspects of the real estate sector's compliance programs that render it more vulnerable of being used by criminals to launder illicit funds.

FINTRAC provides guidance on indicators in order to improve quality reporting on suspicions of money laundering related to relevant real estate transactions, and to dispel misunderstandings related to the nature of money laundering methods and their complexity. For example, indicators may be misattributed to more easily identifiable forms of crime, such as fraud, or may be simplistically applied only when cash is involved. Misunderstandings may also be reinforced by the misconception among real estate brokers and agents that potential money laundering risks are non-existent due to the involvement of heavily regulated financial institutions. Furthermore, financial institutions and securities dealers may under-report because of an erroneous belief that brokers/agents/developers have already submitted suspicious transaction reports. In fact, real estate involves many distinct types of financial transactions that may warrant the reporting of suspicious transaction reports. For example, the suspicions surrounding deposits for a purchase may be primarily visible to and reported by real estate agents, brokers and developers, whereas those related to loans may be more visible to and reported by financial institutions.

3.2 The Importance of Reporting Suspicious Transactions

Money laundering is a crime that further reinforces criminal activities because it provides a means by which illicit funds can be enjoyed by criminals in a normal way. It affects society in many ways, from individual level impacts like coercion, threats and business risk to societal impacts on security and on the stability of the Canadian financial system. As an example, in the real estate sector, the injection of illicit funds into the housing market can artificially inflate selling prices thus making homes unaffordable, and increase the risk of investment losses when criminals move their operations to other markets[6].

Reporting suspicious financial transactions or attempted suspicious financial transactions is a key part of a financial intelligence system which enables FINTRAC to meet its mandate to detect, deter and prevent money laundering and terrorist financing activity. Using this information, FINTRAC produces financial intelligence relevant to investigations of

2 Canadian Mortgage and Housing Corporation, *CHS Mortgage Lending 2014*.

3 Canadian Mortgage and Housing Corporation, *Housing Market Outlook: Canada Highlights Edition*, 4th Quarter 2015.

4 Financial Action Task Force, *Money Laundering and Terrorist Financing Through the Real Estate Sector*, June 29, 2007 (http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingandterroristfinancingthroughtherealestatesector.html).

5 Stephen Schneider, *Money Laundering in Canada: An Analysis of RCMP Cases*, Nathanson Centre for the Study of Organized Crime and Corruption, York University, March, 2004.

6 *Latin American Urban Development into the Twenty First Century: Towards a Renewed Perspective on the City*. Editors, D Rodgers, J. Beall, R. Kanbur. Palgrave Macmillan. 2012.

money laundering, terrorist activity financing and threats to the security of Canada. In addition, research and analysis of this information along with a variety of other sources shed light on trends and patterns in money laundering and terrorist financing for domestic and international partners, reporting entities and the general public.

Under Section 7 of the PCMLTFA, all reporting entities subject to the Act must report suspicious transactions, and attempted suspicious transactions, to FINTRAC when there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering or a terrorist activity offence. This Operational Brief is primarily concerned with informing reporting entities that deal with financial transactions related to real estate in some way. These include the real estate brokers and sales representatives acting as agents for the purchase and/or sale of real estate, as well as developers who sell property to the public[7]. Also included are other sectors of reporting entities such as banks, securities dealers, trust/loan companies, life insurance companies/brokers/agents, credit unions, "Caisses Populaires", British Columbia notaries, and accountants that may also be involved in financial transactions or attempted financial transactions related to real estate. Failure to report suspicious transactions may result in serious civil or criminal penalties (up to $2 million and/or 5 years imprisonment).

Businesses and individuals not subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) – which includes lawyers, notaries outside of British Columbia, and the general public – especially buyers and sellers, are strongly encouraged to send a voluntary information record to FINTRAC[8] using the indicators listed in this Operational Brief. Suspicious transaction reports and voluntary information records, when brought together by FINTRAC, may provide a more complete picture of how money laundering may be occurring in the real estate sector.

4. INDICATORS OF MONEY LAUNDERING IN REAL ESTATE

Criminals bring illicit funds into the Canadian financial system through methods and techniques that disguise them as legitimate financial transactions. This allows criminals to purchase assets and eventually sell them in order to enjoy the funds generated by what otherwise appear as honest activities. They may also keep an asset purchased with illicit funds for investment, housing of illegal activity or as a mechanism for future laundering activities. Some examples of common methods used by criminals to launder illicit funds through real estate related transactions may include the under-valuing or over-valuing of property value, rapid successive buying and selling, use of third parties or companies that distance the transaction from the criminal source of funds, witting participation by some lawyers, accountants, real estate agents and financial advisors, cash from criminal sources, and private sales. Criminal organizations often combine methods in novel ways in order to avoid the detection of money laundering. As a result of the appearance of legitimacy provided by money laundering methods, reaching reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence, and submitting a suspicious transaction report to FINTRAC, requires more than a "gut feel" or "hunch", but does not require evidence that money laundering is actually occurring.

What is required is to consider the facts related to a transaction and its context that can, when taken together, stand out as unusual. Potential indicators of money laundering can include, for example, a customer's business, financial history, background and behaviour, even information that one may not be able to confirm. The trail of indicators may follow various scenarios and lead to different conclusions. A transaction that originally appeared to be normal could increase suspicion of money laundering upon consideration of other relevant factors and lead to enhanced due diligence; for example, lack of concern over the quality of the property one intends to purchase. Conversely, new information may remove an initial suspicion of money laundering. A single fact may have an overriding effect, for example, a purchaser identified as the subject of a criminal investigation related to proceeds of crime would increase suspicion of money laundering regarding a financial transaction that otherwise appeared normal. Finally, it is important to note that in reaching reasonable

7 For more details on the obligations of the real estate sector, please consult: http://www.fintrac-canafe.gc.ca/re-ed/real-eng.asp

8 For more details on submitting a voluntary information report, please consult: http://www.fintrac.gc.ca/reporting-declaration/vol/1-eng.asp

grounds to suspect, real estate agents, brokers and developers who sell property should consider any aspect of the transaction as potentially relevant, even those for which they are not directly involved; for example, a real estate broker who receives reliable information that a real estate client negotiated a suspicious mortgage, even if that client is a client of another agent, brokerage or developer that sells homes. This information should be considered as a potential indicator along with other available information in determining whether reasonable grounds to suspect exist[9].

Appendices 1 and 2 provide examples of a residential and a commercial scenario to illustrate how the trail of suspicion might start with one or two indicators, and then expand to include other indicators resulting in reasonable grounds to suspect that a real estate transaction may be related to the commission or attempted commission of a money laundering or terrorist activity financing offence. In reporting suspicious transactions to FINTRAC, the facts related to the indicators should be included along with the indicators. The appendices also link the relevant elements of the stories to indicators listed in the table below by referencing in-text relevant themes from column 1, for example, anonymity, transaction speed, geography and inconsistency.

9 For more details on reporting suspicious transactions, consult STR guidance (http://www.fintrac-canafe.gc. ca/guidance-directives/transaction-operation/1-eng.asp).

The table below lists indicators that were compiled by FINTRAC[10] and should be consulted by reporting entities that deal with real estate related financial transactions[11] in order to recognize, assess and report suspicious financial transactions. FINTRAC will use these indicators, along with other sources of information, to assess compliance with reporting obligations. In addition, reporting entities should build and maintain training programs that ensure the submission of high quality suspicious transaction reports. The first column labelled as "Theme" is intended to suggest meaningful groupings of indicators.

10 Indicators related to money laundering through real estate transactions are based on an analysis of FINTRAC's holdings of suspicious transaction reports, and a number of publicly available sources from the Australian Transactions Reports and Analysis Centre (AUSTRAC), the Financial Crimes Enforcement Network (FinCEN), the Criminal Intelligence Service of Canada Central Bureau, and the Organization for Economic Co-operation and Development; other sources include the Report of the Standing Senate of Canada Committee on Banking, Trade and Commerce (*Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really.* March 2013: A-28); Schneider, Stephen. *Money Laundering in Canada: An Analysis of RCMP Cases*. York University, March 2004; Schneider, Stephen. "Organized Crime, Money Laundering, and the Real Estate Market in Canada." *Journal of Property Research* (2004). 21(2) June; Stowell, Nicole, et al. "Mortgage Fraud: Current Trends and Issues". *Real Estate Issues* (2012). 37(2-3).

11 Included are real estate brokers and sales representatives acting as agents for the purchase and/or sale of real estate, developers who sell property (please see FINTRAC http://www.fintrac-canafe.gc.ca/re-ed/real-eng.asp), but also other sectors of reporting entities such as banks, securities dealers, trust/loan companies, life insurance companies/brokers/agents, credit unions, "Caisses Populaires", British Columbia notaries, and accountants that may also be involved in financial transactions or attempted financial transactions related to real estate.

4.1 TABLE OF INDICATORS

THEME	INDICATOR
Value	Client negotiates a purchase for the market value or above, but requests that a lower value be recorded on documents, and pays the difference "under the table".
Value	Loan/mortgage amount is above the market value of the property/real estate.
Anonymity	Client purchases property in someone else's name such as an associate, nominee, from a company, corporation, trust or a relative (other than a spouse).
Anonymity	Client inadequately explains the last minute substitution of the purchasing party's name.
Anonymity	Client pays initial deposit with a cheque from a third party, other than a spouse or a parent.
Anonymity	Transaction is completed anonymously, in collusion or innocently, through lawyer or notary. Deposits are made into lawyer's or notary's trust account.
Anonymity	Use of real estate brokers/agents/developers, lawyers or notaries, wittingly or unwittingly, to accept false personal or financial information related to any aspect of a real estate deal, or to mortgage/loans.

THEME	INDICATOR
Anonymity	Company purchasing real estate has a complex ownership structure.
Anonymity	Company or individual has no e-mail address, physical address, home or business telephone number (disconnected or fake), company logo, contact person.
Anonymity	Client refuses to provide own name on documents, or uses different names on offers to purchase, closing documents and deposit receipts.
Anonymity	Client insists on providing signature on documents by fax only.
Anonymity	Client uses a post office box or general delivery address where other options are available.
Flipping	Client buys back a property that he or she recently sold.
Flipping	Successive buying and selling transactions of the same real estate.
Transaction Speed	Client shows strong interest in quickly completing the transaction without good cause, or without interest in property characteristics, price negotiations, risks, commissions or other related details, or may offer unusually high bids relative to current value/industry standard.
Transaction Speed	Clients show considerable interest in transactions relating to buildings in particular areas without caring about the price they have to pay.
Transaction Speed	Accelerated repayment of loan/mortgage shortly after deal is completed even if penalties are incurred.
Loan	The information in the loan agreement is inconsistent or incorrect.
Loan	The conditions in the loan agreement are unusual (for example, no collateral was required) or the complex nature of the loan scheme could not be justified.
Loan	Underlying collateral is either not referenced in a loan agreement, is insufficient or fictitious or the collateral provider and other parties involved in the loan structure are not known.
Loan	Company lending the money for the purchase of real estate, possibly an offshore company, has no direct relation with the borrower.
Renovations	Invoices for real or phantom large remodelling or renovations are paid with cash.
Income generating	Buyer of income-generating property shows no interest in generating profit by filling-in vacancies or by adjusting rent or lease value based on market value.
Flow through	Incoming payments from abroad possibly linked to a trust account, followed immediately by wire transfers abroad without a logical reason.
Structuring	Multiple transactions involving payments in cash or in negotiable instruments (for example, bank drafts) which do not state the true payer and where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
Geography	Foreign buyer, either an individual or company, or source of funds are from a jurisdiction with strict bank secrecy laws, weak anti-money laundering regimes, or with a high level of political corruption[12].

12 Various authoritative lists identify relevant individuals, businesses and countries of interest that may be used to further operationalize these indicators. Although not exhaustive, here are some common examples: Global Affairs Canada lists sanctions on countries, organizations, or individuals administered for a variety of reasons (http://www.international.gc.ca/sanctions/countries-pays/index.aspx?lang=eng); the Financial Action Task Force (FATF)'s list of high-risk and non-cooperative jurisdictions (http://www.fatf-gafi.org/countries/#high-risk) and FINTRAC Advisories on financial transactions related to countries identified by the Financial Action Task Force (FATF), which focus on countries requiring increased diligence for money laundering and terrorist financing (http://www.fintrac-canafe.gc.ca/new-neuf/1-eng.asp); Public Safety Canada's Listed Terrorist Entities (http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/index-eng.aspx); CBSA's list of individuals subject to a Canada-wide arrest warrant, issued pursuant to the *Immigration and Refugee Protection Act* (http://www.cbsa-asfc.gc.ca/wc-cg/menu-eng.html) and the RCMP's list of individuals wanted domestically and internationally for various crimes (http://www.rcmp-grc.gc.ca/en/wanted).

THEME	INDICATOR
Geography	Foreign buyer, either an individual or company, especially if on a watch list, whose only connection to Canada is the real estate transaction.
Inconsistency	Client purchases personal use property through his or her company when this type of transaction is inconsistent with the client's ordinary business practice.
Inconsistency	Client persists in representing his financial situation in a way that is unrealistic or that cannot be supported by documents.
Inconsistency	Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
Inconsistency	A transaction involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
Inconsistency	Unusually large cash amounts used to fund any financial aspect of a real estate transaction; for example, deposits, down payments, loans/mortgages, etc.
Defaulting	Transactions which are not completed in seeming disregard of a contract clause penalizing the buyer with loss of the deposit if the sale does not go ahead.
Defaulting	No payment of interest or repayment of the principal.
Defaulting	Place a deposit for a house, renege on the deal shortly thereafter, then obtain a legitimate cheque from the solicitor's office for the value of the deposit.
Direct	Direct sale or purchase without using a real estate broker or sales agent.
Direct	There was no loan agreement between the lender and borrower.
Direct	Existing mortgage on a purchased property is assumed by another individual without involvement of a financial institution.
Direct	A financial institution was not involved in the loan structure and may involve multiple unknown investors.

5. CONTACT US

For more information on these indicators, please feel free to contact FINTRAC and specify "Operational Brief" as the subject.

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th floor, 234 Laurier Avenue West, Ottawa, ON, K1P 1H7, CANADA
- **Telephone:** 1-866-346-8722 (**toll free**)

To provide voluntary information to FINTRAC about money laundering or the financing of terrorist activities, please contact us as follows:

- **Facsimile:** 1-866-538-0880
  No long distance charges will apply.
- **Mail:** FINTRAC, 24th floor, 234 Laurier Avenue West, Ottawa, ON, K1P 1H7, CANADA
- **Web form:** https://www15.fintrac-canafe.gc.ca/vir-drtv/public/

APPENDIX 1

Illustration of How Indicators Might Raise Suspicions *in* RESIDENTIAL REAL ESTATE

Background

Jane Doe contacted real estate broker Mary Smith to enquire about two properties she was considering for a purchase. Jane stated that she worked as a server in a restaurant. Mary conducted research into the two properties and emailed Jane with pros and cons for each. They made appointments for viewings.

Initial Suspicion Is Triggered

On the day in question, Jane advised Mary by email that she was unable to attend due to illness, and that in any case she had already decided to purchase the $800,000 home. Jane explained that she was in the middle of a custody battle and was in a rush to buy a house in order to demonstrate that she was capable of providing for her two children. Mary was taken slightly aback by her choice of the most expensive home and her willingness to buy without first viewing the house or having anyone else inspect it first [Trigger: Transaction speed, Inconsistency]. Concerned about this choice, Mary pointed out that the selling price was overvalued by $50,000 and that she was in a good position to benefit by making a first offer under the asking price, but that in any case it would be important for Jane to visit the house in order to ensure that it met her needs. Jane emailed Mary to let her know that given her pressing need to find a home for her children that she had already made up her mind and directed Mary to offer the asking price [Escalation of suspicion: Value; Transaction speed, Inconsistency].

Trail of Additional Indicators and Decision to Report Suspicions to FINTRAC

Mary explained that in order to write up an offer, Jane would have to provide a deposit and identification. At this point, Jane emailed Mary and unexpectedly advised her that her brother would actually be mortgaging the house because he would be living with them [Anonymity – last minute third party]. Mary offered to make the 45 minute drive to meet them and write the offer, however Jane requested that she be emailed the form with the purchaser's name blank in order to enter the brother's name [Anonymity]. Her brother was arriving from Iran [Geography] on May 1 and would fill in the details when he got there. They would then scan the offer and email it back to Mary [Anonymity].

Given the rise in suspicion, Mary explained that the brother's ID would need to be checked personally. She offered to drive over to pick-up the deposit cheque and validate her brother's identification at the same time. Mary also requested bank and lawyer information as part of the standard financing and legal steps. Jane explained that they preferred to mail out the deposit cheque because her working hours at the restaurant were unpredictable [Anonymity].

Along with the deposit cheque signed by her brother on April 25 (several days before he was actually scheduled to arrive) [Inconsistency], Jane faxed a copy of her brother's driver's license [Anonymity], and provided only mortgage pre-approval with none of the required details.

When Mary called Jane and started to explain once again that the brother's identification document would have to be validated in person in order to proceed, Jane became very defensive and threatened to find another real estate agent. At this point, Mary explained that without proper ID validation, it would not be possible to go through with the deal. Jane informed Mary that her brother had decided to cancel the deal and requested that her brother's deposit be put into his bank account [Defaulting].

As a result of the overall level of suspicion raised by the combination of observable factors linked to indicators of suspicion, a suspicious transaction report was submitted to FINTRAC.

APPENDIX 2

Illustration of How Indicators Might Raise Suspicions *in* COMMERCIAL REAL ESTATE

Background

Fictitious Real Estate Broker Ltd. represented a developer that was interested in selling an office tower called Generic Park. A two-step process was used to first select a subset of the highest bidders who would then be given the opportunity to provide revised bids in a second step. The bid from Unrealty Investors Group, $200 million, was rejected as too low.

Initial Suspicion Is Triggered

Suspicion was initially raised because the bidder had never made a request to conduct any form of due diligence related to the property [Transaction speed]. Suspicion was further reinforced when, despite having been excluded from the second step of the process, the purchaser's real estate representative insisted on holding a meeting to position Unrealty Investors Group as a desirable purchaser by increasing the value of their original bid by approximately $40 million. This increase was very unusual according to industry standards [Value]. In addition, when asked if approval was required by their board of governors, Unrealty Investors Group said that it was not [Anonymity; Transaction speed]. The overall level of suspicion triggered a review of current facts and to seek additional contextual information surrounding the event for other indicators of suspicion.

Trail of Additional Indicators and Decision to Report Suspicious Transaction to FINTRAC

The bidding company was owned by a university student who had described it as specializing in the purchase of real estate in Canada by investors in the Caribbean [Inconsistency]. This was the company's first real estate purchase. Details regarding the nature and corporate structure of the bidding company were vague and authored directly by its owner without corroborating official documentation [Anonymity]. The law firm handling the purchaser's bid was a small multi-purpose firm with no specialization or previous history in corporate real estate [Anonymity, Inconsistency]. The lawyer's name was not listed as a member on the firm's website nor in the relevant lawyers' directory [Anonymity, Inconsistency]. Multiple businesses held the same address [Anonymity]. Funds appeared to be originating from an individual with no connection to Unrealty Investors Group [Anonymity].

As a result of the overall level of suspicion raised by the combination of observable factors linked to indicators of suspicion, a suspicious transaction report was submitted to FINTRAC.

FINTRAC-2016-OB001
November 14, 2016

Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

Canada

Appendix 7

FINTRAC - *Risk-Based Approach to Workbook Real Estate Sector* – December 2018

Canada

Financial Transactions and Reports Analysis Centre of Canada

Home ➜ Guidance ➜ Compliance program ➜ Risk-based approach workbook for the real estate sector

Risk-based approach workbook Real estate sector

December 2018

Introduction

FINTRAC has designed this workbook to help you with your risk-based approach (RBA). It is structured to help you identify risks by products, services and delivery channels; clients and business relationships; geography and other relevant factors. It will also help you implement effective measures and monitor the money laundering and terrorist financing (ML/TF) risks you may encounter as part of your activities and business relationships.

For more detailed information on implementing a risk assessment, please refer to the information contained in the FINTRAC Guidance on the Risk-Based Approach and Compliance program requirements.

Note: Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations including new technologies and developments will be coming into force in June 2017. This new element will be further developed in this guidance document in the coming months.

Who should use this document?

This document was designed for a small brokerage, firm or developer in the real estate sector. The approach outlined in this document applies to you if you are a real estate broker, a sales representative or a real estate developer:

- a real estate broker or sales representative means an individual or an entity that is registered or licensed in a province to sell or purchase real estate; or
- a real estate developer means an individual or an entity other than a real estate broker or sales representative, who in any calendar year after 2007 has sold the following to the public:
  - at least five new houses or condominium units;
  - at least one new commercial or industrial building;
  - at least one new multi-unit residential building each of which contains five or more residential units; or
  - at least two new multi-unit residential buildings that together contain five or more residential units.

It is important to note that while the use of the RBA workbook is not mandatory, assessing and documenting risk is a requirement under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). This document has been specifically designed to assist entities with the RBA process, however, entities can develop their own approach, use their own materials or create their own risk-rating scales, so long as a justification or rationale is provided as to why a specific rating was assigned to a given risk factor.

How should you assess your risks?

As part of your risk assessment, you need to identify the areas of your business that are vulnerable to being used by criminals for conducting money laundering or terrorist financing (ML/TF) activities.

Appendix 7

This means that you need to assess the risks associated with all your business services and activities, and develop a risk assessment specific to your situation. Specifically, you must address the following four areas:

- Products, services, and delivery channels (to better reflect the reality of the real estate sector, this workbook will now only refer to services and delivery channels);
- Geography;
- Clients and business relationships; and
- Other relevant factors.

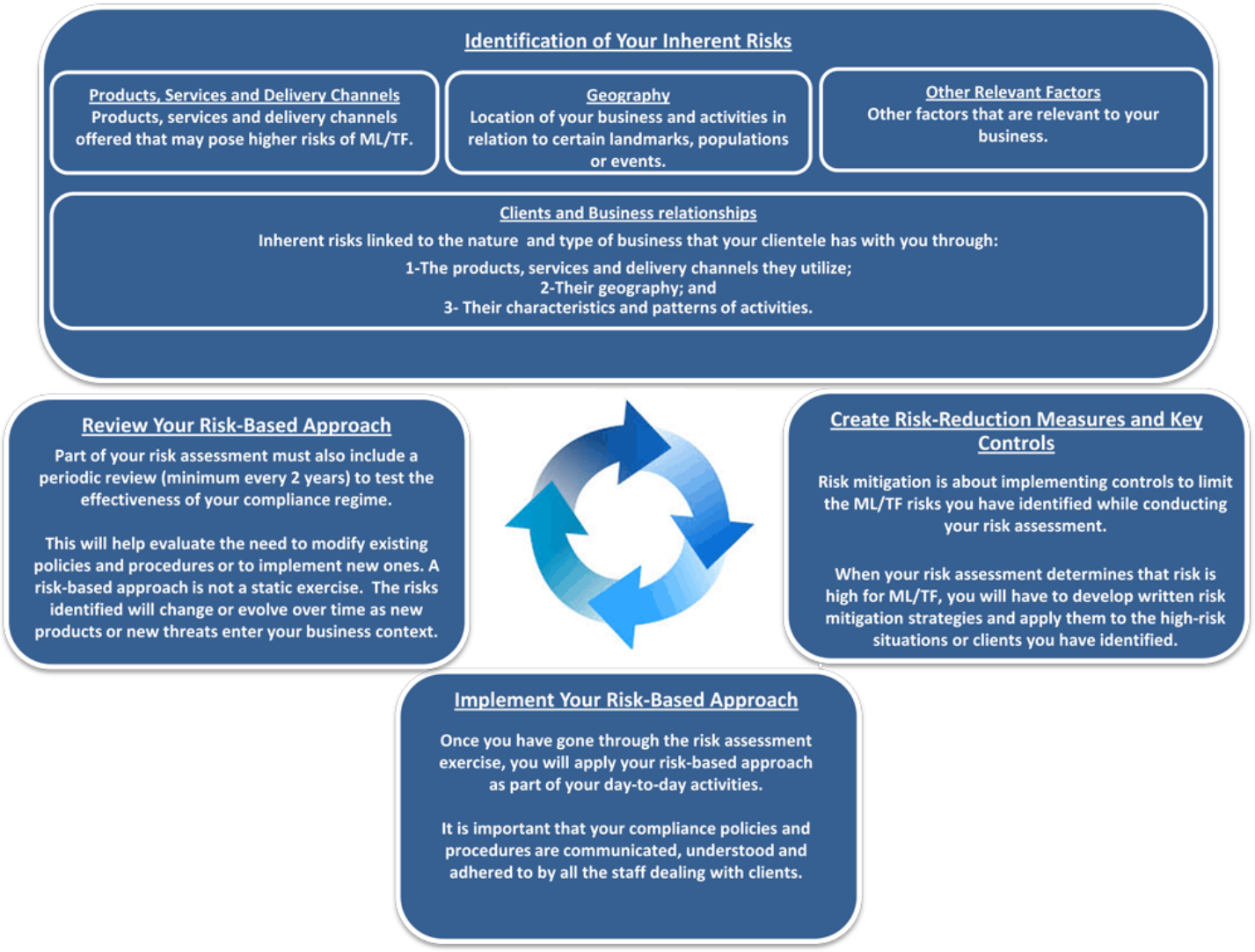
To do so, you need to consider the types of clients you deal with, the services you provide, how you deliver your services and the location of your business.

If you identify situations that represent a high risk of ML/TF activities, you need to control these risks by implementing mitigation measures, including conducting enhanced ongoing monitoring and keeping client information up to date. This will be further explained in the document.

Risk-based approach cycle

The following cycle represents the main steps of your risk-based approach:

1. identification of your inherent risks;
2. creating risk-reduction measures and key controls;
3. implementing your risk-based approach; and
4. reviewing your risk-based approach.



▶ View the text equivalent

To better assess your inherent risks effectively, you can divide your risk assessment into two parts:

1. **Business-based risk assessment**: your services and delivery channels; the geographical location in which your business operates along with other relevant factors.
2. **Relationship-based risk assessment**: services your clients utilize, the geographical locations in which they operate or do business as well as their activities, transaction patterns, etc.

It is important to note that there is no prescribed methodology for the assessment of risks. What follows is FINTRAC's suggested assessment process which will need to be adapted to your business situation. Although presented separately, parts 1 and 2 could be done simultaneously. You can also create your own assessment process.

1-Business-based risk assessment

Services and delivery channel

Begin your risk assessment by taking a business-wide perspective. As a business in the real estate sector, you must assess all your services and delivery channels to determine if they pose a high risk of ML/TF.

You may want to consider the following:

- Assess the services by the type of client they are meant for (e.g. corporate, individuals, families, third party, etc.)

Appendix 7

- Assess the services by the type of property listing (e.g. residential or commercial, vacant land, investment, high-turnover properties, agricultural land, or multi-unit properties for leasing purposes)
- Do the services you provide allow your client to engage in high-risk transactions? For example, do you provide services where clients register property in a nominee's name? Are there third party intermediaries involved in the purchase or sale of the property?
- How do you identify your client? Do you meet with your clients face-to-face or identify them by non-face-to-face means? Does the communication between the real estate agent or broker and client take place in person; or via email, fax, etc.?

Some examples of potential high-risk services and delivery channels are:

- The use of third party vehicles, such as trusts, to purchase property. There is a greater risk of ML as third party vehicles can obscure the identity of the true owner or buyer.
- Clients identified through agency or mandatary agreements. When a third party identifies clients on your behalf, there may be a greater risk that they may not be following policies and procedures to properly identify the client.
- Offering services by non-face-to-face means (phone, fax, online). These delivery channels may pose higher risks as it may be more difficult for your business to identify the client.

For examples on how to assess risk for services and delivery channels, see the RBA Guidance document.

Geography

Assess whether your own office location or the countries in which your clients are based could pose a high risk for ML/TF activities.

In the assessment of your geography, you have to consider whether the geographic locations in which you operate or undertake activities potentially pose a high risk for money laundering and terrorist financing. Depending on your business and operations, this can range from your immediate surroundings, whether rural or urban, to a province or territory, multiple jurisdictions within Canada (domestic) or other countries.

Some examples of geographic elements that need to be reflected in your assessment are:

- Property listings in high crime areas, as they may present additional ML/TF risks.
- Property in close proximity to the border.
- Significant and unexplained geographic distance between the agent and the client.
- A rural area where clients are known to you could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime in a rural area would obviously present a higher risk.
- Transactions involving persons residing in tax havens, high-risk jurisdiction or countries lacking appropriate ML/TF laws.
- If you provide services to foreign clients who are based in countries that are subject to sanctions, embargoes or other measures, you should consider that as high-risk. For example, the United Nations will occasionally issue an advisory about a certain country. Refer to:
  - FINTRAC Advisories
  - Financial Action Task Force's high-risk and non-cooperative jurisdictions
  - Canadian Economic Sanctions

For more examples on how to assess risk for geographic locations, see the RBA Guidance document.

Other factors relevant to your business (if applicable)

Assess other factors that may apply to your business that do not fall in the other categories. There may be something about your business that can make it more attractive to individuals who want to carry out ML/TF activities.

Some examples that may apply to you are:

- The size of your business, e.g. the financial value of the transactions facilitated.
- Your operational structure, number of branches, satellite offices, agents, brokers and employees.
  - For example, a business with a high employee turnover may present greater risk.
  - Does your business model include purchasing and selling services along with builder or developer activities?
- Trends and typologies for your respective activity sector may include specific elements of risks that your business should consider.

Business-based risk assessment worksheet

The following worksheet is for illustrative purposes only (please see additional instructions in Annex A). Using this worksheet could be an easy way for your entity to present the inherent risks related to your business, or you may develop your own worksheet.

Note: The information below is provided as an **example** only. Your entity may have more risk factors to consider. Furthermore, you may have different risk ratings. For more options, you can consult the matrix included in the RBA Guidance document.

Column A: **LIST OF FACTORS** **Identify all the factors that apply to your business (i.e. products,services and delivery channels, geography, other relevant factors)**	**Column B:** **RISK RATING** **Assess each factor (e.g. low, medium or high)**	**Column C:** **RATIONALE** **Explain why you assigned that particular rating**	**Column D:** **DESCRIBE MITIGATION MEASURES FOR HIGH RISKS IDENTIFIED IN COLUMN A.**
Use of a mandatary to identify clients.	High risk	There is greater risk that the mandatary is not adequately following policies and procedures to properly identify the client.	• Increase awareness of the real estate agents or brokers that it is their responsibility to make sure the ID requirements are met. • Randomly select client files where information was obtained by a mandatary and try to confirm the accuracy of the information with other sources.

Use of a mandatary to identify clients.	Low risk	The real estate broker or firm has a long-standing relationship with the mandatary and is aware of and confident in their identification processes.	• No mitigation measures are required because of low risk.
Offering services through non-face-to-face means, such as by email, fax or online.	High risk	There is greater risk of third parties being used to conceal the true owner or buyer, especially if a transaction is conducted through non-face-to-face means for no apparent reason.	• Request that the first payment be carried out from an account in the client's name through a bank subject to similar due diligence standards. • If third party involvement is suspected, take reasonable measures to determine the individual's name, address and principal business or occupation.
Offering services through non-face-to-face means, such as by email, fax or online.	Low risk	The clients are known to the broker or firm, have been identified in person previously and there is no third party involvement suspected.	• No mitigation measures are required because of low risk.
A high turnover of agents or brokers who deal directly with clients	High risk	New agents or brokers may have less knowledge of certain clients and less experience with ML/TF indicators.	• Provide training for new staff in a timely manner, in order to ensure the continuity of your compliance regime despite employee turnover. • Include ML/TF obligations in job descriptions and performance reviews (where appropriate) and monitor regulatory changes that could affect your entity.
Etc.			

2-Relationship-based risk assessment (i.e. your clients)

If you have a business relationship, you need to make a risk assessment based on the inherent characteristics of your client. This can be done based on the combination of the following factors, some of which were identified in the previous section:

- The services and delivery channels your client uses;

- The geography related to your client (at which location is the client conducting the transaction and where does the financing come from); and
- Your client's characteristics and your client's activities and transaction patterns.

However, it is possible that your business is dealing with clients outside of a business relationship. The interactions with these clients may be sporadic (e.g. few transactions over time that are under the identification threshold requirement or even a single transaction). As such, there will not be a lot of information available for your business to fully assess this client (as opposed to a client in a business relationship with information, patterns of activities, etc.). The risk assessment of such clients will most likely focus on the monitoring of transactions as opposed to having a client file. This monitoring is basically your obligation to report a suspicious transaction if you suspect that the transaction is related to a money laundering or terrorist financing offence.

If you do not have business relationships, it is not necessary for you to complete the Relationship-based risk assessment worksheet. However, if you have **high-risk clients outside a business relationship**, you need to include them in the following worksheet.

Below are some examples of client and transaction characteristics that can be considered high-risk:

Clients

- A client arriving at a real estate closing with a significant amount in cash.
- A client who wants to purchase a residential property in the name of a nominee, other than a family member, for no apparent reason.
- A client who resides overseas purchases a commercial property for no apparent reason.
- A client who is contacting you to purchase or sell real estate but the reason as to why they are contacting you makes no sense (e.g. client is not a local resident or is outside your normal customer base).
- A client is based in, or conducts business in a country with known higher corruption, known organized criminal activity, is known tax haven or is known to have links to terrorist organizations.
- A client negotiates a purchase at market value or above asking price, but requests that a lower value be recorded on documents, paying the difference under the table.
- A client buys back a recently sold property, or is involved in multiple transactions (purchases and sales) for reasons unknown or that do not make sense; or a client sells a recently purchased property for no apparent reason.
- A client has been named in the media as being involved with criminal organizations is purchasing a residential property.
- The value of a property is not within the means of a client based on his stated occupation or income.
- A client insists on providing signatures for transactions through non-face-to-face means.
- A client over justifies or over explains a purchase, or exhibits unusual concerns regarding the agency's compliance with government reporting requirements and the firm's anti-money laundering principles.

Transactions

- Behaviour or transactions that are unusual compared to other similar clients. For example, high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Transactions involving an individual whose address is unknown, or is likely to be false.
- Transactions involving foundations, non-profit entities, where the characteristics of the transaction do not match the goals of the entity.
- Multiple transactions involving one party or transactions carried out by groups of legal persons that may be related, where the transactions are otherwise unusual.
- Transactions that use unusual or unnecessarily complex legal structures for no apparent legitimate business reason.
- Transactions where the parties do not show particular interest in the characteristics of the property (quality of construction, location, date on which it will be handed over, etc.).

- Transactions conducted by foreign or non-resident parties for the purpose of capital investment (e.g. clients do not show any interest in living at the property they are buying).
- Transactions that must be completed quickly, without reason.
- Transactions that make use of third party vehicles (e.g. trusts) may obscure the ownership or the buyer.
- Transactions involving complex loans or other obscure means of financing.
- Transactions involving foreign individuals where the property is paid entirely without using a mortgage.
- Transactions involving properties that are likely over- or under-valued, when compared to similar properties in the area.
- Transactions where the buyer has no interest in a property inspection, for no apparent reason.

Please note that the following indicator, when encountered, will place clients in the overall high-risk category, regardless of other factors:

- If you file a Terrorist Property Report, the client automatically becomes high-risk.

For more examples of how to assess risk for client and business relationships, see the RBA Guidance document.

Relationship-based risk assessment worksheet

The following worksheet is for illustrative purposes (please see additional instructions in Annex B). Using this worksheet could be an easy way for your entity to present the inherent risks related to your business relationships, or you may develop your own worksheet.

This worksheet is to assess all your business relationships and high-risk clients. For more information on business relationships, see FINTRAC's Business relationship requirements.

Note: The information below is provided as an **example** only. For more options, you can consult the matrix included in the RBA Guidance document.

Column A: **BUSINESS RELATIONSHIPS** **Identify all your business relationships or high-risk clients (individually or as groupings)**	**Column B:** **RISK RATING** **Assess each business relationship (e.g. low, medium or high)**	**Column C:** **RATIONALE** **Explain why you assigned that particular rating**	**Column D:** **DESCRIBE ENHANCED MEASURES TO ASCERTAIN ID FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Column E:** **DESCRIBE MITIGATION MEASURES FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Column F** **DESCRIBE THE PROCESS TO KEEP CLIENT INFORMATION UP TO DATE FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Colu** **DES ENH ONG MON FOR BUS REL**
• Group A	Low	A known local family purchasing a residential property with the intention of living there.	**N/A**	**N/A**	**N/A**	**N/A**

Appendix 7

• Client B (or group B)	High	A foreign client originating from a high-risk country who is interested in purchasing property for the sole purpose of capital investment.	Obtain additional information on the client, such as occupation, volume of assets, as well as publicly available information. Determine if there is third party involvement, and take reasonable measures to identify them.	Increase awareness of higher-risk clients and transactions among agents and brokers. Require the first payment to be carried out from an account in the client's name through a bank subject to similar due diligence standards.	Ask clients to confirm that their information is up to date by using the same measures taken to ascertain their identity (e.g. refer to an original birth certificate, passport, etc.). Ensure that the intended nature of the business relationship is kept up to date.	Incre dilige know clien moti purp obje purc prop
• Etc.						

ANNEX A
Instructions to complete the Business-based risk assessment worksheet (Products, services and delivery channels; geography; other relevant factors)

This worksheet is for illustration. You may develop your own, so long as it includes the concepts that are described below.

Column A:	List of factors	Describe your services, delivery channels, factors related to your geographical location(s) and other relevant factors.
Column B:	Risk rating	Rate each risk factor (services, delivery channels, factors related to geographic location(s) and other relevant factor). **Please note** that the PCMLTFA and Regulations do not require you to use a low, medium and high scale. You could decide to have low and high risk categories or to have a more complex rating scale. A scale must be established, tailored to the size and type of business you have.
Column C:	Rationale	Provide the reasons why you assigned a particular risk rating to each service, delivery channel, geography, or other relevant factor. You can make reference to a website, a publication, a report, etc.

Column D:	Describe mitigation measures for high-risk factors	By law, all factors identified as "high-risk" must be addressed with documented mitigation measures. You have to write policies and procedures to explain how you are going to reduce and how you will control these risks in your day-to-day activities. Below are some examples of mitigation measures you may want to consider (not an exhaustive list): • Increase awareness of high-risk situations within business lines across your organization; • Provide adequate controls of higher-risk services, such as management approvals; • Create a culture of compliance amongst all, which includes developing, delivering and maintaining a training program for all designated agents and employees. • Increase due diligence and know your customer, and document the information gathered. For more examples of controls or ways to reduce risks, see the RBA Guidance document. and Compliance program requirements.

ANNEX B
Instructions to complete the Relationship-based worksheet (clients and business relationships)

This worksheet is for illustration. You may develop your own, so long as it includes the concepts that are described below.

Column A:	Business relationships or high-risk clients.	Identify all your business relationships and high-risk clients. You may decide to risk assess each business relationship separately or to do so by groups that share similar characteristics.
Column B:	Risk rating	Rate each business relationship. You can use a scale of low, medium and high to rate your business relationship. **Please note** that the PCMLFTA and Regulations do not require you to use a low, medium and high scale. You could decide to have low and high risk categories or to have a more complex rating scale.
Column C:	Rationale	Provide the reasons why you assigned a particular risk rating to each client type/business relationship.

Column D:	Describe enhanced measures to ascertain the identity of high-risk clients or to confirm the existence of a high-risk entity	You need to describe how identification was ascertained or how the existence of an entity was confirmed for each high-risk business relationship and high-risk client. Below are some examples: • Seeking additional information beyond the minimum requirements to ascertain the client's identity; • Obtaining independent verification of the information (that is, from a credible source other than the client); • Establishing more stringent procedures for validating client identification documents. For more information see Methods to identify individuals and confirm the existence of entities
Column E:	Describe mitigation measures for high-risk business relationship	You need to put controls in place for each high-risk business relationship and high-risk client that you identified. Below are some examples of mitigation measures that you may want to consider (not an exhaustive list): • Set limits to cash transaction amounts in certain situations; • Request bank drafts instead of accepting large amounts of cash; • Conduct certain transactions only in person. • Obtain appropriate additional information to understand the client's business or circumstances, including the purpose of being involved in numerous real estate transactions; • Establish more stringent thresholds for ascertaining identification, particularly if third party involvement is suspected. • Obtain information on the source of funds or wealth of the client. For more examples of controls or ways to reduce the risk, see Compliance program requirements.

Appendix 7

Column F:	Describe how you will keep client information and beneficial ownership information up to date for high-risk business relationships	You have to develop policies on how often and how you will update the client information of high-risk business relationships and high-risk clients. The information that needs to be updated generally includes: • For an **individual**, the individual's name, address and occupation or principal business. • For a **corporation**, its name and address and the names of the corporation's directors. • For an **entity other than a corporation**, its name, address and principal place of business. Measures to keep client identification up to date include asking the client to provide information to confirm or update their identification information. For example, you may ask a client for an additional piece of identification. You may also confirm the information through public sources if available. For more information see When to identify individuals and confirm the existence of entities – Real Estate

Column G:	Describe enhanced monitoring for high-risk business relationships	For all business relationships, you will need to conduct ongoing monitoring. This means that you will monitor your business relationships on a periodic basis for the purpose of: 1. Detecting any transactions that are required to be reported in accordance with the PCMLTFA; 2. Keeping client identification information up to date; 3. Reassessing the level of risk associated with the client's transactions and activities; and 4. Determining whether transactions or activities are consistent with the information you obtained about your client. However, **for high-risk business relationships and high-risk clients**, you need to conduct monitoring more frequently and with more scrutiny than with your other business relationships. This is called enhanced monitoring. Describe all aspects of your enhanced monitoring: • When is it done (frequency); • How is it conducted; and • How is it reviewed. Examples of how enhanced monitoring is conducted and reviewed for high-risk business relationships: • Obtain additional information on the client (occupation, volume of assets, information available through public database); • Review transactions based on an approved schedule that involves management sign-off; • Review transactions that have been identified as high risk on a regular basis (e.g. monthly). Flag and elevate concerns as necessary. • Determine whether transactions or activities are consistent with the information previously obtained from the client. • Set business limits or parameters regarding transactions that would trigger early warning signals and require mandatory review; and/or • Review transactions more frequently against suspicious transaction indicators relevant to the relationship. See STR guidance for more information about indicators. For more information on enhanced ongoing monitoring, see Ongoing monitoring requirements .

ANNEX C
Glossary and useful links

Business relationship:

You enter into a business relationship when a client opens an account or undertakes two or more transactions with you that require you to ascertain the identity of the client, regardless of whether the transactions are related to one another.

Delivery channels:

Medium that can be used to obtain a product or service, or through which transactions can be conducted.

FINTRAC:

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), is Canada's financial intelligence unit.

Inherent risk:

Risk that exists before the application of controls or mitigation measures.

Mitigation measures:

Controls put in place to limit the potential money laundering and terrorist financing risks you have identified while conducting your risk assessment.

Non-face-to-face transactions:

Transactions where the client is not physically present (for example, Internet, telephone or mail)

Risk-based approach:

In the context of ML/TF, a risk-based approach is a process that encompasses the following:

- The **risk assessment** of your business activities and clients using certain prescribed elements: Products, services and delivery channels; geography; clients and business relationships; and other relevant factors.
- The **mitigation of risk** through the implementation of controls and measures;
- Keeping **client identification** and, if required, beneficial ownership and business relationship information up to date; and
- The **ongoing monitoring** of transactions and business relationships.

Third party:

Individual or entity other than the individual who conducts the transaction. When you are determining whether a third party is involved, it is not about who "owns" the money, but rather about who gives instructions to deal with the money.

Vulnerabilities:

Elements of a business that could be exploited. In the ML/TF context, vulnerabilities could be weak controls within a business offering high-risk products or services.

Regulatory references:

http://laws-lois.justice.gc.ca/eng/acts/P-24.501/
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-317/
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-121/
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/

Guidance References:

Guideline 1: Backgrounder
Guidance – Main Page
Real estate developers, brokers and sales representatives – Main Page
Reporting entities – Main Page
Risk-based approach
Compliance program requirements

Appendix 7

FATF Money Laundering & Terrorist Financing Through the Real Estate Sector
http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingandterroristfinancingthroughtherealestatesector.html

FATF Guidance on the Risk-Based Approach for Real Estate Agents
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforrealestateagents.html

Date Modified:
2020-08-13

Appendix 7

Appendix 8

FINTRAC - *Money Laundering and Terrorist Financing Indicators – Real Estate*

Canada

Money laundering and terrorist financing indicators - Real estate

January 2019

This guidance on suspicious transactions is applicable to real estate developers, brokers and sales representatives that are subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. It is recommended that this guidance be read in conjunction with other suspicious transaction report (STR) guidance, including:

- What is a suspicious transaction?
- Reporting suspicious transactions to FINTRAC

This guidance provides money laundering (ML) and terrorist financing (TF) indicators (ML/TF indicators) organized by topic:

- ML/TF indicators related to identifying the person or entity
- ML/TF indicators related to client behaviour
- ML/TF indicators related to the person/entity financial profile
- ML/TF indicators based on atypical transactional activity
- ML/TF indicators related to transactions structured below the reporting or identification requirements
- ML/TF indicators related to transactions that involve non-Canadian jurisdictions
- ML/TF indicators related to use of other parties
- Indicators specifically related to terrorist financing
- ML/TF indicators real estate agents and developers
- ML/TF indicators real estate brokers and sales representatives

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours, patterns or other contextual factors that identify irregularities related to financial transactions. These often present inconsistencies with what is expected of your client based on what you know about them.

The ML/TF indicators in this guidance were developed by FINTRAC through a three-year review of ML/TF cases, a review of high quality STRs, published literature by international organizations such as the Financial Action Task Force (FATF) and the Egmont Group, and consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation but were developed to provide you with a general understanding of what is or could be unusual or suspicious. On its own, a single ML/TF indicator may not appear suspicious. However, observing an ML/TF indicator(s) could lead you to conduct an assessment of the transaction(s) to determine whether there are further facts, contextual elements or additional ML/TF indicators that require the submission of an STR.

Criminal organizations often combine various methods in different ways in order to avoid the detection of ML/TF. If you detect unusual or suspicious behaviour or a transaction that prompts the need for an assessment, ML/TF indicators combined with facts and context can help you determine if there are **reasonable grounds to suspect** that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators may also be used to explain or articulate the rationale for your reasonable grounds to suspect in the narrative portion of an STR, as they provide valuable information from a financial intelligence perspective.

Important considerations

One piece of the puzzle

The ML/TF indicators in this guidance are not an exhaustive list of ML/TF indicators to support all suspicious scenarios. These ML/TF indicators should be considered as examples to guide the development of your own process to determine when you have reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators are one piece of the puzzle and are designed to complement your own STR program and can be used in conjunction with other publicly-available ML/TF indicators.

During an assessment, FINTRAC will review your policies and procedures to see how you use ML/TF indicators within your STR program. Part of the assessment will include evaluating how the actual policies follow your documented approach and determining its effectiveness with respect to the use of ML/TF indicators. This can include a review of transactions to determine how your STR program identifies potential STRs and assesses them using facts, context and ML/TF indicators. For example, you can receive questions if you have not reported an STR for a client you have assessed as high risk and that client activity also matches against multiple ML/TF indicators.

Combination of facts, context and ML/TF indicators

If the context surrounding a transaction is suspicious, it could lead you to assess a client's financial transactions. Facts, context and ML/TF indicators need to be assessed to determine whether there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. On its own, a single financial transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the associated individual or their actions may help you reach the reasonable grounds to suspect threshold.

Alert or triggering system

FINTRAC acknowledges that a reporting entity may have developed a system that relies on specific alerts or triggering events to signal when to assess a transaction to determine if an STR should be submitted to FINTRAC. If you rely on such a system, FINTRAC expects that you review the alerts in a timely manner in order to determine if an STR should be submitted. Regardless of how you choose to operationalize these ML/TF indicators, FINTRAC expects that you will be able to demonstrate that you have an effective process to identify, assess and submit STRs to FINTRAC.

General ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected money laundering and/or terrorist financing. The ability to detect, prevent and deter money laundering and/or terrorist financing begins with properly identifying the person or entity in order to review and report suspicious financial activity.

As a real estate developer, broker or sales representative, you may observe these ML/TF indicators over the course of your business activities with a client. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

ML/TF indicators related to identifying the person or entity

The following are examples of ML/TF indicators that you may observe when identifying persons or entities.

- There is an inability to properly identify the client or there are questions surrounding the client's identity.
- The client refuses or tries to avoid providing information required or provides information that is misleading, vague, or difficult to verify.

- The client refuses to provide information or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification presented by the client cannot be verified (e.g. it is a copy).
- There are inconsistencies in the identification documents or different identifiers provided by the client, such as address, date of birth or phone number.
- Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Client displays a pattern of name variations from one transaction to another or uses aliases.
- Client alters the transaction after being asked for identity documents.
- The client provides only a non-civic address such as a post office box or disguises a post office box as a civic address for the purpose of concealing their physical residence.
- Common identifiers (e.g. addresses, phone numbers, etc.) used by multiple clients purchasing properties that do not appear to be related.
- Transactions involve individual(s) or entity(ies) identified by media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client are difficult.

ML/TF indicators related to client behaviour

The contextual information acquired through the know your client (KYC) requirements or the behaviour of a client, particularly surrounding a transaction or a pattern of transactions, may lead you to conduct an assessment in order to determine if you are required to submit an STR to FINTRAC. The following are some examples of ML/TF indicators that are linked to contextual behavior and may be used in conjunction with your assessment and your risk based approach.

- Client makes statements about involvement in criminal activities.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client exhibits nervous behaviour.
- The client refuses to provide information when required, or is reluctant to provide information.
- Client has a defensive stance to questioning.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client avoids contact with reporting entity employees.
- The client refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect.
- The client exhibits a lack of concern about higher than normal transaction costs or fees.
- Client makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for source of funds.

ML/TF indicators related to the person/entity financial profile

Clearly understanding the expected activity of a person or entity will allow you to assess their financial activity with the proper lens. For example, a person who is unemployed but has a very large budget to purchase a home may be conducting a financial transaction atypical of what is expected. The following are some examples of ML/TF indicators linked to person/entity profile.

- The transactional activity (level or volume) suddenly changes and/or is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- Client appears to be living beyond their means.
- Rounded sum transactions atypical of what would be expected from the client.

- Size or type of transactions atypical of what is expected from the client.
- There is a sudden change in client's financial profile, pattern of activity or transactions.
- Client uses notes, monetary instruments, or products and/or services that are unusual for such a client.
- Client uses multiple accounts at several financial institutions for no apparent reason.
- Suspected use of personal funds for business purposes, or vice-versa.
- Use of multiple foreign bank accounts for no apparent reason.

ML/TF indicators based on atypical transactional activity

There are certain transactions that are outside the normal conduct of your everyday business. The following transactions are examples that may be indicative of a suspicious transaction, and would require additional assessment.

- A series of complicated transfers of funds for a deposit that seems to be an attempt to hide the source of the funds.
- Transaction is unnecessarily complex for its stated purpose.
- Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- Transaction consistent with publicly known trend in criminal activity.
- Client transacts using musty, odd smelling or extremely dirty bills.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).

ML/TF indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML/TF offence. There are multiple thresholds which trigger reporting/identification requirements by a reporting entity. Some examples of ML/TF indicators which may be indicative of a person or entity attempting to evade identification and/or reporting thresholds are listed below.

- Client appears to be structuring amounts to avoid client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid client identification or reporting thresholds.
- Multiple transactions conducted below the reporting threshold within a short time period.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client exhibits knowledge of reporting thresholds.

ML/TF indicators related to transactions that involve non-Canadian jurisdictions

There are certain types of transactions that may involve jurisdictions outside of Canada where there is higher ML/TF risk due to more permissible laws or the local ML/TF threat environment. The following are examples to consider when making an assessment of the real estate transaction conducted by a person/entity through your business.

- Transactions with a person who lives in or an entity that operates out of a jurisdiction that is known to be at a higher risk to facilitate ML/TF.
- Transactions involving a person who lives in or an entity that operates out of a location of concern, which can include jurisdictions where there are ongoing conflicts (and periphery areas), countries with weak money laundering/terrorist financing controls, or countries with highly secretive banking or other transactional laws such as transfer limits set by a government.
- Transactions involving any countries deemed high risk or non-cooperative by the Financial Action Task Force.

Due to the ever-evolving nature of the ML/TF environment, high risk jurisdictions and trends are often subject to change. To ensure that you are referencing accurate information, FINTRAC encourages you to research publicly-available sources on a regular basis to support these ML/TF indicators as part of your STR program. There are multiple sources that identify jurisdictions of concern, including the FATF which publishes contextual information on high-risk jurisdictions in relation to their risk of money laundering and terrorist financing. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorists operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk based approach and internal STR program.

ML/TF indicators related to use of other parties

In the course of a ‘normal' real estate purchase or sale, there are a ‘normal' number of parties who are engaging in the transaction, depending on the nature of the transaction at hand. For example, in the instance of a real estate purchase, there are generally two parties to the transaction: the individual(s) selling a property and the individual(s) purchasing the property.

Transactions that involve parties not typically associated with a transaction can present an elevated risk of money laundering and/or terrorist financing. These additional parties can be used to allow a criminal to avoid being identified or being linked to an asset. This section includes examples of how the involvement of other parties may be indicative of the structure of a criminal enterprise. Some examples of such other parties include the use of a third party, nominee or gatekeeper.

Use of third party

A third party is any individual or entity that instructs someone to act on their behalf for a financial activity or transaction. There are some situations where there is an apparent and discernable rationale for the inclusion of the third party in a transaction and this may not be suspicious. However, you may become suspicious in a situation where the reason for a third party acting on behalf of another person or entity does not make sense based on what you know about the client or the third party. Use of third parties is one method that money launderers and terrorist financiers use to distance themselves from the proceeds of crime or source of criminally obtained funds. By relying on other parties to conduct transactions they can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Some examples of ML/TF indicators related to the use of a third party indicators can be found below.

- Unrelated parties with no apparent relation to the person/entity provide a deposit for the transaction.
- A client conducts transaction while accompanied, overseen or directed by another party.
- Client appears or states to be acting on behalf of another party.

Use of nominee

A nominee is a particular type of other party that is authorized to conduct transactions on behalf of a person of entity. There are legitimate reasons for relying on a nominee to conduct financial activity of behalf of someone else. However, this type of activity is particularly vulnerable to ML/TF as it is a common method used by criminals to distance themselves from the transactions that could be linked to suspected ML/TF offences. Below are some examples of ML/TF indicators relating to the misuse of nominees.

- An individual or entity other than the person or entity purchasing or selling property conducts the majority of the transaction activity which seems unnecessary or excessive.
- Client is involved in a transaction that is suspicious but refuses or is unable to answer questions related to the transaction.

Use of gatekeeper

A gatekeeper is an individual who controls access to the financial system and can act on behalf of a client. Such services can be abused so that criminals have access to the financial system without being identified. Gatekeepers may include lawyers, accountants and other professions which can access the financial system on behalf of a client. While there are many transactions where it is ‘normal' to have a gatekeeper represent the interests of a client, such an appearance of normalcy can also be utilized to the advantage of criminals to provide the veneer of legitimacy to their transactions. The use of gatekeepers themselves is not an indicator of an ML/TF offence. However, entities should consider the following examples which can indicate misuse of the financial system access provided to gatekeepers.

- Gatekeeper avoids identifying their client or disclosing their client's identity when such identification would be normal during the course of a transaction.
- Gatekeeper is willing to pay higher fees and seeks to conduct the transaction quickly when there is no apparent need for such expediency.

Indicators related to terrorism financing

In Canada, terrorist financing offences make it a crime to knowingly collect or provide property, which can include financial or other related services, for terrorist purposes. This section is focused on examples that are specific to the possible commission of a terrorist financing offence. However, please note that the other ML/TF indicators in this guidance may also prove relevant in determining when you have reasonable grounds to suspect the commission of terrorist financing as the methods used by criminals to evade detection of money laundering are similar.

Indicators specifically related to terrorist financing:

These are some examples of indicators relating to terrorist financing.

- Transactions with a person who lives in or an entity that operates out of certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individual(s) or entity(ies) identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individual(s) or entity(ies) may be linked to a terrorist organization or terrorist activities.
- Individual or entity states or eludes that they support violent extremism or radicalization.
- Client provides multiple variations of name, address, phone number or additional identifiers.

Indicators specific to real estate agents and developers

In addition to the general ML/TF indicators that have been highlighted in this guidance, there may be more specific ML/TF indicators related to your business, when you act as an agent in the purchase or sale of real estate or as a real estate developer, when you sell a new house, a new condominium unit, a new commercial or industrial building or a new multi-unit residential building to the public. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Client arrives at a real estate closing with a significant amount of cash.
- Client purchases property in someone else's name such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.

- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client negotiates a purchase for the market value or above the asked price, but requests that a lower value be recorded on documents, paying the difference “under the table”.
- Client pays initial deposit with a cheque from a third party, other than a spouse or a parent.
- Client pays substantial down payment in cash and balance is financed by an unusual source (for example a third party or private lender) or offshore bank.
- Client purchases personal use property through his or her company when this type of transaction is inconsistent with the ordinary business practice of the client.
- Client purchases multiple properties in a short time period, and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property.
- Client insists on providing signature on documents by fax only.
- Client over justifies or over explains the purchase.
- Client's home or business telephone number has been disconnected or there is no such number.
- Client uses a post office box or General Delivery address where other options are available.
- Client wants to build a luxury house in non-prime locations.
- Client exhibits unusual concerns regarding the firm's compliance with government reporting requirements and the firm's anti-money laundering or anti-terrorist financing policies.
- Client exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- Client persists in representing his financial situation in a way that is unrealistic or that could not be supported by documents.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- A transaction involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions in which the parties show a strong interest in completing the transaction quickly, without there being good cause.
- Transactions in which the parties are foreign or non-resident for tax purposes and their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying).
- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments.
- Transactions which are completed in seeming disregard of a contract clause penalizing the buyer with loss of the deposit if the sale does not go ahead.
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Transaction is completely anonymous–transaction conducted by lawyer–all deposit cheques drawn on lawyer's trust account.

Indicators specific to real estate brokers and sales representatives

In addition to the general ML/TF indicators that have been highlighted in this guidance, there may be more specific ML/TF indicators related to your business as a real estate broker or sales representative. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program.

- Client sells property below market value with an additional “under the table” payment.
- Client purchases property without inspecting it.

- Client is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided.
- Client buys back a property that he or she recently sold.
- Frequent change of ownership of same property, particularly between related or acquainted parties.
- If a property is re-sold shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.

Please refer to the FINTRAC Operational Brief which provides ML/TF indicators that are intended to assist reporting entities involved in real estate transactions to meet their obligations to report suspicious transactions or attempted suspicious transactions that are related to the commission or attempted commission of a money laundering or terrorist financing offence.

Date Modified:

2019-08-16

Appendix 8

Appendix 9

Grant Thornton – *Reporting Entity Sector Profiles: Money Laundering and Terrorist Financing Vulnerability Assessments, prepared for FINTRAC* – March 31, 2014

Grant Thornton

Reporting Entity Sector Profiles

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. Introduction

Grant Thornton was retained by FINTRAC to conduct an information and intelligence gathering exercise, in relation to industry sectors covered by the Proceeds of Crime (Money-Laundering) and Terrorist Financing Act (the "PCMLTFA") and regulations, in order to assist in preparing sector risk profiles for money laundering and terrorist financing, including Grant Thornton providing a comparative analysis of the sector risks.

The purpose of the exercise was to enable FINTRAC to have a better understanding of the sectors and with a focus more on the structure of each sector in the identification and assessment of risk.

Our work involved accessing a number of different information sources, including obtaining privileged insights and information from knowledgeable industry insiders and other sector experienced and expert individuals. FINTRAC provided a prioritized list of the sectors and this was utilized to organize our efforts. This prioritized list is detailed below:

- Real Estate
- Dealers in Precious Metals & Stones (DPMS)
- Securities Dealers
- Accountants
- Life Insurance
- British Columbia Notaries (BC Notaries)
- Credit unions
- Casinos
- Financial Entities
- Lawyers
- Money Service Businesses (MSB's)

This was not an exercise to simply document how money laundering was, or may be, occurring in each sector; while in some cases we did seek and receive the opinions of persons we interviewed on this, the work effort undertaken was broader. We really attempted to obtain a deeper understanding of how individuals and companies within the sectors worked as potentially related to risk areas. The resulting sector profiles report reflects our prioritized efforts, meaning simply that we conducted more interviews with people for the higher prioritized sectors and this accordingly provided us with a greater amount of privileged insights and information. As well, interviews resulted from the people available and willing to speak with us.

We understand that this resulting report will inform the work that FINTRAC does in several areas, including possibly their work with each sector specifically.

1.1 Methodology and approach

1.1.1 Information gathering: Methodology and approach

Our methodology involved information gathering from four primary sources:

1. Review of relevant authoritative anti-money laundering ("AML") guidance, e.g. Financial Action Task Force ("FATF") sector guidance; other country sector risk assessments;

2. Public records research including news media, Statistics Canada, market and sector economic data industry statistics, etc.;

3. Interviews with Grant Thornton Canadian sector and international AML specialists; and

4. Interviews with industry insiders in each of the ten sectors.

1.1.2 Compilation and review of relevant authoritative AML materials

We conducted a detailed search and review of contemporary authoritative AML materials focusing on surveys, case studies, typology studies, risk assessments and other reports in order to facilitate our development of a 'Discussion Tool' to assist our interviews. We collected an extensive range of materials from around the world in order to guarantee a broad reach and coverage in this aspect of the research; the materials were not restricted to Canada.

1.2 Public records research undertaken

Our public records research included the use of a range of specific tools which were used in a number of ways to maximize coverage for each of the research phases. We conducted searches within Canada and also internationally. Phase one of our research focused on identifying relevant information to build out data for each of the following reported on sections:

- General sector profile;
- Economic and financial statistics;
- Structure of sector;
- Size and segmentation of sector;
- Entity population, primary and secondary;
- Regulatory environment of sector; and
- Description of any associations that exist.

Phase two of our research was more focused and concentrated on the following:

- Products and services offered, including consideration for more cash intensive products/services;
- Delivery channels;
- Emerging trends, new products and services in future;
- Types of customer, including consideration for proportion of high risk customers; and
- Geographic considerations (operations, where business is conducted, where there is a presence (direct and indirect), international transactions).

Phase three of our research really focused on developing further the data obtained from the other research sources, including determining:

- Any other relevant information;
- Commonly understood money laundering and terrorist financing risk and vulnerabilities;
- Typologies including: use of agents, brokers, cross border movement of funds, current vulnerabilities and emerging/potential vulnerabilities; and
- Understanding further any specific regulations/guidelines in place, market entry barriers and controls.

These research topics mirrored closely the areas requested by FINTRAC and the section headings delivered in our final sector profiles report. The research tools used were as follows:

- News media databases (Factiva, Lexis and Infomart);
- Corporate information databases (OneSource, Factiva, Dun & Bradstreet);
- Litigation databases (Quicklaw);
- Industry classification codes and related tools;
- Internet based research including, Statistics Canada, market and sector economic data websites, trade and industry publications, regulators and sector associations etc.; and
- Library research (various ML/TF related books).

1.3 Experienced sector knowledge

We were fortunate to be able to have discussions with many individuals who spoke freely and frankly with us and who provided valuable insights into the work and reality of the sector they were involved with. These individuals understood that we were undertaking research on the sectors in regards to money laundering and terrorist financing risks and that we would keep their input anonymous. We completed 57 interviews as follows:

Sector	Number of Interviews
Real Estate	7
DPMS	6
Securities	10
Accountants	5
Life Insurance	2
BC Notaries	1
Credit Unions	7
Casinos	2
Financial Entities (other than credit unions)	6
Lawyers	6
MSBs	5

1.4 Risk factor identification and assessment

Based on the research completed, we developed and documented specific risk factors for each of the sectors. The factors were determined in large part from the interviews undertaken, our own experiences with different clients, projects and investigations within the sectors and our review of the other sector profile information. We had the opportunity in some cases to review the risk factors initially identified with sector expertise, specifically we were able to have Grant Thornton sector experts review the risk factors developed to obtain their further input.

The risk factors identified were generally organized into the following headings for each sector:

- General market;
- Product and service;
- Delivery channel;
- Geography;
- Business relationships/linkages with other sectors;
- Transaction methods and types; and
- For Accountants and Lawyers, as service providers to other sectors, client type and characteristics.

Once identified, the risks by sector, grouped according to the list above, were pulled together in a schedule format for further review and to assist with the assessment and comparative analysis. At this point we then conducted a global review of the identified sector risk factors and this level of review enabled us to identify risk factors which had been identified specifically in one sector and were also applicable to others.

Based primarily on the privileged insights information gathered through the interviews and our own experiences, each risk factor grouping was rated. A four point scale (low, medium, high, and very high) was used for the rating; the rating was determined primarily through the consideration of the probability or likelihood that the risk would materialize and the impact of it materializing. Our assessment, while subjective, was based on the information known and available to us and we exercised our professional judgment.

2. Key risk factors identified and assessment

As indicated, key risk factors were identified for each of the sectors researched and we then determined a rating for each risk factor grouping by sector and this is documented in the attached Table 1. A number of our observations are noted below.

2.1 General market and delivery channel risk factors

Market competitiveness and the structures in place to support the quality of services provided and the ethics of individual persons working within the sector are of critical importance. This became clear both as a general market condition and when trying to understand how the size of the party within the sector impacted their vulnerability to abuse for money laundering and terrorist financing. Based on the research performed, these areas are of critical importance for the real estate and money service businesses sectors. Our research indicates that at the smaller end of the market there is often no quality and ethics infrastructure in place for these sectors. This is also the case for the securities, accountants, lawyers and credit union sectors except that while there is no or limited infrastructure in place at the smaller end of the market, there is a regulated environment for these sectors which to some extent mitigates the vulnerability.

These factors were given a higher weighting for the determination of risk for these sectors.

2.2 Geography risk factors

The purchase of Canadian real estate assets with offshore money and/or by offshore persons was noted as a significant risk factor. Similarly, the purchase of investment assets whether the Canadian or other markets, through Canadian securities firms with offshore money, particularly through the use of off shore companies, in some cases institutional accounts, was noted as a significant risk. These factors were given higher weighting in the determination of risk.

The ability to access global markets through Canadian sector participants, particularly via dealers in precious metals, credit unions, financial entities and MSBs was rated higher for money laundering and terrorist financing vulnerability risks.

2.3 Business relationships/linkages risk factors

The use of legal trust accounts was noted specifically as an area of concern, particularly for the real estate, accounting and legal sectors.

The concept of the 'gatekeeper role' came through in our research for each of securities, accounting, life insurance, MSB's and the legal sectors.

These factors were given higher weighting in the consideration of risk.

2.4 Transaction methods & types risk factors

The use of corporate vehicles was specifically noted as a higher risk factor in the real estate and securities sectors and is generally seen as a method to conceal ownership, source and purpose of funds/transaction and adds to the opacity of the environment. Given the lack of accessible resources in the Canadian market (to research corporate ownership) this was assessed as a higher risk factor.

2.5 Customer types and characteristics risk factors

This category and grouping of risk was seen as generally applicable across all sectors and it was not one we concentrated on in conducting the research as the focus was intended to be more on the structured risk of the sector rather than the user of sector services. However, in reviewing the sectors researched, it was noted that the accounting and legal sectors are both ones which provide professional services across and within markets and also to participants of the other sectors researched. For each of these two sectors, our knowledge and experience indicates a wide range of customer due diligence and acceptance policies and procedures and that at the smaller end of the market, practices varied considerably. Accordingly, these risk factors were rated higher when assessing risk.

3. Comparative analysis

The focus of our work prior to the completion of the comparative analysis was the identification and assessment of risk factors, and was aimed at understanding and assessing the inherent risk of each of the risk factors.

In performing the comparative analysis we have tried to consider further elements, including:

- Levels of awareness within each sector of money laundering and terrorist financing issues and compliance activity/engagement with the PCMLTFA;
- Interplay and linkages between the sectors including awareness of risk and consideration of this by other sectors of sector participants;
- Sectors where the participants have gatekeeper roles;
- Attractiveness to potential money launderers; and
- To some degree, (based on our knowledge and experience) the mitigating controls in place by sector participants, and in some cases, controls which are starting to be viewed as "best practices". A best practice example would be a financial institution's requirement for, and review of, other entities' independent compliance regime review reports.

Accordingly, this analysis provides a comparative rating of the unmitigated risk, as either higher, medium or lower. Provided below is an outline of our reasoning as to the sector ratings.

3.1 Sectors rated with higher comparative risk

3.1.1 Real Estate

This sector is rated as higher as it is our understanding that significant portions of the sector are apparently unengaged (specifically the smaller end of the market) in AML compliance, and other sectors (e.g. banking and securities) are not sufficiently viewing this sector as one with higher risk transactions, meaning that higher degrees of scrutiny are not being applied.

Of concern was an example shared by an interviewee wherein Canadian banks would not be involved in transactions between parties and accordingly, transaction activity could not be identified and monitored by Canadian regulated entities even though Canadian real estate was involved.

There are many participants in the marketplace and they are not necessarily seen by other sectors as high risk or having the potential for high risk; e.g. real estate companies, realtors, property owners and finance companies.

In general, it is understood that real estate transactions involve lawyers and their trust accounts, and this assistance can knowingly or unknowingly provide legitimacy and/or obscure the source of illegally sourced funds. As well, at the smaller end of the market there reportedly continues to be a high number of cash transactions.

3.1.2 DPMS

This sector is similarly rated as higher, as the levels of awareness and AML compliance engagement by sector participants was cited as lower. As well, there reportedly continues to be a high number of cash transactions and a higher number of smaller players.

The barriers to entry are generally low, except for the diamond industry, and can attract illicit funding. While it is evolving in the right direction, scrutiny of this sector's participants and transactions has not been as rigorous by the banking sector as it has been with other sectors (e.g. MSBs).

3.1.3 Securities

This sector is rated as higher as the exempt market products and dealers were cited as significant risk areas for illegal funds; and as well, it is our understanding that other sectors (e.g. banking) are not sufficiently viewing transactions within this sector as having the potential for higher risk.

Specifically, while the larger and/or bank-owned participants are highly regulated, by other regulators (e.g. IIROC, provincial securities commissions), one particular segment exposes the entire sector – the exempt market. Exempt market dealers can access capital funding privately and often these transactions are not scrutinized as high risk by other participants in the securities sector and by banks and other financial institutions. While there is high interaction amongst participants (e.g. a securities broker can be a client of another broker), the market does not generally see this as a risk, as there is an expectation that other sector participants and regulators are doing the work that needs to be done (background checks and other know your client procedures for example). The focus of know your client is primarily to support investor protection and not on the risks of money laundering and terrorist financing.

Transactions in this sector can involve large dollar amounts, conducted by accredited investors who are typically individuals with a high net worth. Clients may be international and the transactions activity, movement of funds are not always well understood.

3.1.4 Accountants

Risk for this sector is rated higher given the breadth of services provided, the value of the services to facilitate the movement of funds and particularly the inherent risk at the smaller end of the market. While PCMLTFA regulated activities performed by accountants are considered fewer (as a portion of the activities of accountants as a whole) and are not expected to occur on a large scale; the accountant in the gatekeeper role is a higher risk. Accountants, through association, are often perceived to provide legitimacy to transactions and the individuals and organizations involved with the transactions and businesses; most of the services provided by accountants to their clients are not subject to PCMTLFA regulations.

The sector self-regulation is seen as a mitigating control, although these primarily consider professional standards and the delivery of client work as opposed to the risks of money laundering and terrorist financing.

Effectiveness of the sector's self-regulation is understood to be dependent upon the sector being well aware of its vulnerability to money laundering and terrorist financing risks and abuses. While some are aware conceptually of the risk of how a gatekeeper role might assist money laundering and terrorist financing objectives, this is not generally considered or well understood, except where there are specific client acceptance procedures designed to address this. We note that while there are some cases of specifically designed procedures, this is not understood to be occurring generally throughout the sector.

3.1.5 Lawyers

Risk was rated higher for this sector. Not only was the use of a lawyers' trust account cited as a risk factor for this sector (this was expected and generally is a known risk factor), the use of legal trust accounts, sometimes in conjunction with solicitor/client privilege, came up in our research of the banking and accounting sectors.

Specifically, individuals interviewed as part of the research conducted, shared that they had been confronted with the challenge of not being able to obtain further factual information about the source and use of funds when funds were being transacted through legal trust accounts.

The services of lawyers are fundamental to many real estate transactions, however the level of a lawyer's client due diligence is often self-determined. Our experience is that the risk of the legal gatekeeper role being abused by those with money laundering goals are not generally reviewed for, or considered in this sector. Even if a lawyer were to identify illegal activity, professional standards often prevent disclosure. However, similar to the accounting sector, the level of client due diligence is often correlated with the size of the market participant (independent lawyer versus larger firms managing reputational risk). Notwithstanding this, we are aware of instances where larger firms had client relationships, minimal client due diligence had been performed and specific risk factors were present.

Larger, international law firms expose the Canadian market to foreign, higher risk clients.

3.1.6 BC Notaries

Similar to lawyers, BC Notaries were rated higher risk due to their gatekeeper role, and that they can act in conjunction with bankers, accountants and lawyers. It is noted as a smaller sector and risk is therefore limited given their size and scope (less potential impact). The use of the notary trust account is understood to be the main risk factor.

3.2 Sectors rated with medium and lower comparative risk

The sectors which were rated medium and lower were found to be ones where individuals working within the industry have a higher degree of knowledge and awareness of money laundering and terrorist financing risk factors and generally sectors where anti-money laundering compliance activity is more entrenched. For example, in industries with larger players and better knowledge, we have assessed the comparative risk as lower given that demonstrated, more comprehensive and more effective anti-money laundering programs and continued vigilance is higher. The reasons for this entrenchment are noted as primarily the effect of other regulators (in the case of financial entities, credit unions and casino sectors) or other business partner scrutiny (e.g. MSB sector).

Our more detailed observations are provided below.

It continues to be imperative that the medium and lower rated sectors remain vigilant in their anti-money laundering efforts as the inherent risks are in many cases, high and very high.

3.2.1 Life Insurance

This sector has been rated as lower comparative risk. In our experience the products are not as easily utilized or targeted by money launderers, however, we have seen instances were life insurance products were used for fraud and money laundering.

The sector is dominated by larger players, which means that broadly there is funding for anti-money laundering compliance structures, programs and positions. Although money laundering may be a lower risk in the insurance industry, there are some indications that when the sector is targeted, it is done so by more sophisticated criminals and schemes. Once again, continued vigilance and focused learning from actual sector examples are required.

3.2.2 Credit Unions

We rated this sector with a medium comparative risk rating. While credit unions have a large exposure to potential money laundering and terrorist financing, serve a wide customer base and offer a multitude of various financial products, our research and discussions generally found the industry to be well informed of the requirements and in general, their exposure. The industry is going through some consolidation and this will evolve to provide the larger credit unions with more resources to implement the necessary controls.

Higher risk areas include where a credit union has other lines of businesses including insurance and wealth management products as these have not yet been made subject to the same level of control and monitoring that the core business areas have.

Credit unions generally serve a local community or region and their exposure to international markets would be less than those of Canada's large banks.

The credit union system nationally continues to be fragmented, with a high number of smaller organizations, often working together in smaller groups and/or receiving support from provincial centrals to deal with and address compliance issues. This results in inconsistencies and does not deliver the level of effectiveness that could be achieved if the system worked together to address as a whole. The size of the credit union/caisse populaire sector across the country is generally understood to be equivalent to the size of one of Canada's large banks.

3.2.3 Casinos

While casinos have traditionally been viewed as a higher risk industry internationally for money laundering, in Canada the risk is seen to be lower as Canada is not viewed as an attractive market for gambling. The Canadian casino sector serves mainly local clients. We rated this sector as lower comparatively.

There are a higher number of larger operators, heavy regulation on the sector, and focused police monitoring within the local communities. However, the gaming sector broadly is evolving to much more of an online platform, supporting online payments and transaction processing, new technologies, involvement of operators and suppliers out of the country and these are all serving to increase the risks of abuse for money laundering purposes. While online gaming is not PCMLTFA regulated, it has received some scrutiny from the banking sector; however this appears to have simply moved operators to offshore locations.

3.2.4 Financial Entities

While the inherent risks are very high for many of the products and services, particularly the access to international markets, ability to move money across currencies and countries, we have rated this sector comparatively lower.

Particularly for the larger institutions, the level of resourcing and focus on compliance program objectives is high and entrenched. This considers client due diligence and transaction monitoring, that inherent risk in many ways have been identified and are well understood and being managed, even if not also being effectively mitigated.

The regulatory regime requirements of both OSFI and FINTRAC are understood to have resulted in a higher level of overall awareness and appreciation for what needs to be done to comply with requirements. While the sector serves a diverse background of clients domestically and internationally and through significant foreign operations, compliance departments have in many cases identified these as risk areas and are in the process of monitoring or developing controls to monitor, especially in light of infractions by other banks internationally. AML professionals within this sector, in many cases, are starting to see and deal with issues beyond regulatory compliance. For example, there is a better understanding (not yet a solution) of the consequences of de-marketing/terminating relationships, the desire and need to work with FINTRAC, other intelligence and police agencies to make the whole regime work, not only nationally but internationally as well.

Certainly for smaller financial institutions, which have higher inherent risk (pressure to book business), less resources available, the risk is sees as comparatively higher. However, these organizations tend to be more niche market and thus the compliance program can be more focused and this can in turn support effectiveness.

In many cases it appears that where the banking sector has executed on money laundering risk mitigation effort, this has resulted in significant change within a sector; for example, the banking sectors' consideration and scrutiny of the MSB sector. However, the converse is also true, where there has not been a focused level of risk identification and monitoring, there has correspondingly been less movement towards anti-money laundering compliance broadly within the sector. Also, sectors where transactions are conducted where alternatives to banking are available have more risk.

3.2.5 Money Service Businesses

Money Service Businesses have been higher risk in the past but are viewed currently as a medium risk. The sector has been the subject of significant scrutiny by their banking partners and there have been definite improvements in anti-money laundering compliance across the sector. Although this is positive news, there is no room for complacency as generic factors including global money flows, immigration and economic patterns still mean that there is considerable risk.

This is another sector where the market has few larger players and the smaller businesses struggle with funding for compliance structures and adequate transaction monitoring. The experiences in Quebec and other locations have shown that regulation and enforcement have driven some rogue players underground but they are still to be found on the internet. The recent development of an active industry association is one example of how further gains can be made to increase awareness, and raise the bar as the sector evolves. There is opportunity for strategic level initiatives to have a significant impact on the sector as a whole in helping it to further reduce risks.

The market is highly fragmented and knowledge and awareness of money laundering risks is at time perceived not to be high in certain subsectors. However, this is the exception, the larger players in the sector are knowledgeable and the compliance resources and regimes are becoming more sophisticated. Again, given the less complex services offerings of many of these organizations, the opportunity exists for transaction monitoring and compliance regimes to be highly effective.

Higher risk areas include MSBs that don't have bank accounts or that work exclusively with foreign financial institutions. We are aware of cases where there is significant reliance on foreign financial institutions, to

comply with rules and report in the foreign jurisdiction, as well as reliance on alternative banking service providers; e.g. other MSBs.

The attached Table 1 documents the "overall comparative risk rating" as determined for each sector and should be considered only in conjunction with this report.

Grant Thornton

Reporting Entity Sector Profile: Real estate

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

Canada's real estate market is known for its maturity and stability which continues to attract buyers from both domestic and international markets. Over the past two decades, it has also seen significant growth, over 130% since 1975 and 49% in the last ten years[1]. National geography is an important factor in the size and vibrancy of market sectors with the largest and most active elements in the major urban centres.

Urbanization continues to be the major trend in development with both new and redevelopment projects including mixed use projects. Retail markets remain active and house prices and the availability of homes continue to be significant topics of discussion at all levels.

Canada is also a world leader in the development of major assets through Public Private Partnerships ("PPP").

The market is divided into a number of segments: residential and commercial (office, retail, industrial, residential) brokers and agents, construction, developers, building managers and mortgage brokers.

There are over 538,000 reporting entities (including employers and others including individual agents) in the sector. The construction and real estate segments together, representing the whole sector, account for almost 20% of the Canadian economy.[2]

A significant number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Use of foreign money to purchase real estate
- Quality of the real estate property including higher end residential properties, lower dollar value commercial properties, type and location of the property
- High level of accepted cash transactions
- Private lending and the 'legitimizing' use of lawyers trust accounts
- Broker/realtor oversight (relative lack of)
- Discrepancies in AML awareness and compliance across the sector

1 The Economist – Global interactive house price guide
2 Industry Canada, Canadian Industry Statistics - http://www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/home

2. Structure, size and segmentation, reporting entity population

The Canadian real estate industry is structured on a traditional model with developers and builders creating new stock, brokerages and agencies selling it, and managers operating buildings of all types. Mortgage brokers are a segment dealing in only a specific area but many mortgage brokers are also licensed as real estate agents too.

The SIC codes for the industry contain 14 sub-codes as outlined at Appendix A.

The Canadian industry has also seen a significant rise in the creation and growth of Real Estate Investment Trusts in the past four years.

Statistics Canada provides some high level information on the major segments. The smaller segments are more difficult to define and statistical data is scarce. The Statistics Canada breakdown of the major segments is as follows:

Segment	Employers	Non-employers Indeterminate	Total	Notes
Construction	127,255	151,203	278,458	60% are the micro category (1-4 employees)
Real Estate	46,773*	213,237	260,010	75% are in the micro category
Totals	174,028	365,440	538,468	

See detailed charts and statistics at Appendix A[3]

The segments that we have identified as significant are as follows:

- Real estate sales (commercial and residential)
- Construction
- Developers
- Property managers (including rentals/leasing)
- Mortgage Brokers
- REITS (a category of real estate owners but a potential point of entry for ML/TF)

[3] Industry Canada, Canadian Industry Statistics - http://www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/home

Statistics from industry and other relevant sources also provide some statistical information on the sector:

- *Real Estate Brokerages:* There are over 10,000 Real Estate Brokerages in Canada.[4]
- *Real Estate Agents:* There are approximately 100,000 realtors nationally (includes brokers, agents and sales persons).
- *Real Estate Boards:* There are approximately 100 boards nationally, Ontario has 40; the Toronto Real Estate Board alone has approximately 45,000 realtors; British Columbia has 11 boards with approximately 18,000 realtors5; Quebec has 12 boards with 12,000+ realtors[6] and Alberta has 10 boards and 10,000+ realtors[7].
- *Mortgage Brokers:* The Canadian Association of Accredited Mortgage Professionals is a national association that represents Canada's mortgage industry. CAAMP has over 12,000 members, comprising mortgage lenders, brokers, insurers and other industry stakeholders. In 2010 it was reported that there were between 18,000 and 20,000 people who held mortgage agent and/or mortgage broker licenses in Canada. This number accounts for about 10,000 in Ontario and a total of 6,000 in BC and Alberta. (Source: CAAMP)[8]
- *Property Managers:* Statistics Canada figures for this segment number 5,235 employers and 16,582 non employers/indeterminate participants for a total of 21,817. The Building Owners and Managers Association (BOMA) of Canada is has "over 3,200 members in regional associations across Canada"[9]. Other research has identified 1,139 property managers classified under NAICS 53131.
- *REITS:* There are 49 REITs listed on the TSX and TSXV; there are also private REITS.

In a number of places in this report, we have referred to "the lower end" and "the higher end" of the market and of certain groups and segments. It has proven difficult to quantify these categories but the NAICS table for real estate at Appendix A speaks to this based on number of employees in companies in the "employer" category, and the breakdown of these companies by number of employees.

[4] Canadian Real Estate Association - http://www.crea.ca/
[5] British Columbia Real Estate Board - http://www.bcrea.bc.ca/
[6] Quebec Federation of Real Estate Boards - http://www.fciq.ca/
[7] Alberta Real Estate Association - http://www.abrea.ab.ca/
[8] Canadian Association of Accredited Mortgage Professionals - http://www.caamp.org/
[9] The Building Owners and Managers Association of Canada - http://www.bomacanada.ca/

3. Economic and financial statistics

According to Statistics Canada, from January to November 2013, construction contributed $113.4 billion ($113,464,000,000) or 7.06% of Canada's economic output as measured by GDP. This data is similar to the full previous year where construction represented 7.22% of 2012's GDP.[10]

Real Estate (sales) contributed $190 billion ($190,392,000,000) or 11.84% during the same period. This data is similar to the full previous year where Real Estate represented 11.83% of 2012's GDP.[11]

The Canadian real estate sector avoided the worst of the 2008 downturn and continues to show good potential as both the local and US economy improve. The market is very stable and there is generally believed to be little or no oversupply. Expansion is expected to continue with some commentators predicting plateauing in the residential market 2014 and the layoff of workers.

Returns on commercial properties are high and the investment prospects for the real estate market are good with various capital sources for mortgage borrowing also available. Construction in this sector is also predicted to remain strong.

In the commercial segment, capital investment in buildings was relatively stable from 2007 – 2011. Capital investment averaged about $21 billion per year during this period, declining in 2009-2010 period primarily due to the decline in new building construction. Capital investment in the commercial sector in 2011 totalled $21.6 billion.[12]

Canada's commercial property market is estimated to be worth about $1-trillion (U.S.) compared with $11-trillion for the U.S. market. The total annual economic activity for the commercial real estate sector in 2011 is estimated at $63.3 billion.[13]

Capital investment in renovation has been steady. Ongoing operations of commercial buildings generated $3.5 billion in building management fees in 2011 and almost the same amount in commercial brokerage fees.[14]

Total revenues for the residential segment nationally are hard to come by but we have identified some statistics for recent volumes in home sales, by month in major cities. The full table is at Appendix A. The statistics available are for November 2013 and November 2012 for 13 urban centres including the Vancouver area, Calgary, Regina,

[10] Statistics Canada - http://www.statcan.gc.ca/start-debut-eng.html
[11] Ibid
[12] Altus Group Economic Consulting - The Contribution of the Commercial Real Estate Sector to the Canadian Economy, September 2012 - http://c.ymcdn.com/sites/www.realpac.ca/resource/resmgr/research/altus_report_2012.pdf
[13] Ibid
[14] Ibid

Toronto, Ottawa, Montreal and Halifax. They indicate that in 2012 total November home sales for the areas listed equalled $6,887,800,000. The figure for 2013 was $8,487,100,000.[15]

A detailed analysis by The Economist shows that Canada is the most expensive property market globally, with the highest "price to rent" and "price to average income" ratios. Only two countries are higher than Canada for "real terms" pricing and only one country has shown more "percentage growth" than Canada since 1975.[16] A review of historical material from this source indicates that these analytical factors were successfully used to predict market corrections in the USA, Spain and other countries. The Economist has made similar predictions for the Canadian market but despite the figures moving ever higher, this still has not happened. Full details of this analysis are at Appendix A.

[15] Canadian Real Estate Association
[16] The Economist House Price Index - http://www.economist.com/

4. Regulation of the real estate sector

In both the retail and commercial sales segments of the industry, participants belong to the Canadian Real Estate Association (CREA), a national organization which sets the standards of professional conduct for its over 100,000 members who include real estate brokers, agents and salespeople working through 100 real estate Boards and Associations across Canada.

Each province has passed real estate legislation which is in turn managed by provincial and territorial real estate associations. For example, the Real Estate Business and Brokers Act of Ontario and its associated regulations are administered by the Ontario Real Estate Association (OREA) on behalf of the Ontario provincial government. Similar associations exist in the other provinces and territories to govern industry professionals in the real estate, mortgage broker, and real estate appraisal industries under the various provincial Real Estate Acts.

The construction industry is one of the most highly regulated industries in the world. Under Canadian law the regulation of buildings is a provincial responsibility and is carried out through various laws, Acts, codes and regulations, often administered at the municipal level.

Provincial legislation empowers government agencies or departments to regulate a variety of aspects of buildings. For example, laws protecting the safety and health of building occupants. Examples of other relevant legislation are the National Building Code of Canada (NBC) 2010 (design, construction and renovation) and the Ontario Building Code.[17]

In addition to building codes, various miscellaneous Acts cover specific building types or services within buildings, for example; liquor-licensing, hotel, theatre and factory Acts. Fire-prevention bylaws or fire codes also regulate the ongoing safety of existing buildings. Provincial Workplace Safety and Health Acts and municipal codes and city by-laws also impact the industry and more recently, AML/TFD law and regulations allows Fintrac oversight for brokers, agents and developers.

We have not identified any law or oversight mechanism relating to the purchase of Canadian real estate by non-residents. We do note however that Section 116 of the Income Tax Act creates a requirement for non-resident vendors of certain types of Canadian real estate assets to notify the Canada Revenue Agency (CRA) about their disposition and may be responsible for withholding a portion of the proceeds of the sale to cover potential taxes owing by the vendor.[18]

[17] The Canadian Encyclopedia – Building Codes and Regulations
[18] Income Tax Act (R.S.C., 1985, c.1 –s 116 – disposition by non-resident person of certain property - http://laws-lois.justice.gc.ca/eng/acts/I-3.3/section-116.html

5. Educational and licensing requirements

Provincial regulators are charged with establishing the educational and licensing requirements for participants in the real estate industry. Licensing requirements vary across Canada, but all provinces and territories require prospective salespeople and brokers to pass a written exam. The courses offered cover the rules and regulations associated with the real estate profession, and the laws governing the sale and acquisition of property. In addition, they explore the ethical and practical guidelines to working in the profession.

Continuing education is also required in many provinces for real estate professionals to maintain their licenses by staying up to date about current developments in the profession and industry. Once a person is licensed through the provincial regulator they are then able to become a member of a local Board and CREA and ultimately practice as a realtor.

In Manitoba, the real estate division of the Manitoba Securities Commission is responsible for administering The Real Estate Brokers Act and The Mortgage Brokers Act. Similar to the other provincial associations, this division registers real estate brokers, salespersons, and mortgage brokers, monitors brokers' trust accounts, and investigates complaints against real estate brokers, salespersons and mortgage brokers.[19]

At the market level, local real estate boards (e.g. Toronto Real Estate Board, Real Estate Board of Greater Vancouver, REALTORS® Association of Grey Bruce Owen Sound) are responsible for processing membership, and the recording and collection of dues. They also operate the Multiple Listing Service® that in turn provides data for display on either the residential or commercial properties web site. The local board develops and implements the regulations that support CREA's national policies, and is responsible for the enforcement of the Code of Ethics and the Standards of Business Practice.

In general, mortgage brokers in Canada are licensed at the Provincial level (e.g. in Ontario with the Financial Services Commission of Ontario and in BC with the BC Financial Services Commission). Mortgage Brokers are governed by the relevant provincial legislation (Ontario – Mortgage Brokers, Lenders and Administrators Act, 2006 and British Columbia Mortgage Brokers Act). To earn a license one must complete the requisite education provided by accredited education providers on a Provincial level.

[19] The Manitoba Securities Commission –http://www.msc.gov.mb.ca/real_estate/index.html

6. Constraints

None identified at this point.

7. Description of sector associations

Our research has identified the following Canadian real estate related associations:

- *CREA – Canadian Real Estate Association –* membership includes more than 100,000 real estate brokers, agents and salespeople, working through 100 real estate Boards and Associations across Canada. Assists realtor members to better serve their clients and represents the interests of its members to the federal government and its agencies on existing or proposed legislation that will affect those members, and/or impact homeownership.

- *BOMA - Building Owners and Managers Association Canada –* is the voice of the Canadian commercial real estate industry. BOMA Canada addresses issues of national concern, and promotes excellence in the industry through information, education advocacy and recognition on behalf of the building owners, managers, developers, facilities managers, asset managers, leasing agents, brokers, and the product and service providers to over 2.1 billion square feet of commercial real estate in Canada.

- *REALpac - Real Property Association of Canada –* Canada's senior national industry association for owners and managers of investment real estate. Members include publicly traded real estate companies, REITs, private companies, pension funds, banks and life insurance companies with investment real estate assets each in excess of $100 million.

- *CCA – Canadian Construction Association –* an association of construction practitioners who join CCA through their local or provincial construction association. CCA gives voice to the public policy, legal and standards development goals of contractors, suppliers and allied business professionals working in, or with, Canada's non-residential construction industry.

- *CHBA – Canadian Home Builders Association –* is an association representing the residential construction industry.

- *NAIOP - National Association of Industrial and Office Properties –* Trade association for developers, owners and investors in industrial, office and related commercial real estate.

- *RECO – Real Estate Council of Ontario –* regulates real estate trade on behalf of the Ontario government.

- *SIOR – Society of Industrial and Office Realtors*

- *REIC – Real Estate Institute of Canada* is a not for profit organization that has been educating and certifying specialists in real estate since 1955.

- *UDI – Urban Development Institute –* The UDI is a national non-profit association of the development industry and its related professions that is non-partisan in its activities, dedicated to fostering effective communication between the industry, government, and the public and also serves as the public voice of the real estate development industry, communicating with the media on a number of issues.

- *AOLE – Association of Ontario Land Economists*
- *CORENET Global –* is the world's leading association for corporate real estate (CRE) and workplace professionals, service providers and economic developers.
- *Independent RE Brokers Association*
- *Mortgage Brokers* (each province has an association) they include:
    - Canadian Association of Accredited Mortgage Professionals
    - Mortgage Brokers Association of BC
    - Independent Mortgage Brokers Association of Ontario
    - Alberta Mortgage Brokers Association
- *CREW –* is a nation organization dedicated to providing knowledge, connections and support for women throughout their commercial real estate careers. It has local and regional chapters throughout the country.

8. Emerging business trends

- Foreign investment in the real estate sector is likely to remain strong and is supported by the depreciation of the Canadian dollar and relative market stability.
- Indicators of potential new models for property sales including "virtual real estate agents" and the use of auctions to complete sales to make the competitive bid process more open.
- Private residential sales
- Investment climate and stability
- Projected rise in mortgage rates in later 2014 will increase the costs of owning a home compared to household income. This will make housing less affordable.
- Immigration is towards major centres across the country resulting in in-fill and condominium projects which further result in significant transit issues.
- Macro geopolitical events such as the "Arab Spring" and increased anti-corruption efforts in China for example have led to significant inflow of people and funds, much of it into the real estate sector.
- The recent termination of the federal immigrant investment program is likely to impact the real estate market. The program remains active in Quebec.
- Trends in the growth of the Canadian Construction industry point towards strong non-residential markets and stable residential markets. By 2021, expanding activity is forecast to add 44,000 jobs in non-residential construction, while an estimated 8,000 jobs are estimated to be lost in residential.[20]
- Construction activity will rise significantly over the next few years in the industrial and office sectors, with developers hoping a stronger economy will see these properties leased quickly. The ongoing delivery of new supply in the nation's major downtown office nodes could lead to increased vacancy and downward pressure on rents, if demand fails to keep pace over the next few years.
- CMHC expects total housing starts to remain stable over the next couple of years. With a relatively high number of units under construction in some local markets, builders are expected to adjust the pace of activity in order to manage their inventory levels.[21]
- Existing home sales are expected to rise moderately along with economic conditions in 2014-2015.
- Resale prices are expected to remain in or near balanced market conditions with the average MLS price expected to grow at a rate near inflation over the forecast horizon.

[20] Construction Sector Council – Construction Looking Forward: 2013-2021 Key Highlights - http://www.buildforce.ca/
[21] Canada Mortgage and Housing Corporation - http://www.cmhc.ca

9. Products and services offered

The essential services in the sector cannot really be changed or replaced as they involve the development of land, the creation of buildings and their sale. Models of building and real estate ownership have seen little change; timeshares and REITS being two more recent exceptions.

In the sales segment, there is some discussion within the real estate sector regarding the replacement of real estate agents by "virtual agents" but there is no clear picture of how this would actually work. Similarly we have seen examples of sales by open auction rather than by the standard closed offer process but this is again merely a variant on the method of transaction and does not impact the underlying details.

Delivery channel(s) in the real estate sector are limited because of the service based and geographical nature of the offerings. Segments from residential and commercial brokerage to development and construction are delivered directly to clients in an essentially face to face mode. Some aspects of the sales side of the industry have been supplemented by use of Internet based tools, but at the present time these are not seen as being capable of providing much more than electronic brochures. An exception to this is the use of lawyers as an access channel to purchase Canadian real estate assets.

"Do it yourself" services for home sellers have appeared but the essential elements of the transaction including the use of lawyers and other professional to effect changes to title etc. remain in place and so such transactions do not disappear from view. Such services still involve the use of brokers who work on a flat fee basis and essentially remove the percentage based commissions of standard broker managed sales.

There are two primary links to other products and services in the real estate sector:

- *Financial entities,* especially mortgages and loans secured by title.
- *Legal services –* lawyers remain a key element of all real estate transactions in all market segments. Our research has indicated that this can in some cases add to the risk (abuse of trust accounts, lawyers acting as agents and nominees to hide the identity of true beneficial owners). In BC notaries are also involved in real estate transactions and mortgages.

10. Type of customer(s)

10.1 Business versus individual

In the residential market, buyers are by definition, almost exclusively individuals buying a home in which they will then live. The same generally applies to single dwelling recreational properties.

In the commercial property market, the nature of the customer is significantly tied to the size and scope of the property in question. Although small lower end strip malls and condominium or apartment buildings may belong to individuals, it is more common to see them purchased or developed by corporations of one type or another.

It is generally true that the larger and more valuable the property and the closer it is to an urban center, the less likely it is to be owned by an individual. Generally, multi-unit residential and commercial properties are owned and managed by specialist companies, the largest of which are publicly traded. The high end commercial and retail properties are the exclusive domain of large developers and property/asset managers as well as institutional investors. At this level, both the nature of the players as well as the scale of the financial aspects makes ML problems far less likely to occur.

10.2 Canadian residents/non-residents

There is no doubt that the majority of Canadian properties are owned locally by Canadian nationals or residents and Canadian companies. Despite this, the Canadian real estate sector has long been a magnet for overseas investment and immigration. Interestingly, Canadians and Canadian companies have also become the largest buyers of overseas property in the world. Our research indicates that all aspects of the Canadian sector have exposure to foreign buyers, with a particular focus on high end residential properties and lower end to mid-level commercial, revenue generating properties. Our research has also identified a short list of countries from where a high proportion of the foreign buyers come and it is clear that much of this investment money is closely tied to the politics and security situation in these countries. They are; China, Russia, Middle Eastern Countries (especially Egypt, Iran, Syria), Mexico, USA, the United Kingdom and Australia.[22]

10.3 Geographic area

As outlined in the following section, real estate buyers in Canada are very significantly bound by the location of the property. This means that a significant majority of buyers will already be in the market where they are buying and will be dealing with a local market participant. At the high end of the commercial, and to some degree the residential markets, there are buyers who deal with national and international participants. This would include offshore buyers. Our research indicates that offshore buyers of residential properties still quite often deal with participants in the local market who have the language and social tools to attract them in their home locations.

[22] Sotheby's International Realty Canada – Top Tier Trends Report: A Comparative Survey of Canada's Luxury Real Estate Market

11. Geographic considerations

Whilst the regulations and associations for the real estate sector are primarily provincial, the real estate industry is heavily geographically subdivided into natural market areas at the retail level as typified by the real estate boards of which there are approximately 100 across the country. These subdivisions are significantly, but not entirely based upon urban centres and their surrounding catchment areas.

In the large commercial and development segment of the sector, companies tend to be regional or national in their coverage and in some cases, the market players are global entities (for example engineering and other similar segments). Developers in the residential and low end commercial property space tend to be local to their market and in some cases regional.

Canada is attracting a lot of overseas buyers in a number of market segments. According to the Association of Foreign Investors in Real Estate's 2013 Foreign Investment Survey, Canada ranks second to the USA as a stable and secure country for investing in commercial real estate. Canada was ranked 6th, and is regarded as highly transparent, on Jones Lang LaSalle's Real Estate Transparency Index, which aims to help players in the real estate industry understand important differences when transacting, owning and operating real estate in foreign markets.

12. Any other relevant information on the sector

Our research indicates that the high end residential market in specific areas of Canada is a prime focus of non-residents, both from an investment and a living perspective. Markets such as Vancouver (40%), Montreal (49%) and Toronto (25%) have a significant proportion of home sales in this category to foreign investors/buyers.

Real estate has a number of inherent characteristics which make it both an attractive and effective tool for those wishing to launder funds, these characteristics include:

- A real estate investment can also be used as a residence, to project prestige and power or an effective base from which continuing criminal or terrorist operations can be conducted.
- As a means of laundering money, the cost of laundering is low or zero, a significant advantage over other forms or laundering.
- A real estate investment may increase in value over time.
- The standards of AML due diligence and compliance are low and are not an effective barrier, even for notorious criminals.
- The use of nominees, including professional nominees such as lawyers and accountants, or holding companies is not uncommon in real estate transactions making concealment of beneficial ownership easy.
- Both residential and commercial properties can produce income and or allow the comingling of illicit funds.
- Mortgages are very common and using front companies or individuals to create fake mortgages is straightforward and effective.
- The true value of a property can fluctuate significantly easily allowing over and under-pricing to enable money laundering.
- The use of cash payments, especially in the construction, renovation and upgrading of real estate assets is very common allowing illicit cash into the system.

13. Key points from interviews

13.1 Sector Background

1. The sector focus generally is on the quality of the property for sale, not the quality of the buyer and their funds.

2. Any real estate transactions that involve cash: means that the buyer is getting a deal and the funds will not be reported for tax purposes. This is happening in new construction, e.g. buy a home/condo but it is not quite finished, so the unit is purchased at a discounted price and the finishing and/or any upgrades are all done for cash and the cash is unreported. The transaction amount that is reported is what gets used to determine land transfer taxes etc. There are views that this is happening significantly, across most players.

3. Commercial transactions over $1M are usually tracked in RealNet. RealNet is an online database of historical real estate transactions over $1M. Transaction details are listed for various commercial sectors (office, industrial, retail, residential, hotels, ICI land, residential land, residential lots). RealNet used to be partially owned by CBRE. It is one of the very few commercial real estate transaction databases in existence in Canada.

4. Yes there are cash deals. Sometimes a builder of say 600 units will sell 20 out of the 600 for cash and this just gets buried and not reported. The cash received is often used to finance a personal second/cottage type property. One example provided of the buyer bringing in the cash funds from Manila. Usually there is no bank financing involved in these types of deals, and therefore no Altus type verification audits. Estimate provided that at this level of the market (smaller project construction, 30 condos or townhouse projects for example) that 25% of the activity could be like this (illicit, no questions asked etc.)

5. Banks are currently not dealing with the smaller developers. This segment of the market however is active. Where does the financing coming from? It was noted that there are many 'private bank/consortium' opportunities, this means that the projects are getting financed and done, usually 10-15% profitable, funds are then 'legitimized' through the profitable project completion, and the money is then subsequently getting banked.

6. For deals that require any kind of bank financing, the banks and lawyers are all over the details of the deal, checking and verifying the information. Includes groups like Altus doing verification audits on costs.

7. Many foreign buyers are not worried about making any return on investment or rental money in the market; they simply want a safe, stable place to invest or 'bank' the funds.

8. Many foreign buyers are using Canadian family or friends to be the local purchaser. Funds are actually from the foreign individual but seen to come from the local person when the deal actually closes. The sector at this level (smaller project builders) is not asking what the source of the money is.

9. There have been instances where third parties are involved – this is especially seen in cases where foreign parents are purchasing houses for children – however, agents should be performing background checks to understand source of funds. Realtors would also rely on foreign lawyers to get a better understanding of client.

10. Realtors need to be licensed but background checks are not necessarily performed. Accordingly, there is a large spectrum of realtors in marketplace.

11. With franchised realty companies, the business owner/broker is responsible for their own local operations and is concerned about reputation damage and therefore requires understanding of clients – conducting background checks. However, there is uncertainty as to whether this occurs broadly in marketplace.

12. The broker community is essentially unregulated. It is the broker who sees the buyer first hand, who has direct and significant access to the deal. It needs oversight.

13. While lawyers are part of most purchase and sale agreements, lawyers can be unfamiliar with source of funds – there have been instances where nominee buyers are involved to knowingly/unknowingly assist with money laundering; buyers purchase property with source of funds from a third party deposited into the lawyer's trust account. The mortgage is paid off quickly and/or the property is sold for a profit and the money launderer now has legitimate source of funds.

13.2 AML Compliance

14. Larger commercial real estate firms are aware of the AML regulations and reportedly have strict regimes in place including customer identification, training and reporting of suspicious transactions. Some have procedures including that agents cannot receive their commission until all of the correct AML documentation and procedures have been completed. This information is consistent with the information received regarding larger developers.

15. Larger firms tend to be risk averse and in any case where they are uncomfortable or the client refuses to provide the required AML information, they send an STR to FINTRAC.

16. Larger commercial real estate firms deal with companies a lot, we do not know the percentage but probably above 80%. Companies have to be properly identified including proof that the individual can bind the corporation. Firms do corporate searches themselves to verify details. When companies are overseas, the real estate firm works with a local affiliate in the overseas location or with a law firm to obtain the necessary documentation and proof.

13.3 Trends

17. The level of the Canadian dollar clearly has an impact on the volume of foreign money. Real estate firms generally do not track which countries buyers are coming from.

18. There is a significant volume of flight of capital purchasing- individuals moving money out of at risk countries by investing in Canadian real estate.

13.4 Risk areas

19. One person interviewed cited the top risks for AML as foreign buyers and deals where the money comes into the trust account and the deal never closes so the money goes straight back out (and that this was an automatic flag for an STR).

20. Type of assets is also seen as a risk factor - investing in asset classes which are less conventional and generally shunned by institutional investors, for example, bowling alleys, strip clubs, etc.

21. Location of assets as a risk factor - transactions in areas which are outside of the downtown core/urban area, more remote; these assets are comparatively harder to sell.

22. Transactions financed by offshore banks are seen as riskier - this type of purchaser might not go to a traditional lender and is seen as a risk for illegal funds.

23. Any real estate transactions that involves cash. There are views that cash transactions are happening significantly, across most players.

24. Yes there are cash deals. Sometimes a builder of say 600 units will sell 20 out of the 600 for cash and this just gets buried and not reported. The cash received is often used to finance a personal second/cottage type property. One example provided of the buyer bringing in the cash funds from Manila. Usually there is no bank financing involved in these types of deals, and therefore no Altus type verification audits. Estimate provided that at this level of the market (smaller project construction, 30 condos or townhouse projects for example) that 25% of the activity could be like this (illicit, no questions asked etc.)

25. Many foreign buyers are using Canadian family or friends to be the local purchaser. Funds are actually from the foreign individual but seen to come from the local person when the deal actually closes. The sector at this level (smaller project builders) is not asking what the source of the money is.

26. Some sales to foreign purchasers are possibly settled offshore, meaning that the seller receives the funds in offshore accounts and the money to buy Canadian real estate never enters Canada.

27. Smaller project builders often have more money in the deal and less or no need of bank financing. These self-financed projects are where there is risk. Smaller project builders are often directly involved in the sale of units. Smaller assets (condos or blocks of condos, small commercial premises such as strip malls and small office buildings etc.) are often of interest to overseas buyers with significant but not very large sums of money to invest ($2-$5 million).

28. Banks are currently not dealing with the smaller developers. This segment of the market however is active. Where does the financing coming from? It was noted that there are many 'private bank/consortium' opportunities, this means that the projects are getting financed and done, usually 10-15% profitable, funds are then 'legitimized' through the profitable project completion, and the money is then subsequently getting banked.

29. There is significant competition at the individual agent level; agents include a wide range of people, with varying education/levels of sophistication and there is inherent risk here. At the

realty/brokerage/agency level there is still inherent risk, but the size of the operation means that attention is paid to reputational risk.

30. While lawyers are part of most purchase and sale agreements, lawyers can be unfamiliar with source of funds – there have been instances where nominee buyers are involved to knowingly/unknowingly assist with money laundering; buyers purchase property with source of funds from a third party deposited into the lawyer's trust account. The mortgage is paid off quickly and/or the property is sold for a profit and the money launderer now has legitimate source of funds.

31. Higher end real estate deals are seen as very low money laundering or terrorist financing risk because there are only a few players who are involved at these very higher dollar amounts.

32. The leasing market is seen as low risk but they were aware of one case where [redacted] to launder funds. They got caught when trying to pay for leasehold improvements with cash.

14. Risk factors

14.1 General market factors

14.1.1 Comparative level of stability of the Canadian market

The comparative level of stability of the Canadian real estate market versus other parts of the globe is a risk factor which impacts the level of foreign funds which find their way into Canadian market. Theory is that the Canadian real estate market is safe and stable, easily accessed, and this would include for funds which may be from illicit activities.

14.1.2 Market competitiveness at agent level/minimal level of regulation and/or oversight

The competitiveness of the market and sheer number of agents puts pressure on individual agents to secure deals. Agents operating in the sector who are smaller, more independent have less infrastructure to ensure appropriate KYC and support to do any deal due diligence.

The smaller agent has more incentive to ignore due diligence/AML requirements, inherent risk.

Agents include a wide range of people with varying education and levels of sophistication. There is relative ease of access to agent licensing; new immigrants who obtain licensing can become conduits for foreign networks.

While brokers and realtors need to be licensed, research indicates that background checks are not necessarily being performed and that oversight is minimal to none in many cases. Competition and inherent risk to transact is high.

With franchised realty companies, the business owner/broker is responsible for their own local operations and is concerned about reputation damage and therefore requires understanding of clients – conducting background checks. However, there is uncertainty as to whether this occurs broadly in marketplace.

14.2 Product and service factors

14.2.1 Sale of higher end residential properties

($2.5 million and above: Dollar value depends on geography, generally speaking for the GTA for example, this might be properties in the range of $5M and higher)

Single family homes are the prime target; there are both historical (Beare report 72.3%)[23] and also current indications.

International organized crime groups and figures buying Canadian properties. Some examples of this include senior foreign organized crime figures such as:

[23] Beare, Margaret and Schneider, Stephen. Money Laundering in Canada; Chasing Dirty and Dangerous Dollars. University of Toronto Press, 2007.

- Rakesh Saxena – Indian banker who fled Thailand after a major fraud
- Lai Changxing – Chinese smuggler
- Lai Tong Sang – Dragon head of the Shui Fong Triad from Macao
- Stanley Ho – Asian gambling magnate with proven ties to organized crime
- Rustem Tursunbayev – Former Kazakhstani fugitive accused of embezzling $20m
- Alex Shnaider – Billionaire businessman with extensive former Soviet Union ties
- LEE Chau-ping – The "Ice Queen" head of the world's largest crystal meth trafficking syndicate from Hong Kong.

Articles on these cases are at Appendix B.

Indications that cash deals within the real estate sector are financing higher end second residential/cottage properties. See Appendix B.

14.2.2 Sale of lower dollar value commercial properties

(Dollar value depends on geography; examples provided included 30 unit condominium/townhouse projects and small commercial buildings)

Investments in asset classes which are less conventional and generally shunned by institutional investors. For example, bowling alleys, strip clubs, etc. are seen by industry insiders as less risky for illegal funds.

Lower rent level commercial properties which generate revenue are also popular (Salim Damji fraud case in Canada included both a high end condo and a strip mall in Toronto). We have identified numerous cases of fraudsters and corrupt officials from China using their illicit proceeds to buy homes and other real estate in Canada. News media items detailing some of these cases are at Appendix B.

Smaller project builders may have more money in the deal and less or no need of bank financing. These self-financed projects are where there is risk as the ability to transact in cash funds is easier. Smaller project builders are often directly involved in the sale of units.

14.2.3 Type and location of real estate asset

Transactions in areas which are outside of a downtown or urban core, more remote, are seen as harder to sell compared to conventional assets. To the extent these properties are selling for higher values and/or there is a higher turnover of ownership these are red flags.

14.2.4 Characteristics of real estate investment and transactions

Real estate has a number of inherent characteristics which make it both an attractive and effective tool for those wishing to launder funds, these characteristics include:

- A real estate investment can also be used as a residence, to project prestige and power or an effective base from which continuing criminal or terrorist operations can be conducted

- As a means of laundering money, the cost of laundering is low or zero, a significant advantage over other forms or laundering

- A real estate investment may even increase in value over time

- The standards of AML due diligence and compliance are low and are not an effective barrier, even for notorious criminals
- The use of nominees including professional nominees such as lawyers and accountants or holding companies is not uncommon in real estate transactions making concealment of beneficial ownership easy
- Both residential and commercial properties can produce income and or allow the comingling of illicit funds
- Mortgages are very common indeed and using front companies or individuals to create fake mortgages is straightforward and effective
- The true value of a property can fluctuate significantly easily allowing over and under-pricing to enable money laundering
- The use of cash payments, especially in the construction, renovation and upgrading or real estate assets is very common allowing illicit cash into the system

14.3 Delivery channel factors

14.3.1 Property purchased through a local (Canadian) agent

Foreign buyers are using Canadian agents to purchase property. Indications that some of these deals are done legitimately and other indications that some of these deals are done with no questions asked as to source of funds. Agents can include law firms, immigration lawyers/networks, and individuals. The Montreal condo article at Appendix B highlights this issue.

14.4 Geography Factors

14.4.1 Use of foreign money to purchase real estate asset

Including purchases by PEFPs and their networks, foreign purchaser money which takes a circuitous route into Canada, purchases which include funds loaned by foreign lenders, Canadian purchasers using offshore funds to purchase within Canada.

- Research has identified Canadian markets where up to 50% of all buyers of high end homes are foreign.
- Appendix B contains a series of news media and other articles which indicate real examples of this trend re offshore money.
- Section 116 of the Canadian tax law requires the reporting of taxes on the sale of property belonging to foreign residents but there is no tracking of purchases by foreign buyers.
- Flight of capital purchasing- there is a significant volume of individuals moving money out of at risk countries by investing in Canadian real estate.
- There are indications of the use of Canadian agents (family members, friends and other proxies) by overseas buyers to represent them either formally or informally, which obscures the real details of the foreign buyers

and the source of the funds. Research indicates that the sector at this level is not asking about the source of the funds.

- An article regarding Chinese condo buyers in Montreal, and data on high end Canadian residential sales from Sotheby's both underline this issue. See Appendix B.

- Research indicates that many foreign buyers are not worried about making returns on investment; they are looking for a safe, stable place to 'store' funds.

- Sales to foreign purchasers are possibly settled offshore, meaning that the seller receives the funds in offshore accounts and the money to buy Canadian real estate never enters Canada.

Similarly, we have seen a number of cases where politically exposed foreign persons including those involved in corruption and asset stripping have been found to have accessed the Canadian real estate market. They include:

- Zine el Adbidene Ben Ali – former President of Tunisia
- Belhassen Trabelsi – a relative of Zine el Abdidene
- Saadi Gaddafi – Son of former Libyan dictator Muammar Gaddafi

14.4.2 Use of offshore financing

Transactions financed by offshore banks are seen as riskier - this type of purchaser might not go to a traditional lender and is seen as a risk for illegal funds.

14.4.3 Real estate investments in emerging markets

Hiding illegally obtained funds in real estate in emerging markets could be easier for money launderers due to minimal or limited AML/ATF legislation, less sophisticated banking and financial sectors, lack of training of competent authorities, and higher corruption in developing economies.

14.5 Business relationships/linkages with other sectors

14.5.1 Use of lawyers and their trust accounts

All or most real estate transactions involve a lawyer at some point in a variety of functions. Multiple Canadian cases show that drug traffickers and others have used law firms and their trust accounts to receive cash proceeds and bank them as well as to assist in the purchase of real estate and the creation of companies to own property and make false mortgage loans.

Research also indicates that some sophisticated offshore buyers also use lawyers to funnel funds into the Canadian real estate sector.

14.6 Transaction methods and types

14.6.1 Use of cash in real estate transactions

Examples include:

- Partial cash payments for assets like condominium or townhouse units/multiple unit purchases.
- Properties being sold in unfinished state so that buyer can use cash to pay the trades for the completion/finishing work.
- Real estate developer using cash received to build personal property assets.
- Smaller amounts of cash given to lawyers to deposit into trust account, once funds sufficiently accumulated, real estate transactions undertaken.
- Rental market: privately owned buildings, less to minimal regulation, cash payments from tenants provide explanation for source of cash funds when deposited to accounts. Who looks at the books/accounting? No one required to. Comingling possible and also possible there are no 'legitimate' tenants.

Use of cash for real estate purchase transactions represents circumvention of the financial services sector, comments and indicators received indicate that cash is highly accepted with the residential and smaller building market and that this is happening significantly across most players at the smaller end of the market.

14.6.2 Incomplete real estate deals

Purchase funds are received into legal firm trust and/or brokerage accounts; when the deal falls through/does not close, funds are returned.

One person interviewed cited the top risks for AML as foreign buyers and deals where the money comes into the trust account and the deal never closes so the money goes straight back out.

14.6.3 Use of corporate entities to purchase residential real estate

Use of corporate entities for residential property purchases provides opportunity to hide beneficial ownership; seen as a risk factor, of course there is volume of legitimate purchases which are done this way. Appendix B contains a number of examples of such cases.

14.6.4 Corporate vehicles: Shell companies and property management companies

Corporate vehicles are legal persons of all types including trusts that are particularly used in countries where the opacity of corporations can be exploited to obscure beneficial owners and the origin and destination of funds.

Shell companies are companies that have no operations and/or assets in the jurisdiction where they are registered. In addition they may be owned by a legal entity which makes it harder to identify the individuals that own or control the company.

Property management companies may be used to manage/rent properties that are built/purchased with illegally obtained funds. The rental income generated by these properties provides the appearance of a legal origin of funds, especially when landlord and tenant are located in different jurisdictions. When property management companies are controlled by criminal organizations they can be used to mingle cash with legitimate funds.

14.6.5 Private mortgages and private lending

Private mortgages are generally not sourced from traditional lenders; often the mortgage is with an individual or a smaller company. There is a risk that these are fake mortgages and that registration on title provides credibility. A registered mortgage makes the deal look like it was financed and provides source of funds for property purchase explanation. Could also be funds sourced from illegal activity and/or funds evading tax, and the lender of these funds privately to buyers of real estate is not concerned with KYC/AML regulations and the form of repayment (e.g. likely to accept repayments in cash).

Note that vendor take back mortgages are fairly well accepted in the private market and represent the payment over time by the buyer to the seller.

Several case examples of this issue are at Appendix B including a drug trafficker who arranged multiple fake mortgages using a lawyer who set up front companies to make the "loans".

Private lending is active in the smaller developer segment of the market. Interviews reported that banks are not financing these projects and so 'private banks/consortiums' opportunities are sought and there is no oversight on

the source of the funds. Any illegal funds are then 'legitimized' through profitable project completion and the money is then subsequently getting banked.

Grant Thornton

Reporting Entity Sector Profile: Dealers in precious metals and stones

Money Laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

Canada's Dealers in Precious Metals and Stones ("DPMS") sector has a broad range of players primarily focused on their own segment although some work in more than one, for example jewellery manufacturers and retailers and retail jewellery stores.

The sector includes both regulated and unregulated segments with the activities of mining companies, smelters, refiners, cutters and polishers being unregulated under the PCMLTFA in Canada. Manufacturers are also not generally captured by the reporting requirements but may be if they are involved in transactions beyond the manufacturing of jewellery. The regulated industry segments include: dealers and traders including the Royal Canadian Mint ("RCM") and jewellery retailers. Pawnshops are not specifically regulated under the PCMLTFA but many are involved in significant retail jewellery transactions.

A number of factors specific to this sector make quantification of the sector reporting entity population difficult. These include industry players operating in more than one segment or role. It should also be noted that the nature of statistical reporting for certain segments in the industry includes a broad range of players, some of which are not part of this specifically defined sector, an example of this is the metal dealers which cover a wide range of materials, many of which do not fit in the "precious metals" category.

Another significant factor is that the sector is highly fragmented; a 2009 RCMP intelligence report stated that there are approximately 6,500 dealers of precious metals and stones within Canada[1]. A review of Industry Canada and other statistical sources provides a range of entities from 2,700 to 4,500 for the DMPS sector. In addition, the diamond wholesale business has historically been dominated by certain ethnic groups and in some cases certain families. Entry into parts of the market has therefore been difficult and the industry is still opaque in some respects.

Some evidence of the use of diamonds and precious metals for money laundering has been identified in Canada. A significant number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Product characteristics including being easily transportable, highly liquid, highly concentrated, bearer forms of wealth combined with the global nature of the trade and available markets. Use of precious metals and stones as currency by organized crime groups and individuals.
- High level of cash transactions.
- Uncertified stones and metals, primarily gold and diamonds entering the legitimate production and sales pipeline, including blood diamonds or conflict minerals.
- Ease of smuggling and difficulty in cross border monitoring of precious stones and metals. E.g. smuggling of precious metals and stones across borders.

[1] Financial Post – "RCMP issues warning on Diamonds", August 10, 2011

- Manipulation of the prices of specific shipments of stones; sometimes combined for example with transnational smuggling to effect trade based money laundering.

- Supplier/counterparty risk- as all activity is trade-related, both the supply of the product and the sale of the product must be considered when assessing risk.

2. Structure, size and segmentation and reporting entity population

We have focused in this report on the segments which are regulated in the Canadian DPMS sector. Broadly speaking, this includes dealers in both the precious metals and the stones markets at both the wholesale and the retail level. It also includes jewellery and precious metal retailers.

The segments that we have identified as significant are as follows:

- Precious metals dealers; bullion and/or coins; dealing with refiners and other dealers and/or with the general public;
- Precious coins dealers; smaller local coin stores, online dealers, usually offering products ranging from collectible to investment-grade coins to retail customers;
- Precious stones dealers trading both diamonds and other stones with other dealers, jewellery manufacturers and retail customers;
- Jewellery wholesalers; dealing in metals, stones and finished jewellery at the wholesale level. Some also manufacture jewellery and deal directly with retail customers;
- Jewellery designers and manufacturers; dealing with dealers and/or retail customers;
- Jewellery retailers (small to large) dealing with retail customers;
- Pawnshops dealing with retail customers and dealers; and
- Precious metals recycling dealers; dealing primarily with non-precious scrap metals e.g. copper, brass, aluminum, etc. for recycling but can include precious metals such as dental scrap; trading with dealers and the general public

The industry is highly fragmented with a wide range of participants from very small, one person independent operations, to large multinational companies. In some segments the participants are attached to or affiliated with other sectors such as bullion and coin dealers being attached to Canada's largest banks and also national retailers for jewellery, like Walmart.

It is also useful to consider the complete life cycle of these commodities in order to develop a better understanding of where the various segments fit in.

The DPMS cycle begins with the mining of precious metals and stones and ends with the retail sale of products and can be divided into the following steps:

1. The mining and extraction of the precious metal or stone from the ground. Once extracted, these commodities are sold to refineries for processing; often the mining company itself is involved to further refine the metal or stone.

2. The refinement of the metals or stones. Metals are refined and used for manufacturing processes or processed into refined bars and coins. Rough stones are sorted and then cut and polished.

3. *Wholesale metal sales* – dealers purchase the coins, or refined bars and these dealers in turn distribute their products to other dealers, jewellery manufacturers and/or for sale to the public. The RCM has a specific list of dealers which it sells to and also buys from.

4. *Jewellery manufacturing* – manufacturers of jewellery work with designers, often one and the same, and produce jewellery which will eventually be sold to the public.

5. Jewellery wholesalers deal in both stones and precious metals and are part of a maze of middle men in the process. Some of them also manufacture jewellery and deal directly with retail clients.

6. *Retail sales* – finished jewellery products and precious metals are acquired by jewellery stores and dealers to sell to consumers. Retail points of sale include – jewellery stores, coin stores, online jewellers and precious metals dealers, and coin and jewellery conventions.

7. Diamonds and other precious stones are traded through a more complex process known as the "diamond pipeline" as shown below. The process is unusual, primarily because of its history, which derives from a time when DeBeers, the world oldest and largest diamond producer controlled the global market. This continued until the 1980s, more recently, alternative diamond sources have developed in Russia, Canada and Australia and a number of other global mining companies such as Rio Tinto, Alrose, BHP Billiton and Harry Winston have also eroded DeBeers' market control.

8. The original DeBeers monopoly was secured by their unique business model, in which rough diamonds from all of its mines located throughout the globe, are brought to England for production sorting and aggregation. The diamonds are then aggregated and split into appropriate types and quantities to be sold to clients. The clients are called sightholders, of which there are 78 in the world including one in Canada.

9. When DeBeers controlled the global trade, only sightholders had access to raw diamonds and they had to be purchased according to the strict DeBeers rules. Several other trading oddities still remain in the industry including the practice of "handshake deals" between individuals who have known each other for decades and sometimes generations and loans of diamonds using the "memo transaction or consignment" system. This together with the use of cash to settle diamond deals makes the true state of affairs rather opaque and the tracking of deals particularly difficult. These elements of trust and specialist expertise built up in close knit cliques make market entry very difficult and also significantly increase the risks that this sector is abused by money launderers and terrorist financing.

10. This complexity was further exaggerated because the diamond trade was controlled by a small tight knit group who operated out of Belgium and Israel where most of the global diamond cutting and polishing took place. As new diamond producers have entered the market, these patterns have

changed too and DeBeers now only control approximately 40% of the global diamond market[2]. Similarly, diamond cutting and polishing has now significantly migrated to India and China and so global diamond trading patterns have changed significantly.

11. The market has also been significantly impacted by the Kimberly Process, a global initiative of governments, industry and civil society, developed to stem the flow of conflict diamonds and help to end wars funded by their illicit trade.[3]

There is significant overlap within these steps as companies and individuals often have operations across a number of the steps, for example, wholesale and retail jewellers might also design and manufacture the jewellery that they sell to their customers. Also, some mining companies extract and refine the metals while others might just extract and then sell and send them to be refined elsewhere.

The diagrams below outline the process and different stages underlying the diamond jewellery supply chain. It is important to note the multiple levels of diamond trading as these segments create significant risks.

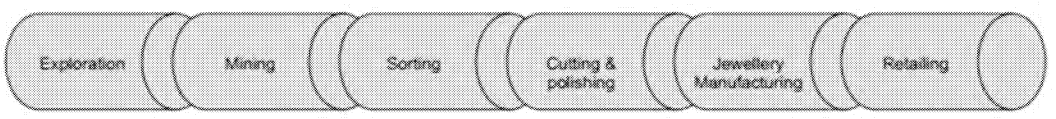
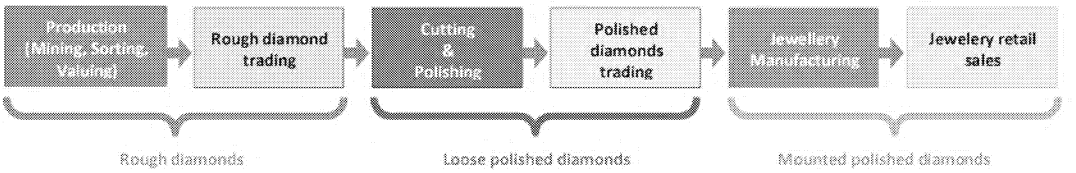


Figure 1: **Diamond pipeline diagram**



Note: This only represents this licit diamond trade.

Source: FATF – Money Laundering and Terrorist Financing through Trade in Diamonds, October 2013

The sector is captured across a range of SIC and NAICS codes, many of which include other sectors and segments not relevant to this report. We have therefore broken out specific numbers where possible or have otherwise identified other sectors that are included in the statistics. See Appendix A.

2.1 Precious metals dealing

This segment is primarily the activity of established and reputable metals dealers selling "recognized bars", which are sourced from certified refiners. A recognized bullion bar is one that was minted by a major refinery that is very well known and may have international locations or presence, such as the Royal Canadian Mint, Johnson-Matthey, Engelhard and Credit Suisse/PAMP. The purity of the bullion of unrecognized bullion products may be the same but they will not be accepted by major financial institutions. Recognized bullion products ultimately fetch higher prices as a result of the confidence instilled as a result of their status.

[2] First Research Industry Profile – Jewellery Stores, February 2, 2014
[3] Kimberley Process - http://www.kimberleyprocess.com/

The London Bullion Market Association produces a list of accredited smelters and assayers whose gold and silver bars they would automatically accept in settlement against transactions conducted between each other and with other acceptable counterparts; these bars earn the distinction of London Good Delivery status.[4]

True bullion coins are minted with designs but are traded primarily for their gold content, such as the USA Gold Eagle and Buffalo, the Canadian Maple Leaf, the South African Krugerrand, and the Chinese Panda.

2.2 Precious stones dealing

As outlined above, this segment consists of dealers in two parts of the market, dealers in rough diamonds, i.e. before they have been cut and polished and dealers in polished diamonds. The diamond trade is dominated by a relatively small group of participants ranging from international corporations to small but well-connected companies and individuals, many of which have long histories in the industry including family businesses. The trade in rough diamonds is global, and the licit market primarily conducts its transactions through the 29 bourses around the world. Bourses are private organized markets with membership generally restricted to individuals; their purpose is to act as a commodity exchange where buyers and sellers can meet.

In Canada there is one bourse, The Diamond Bourse of Canada which is located in Toronto and has 14 founding members. Total membership exceeds 66 companies. The membership is primarily Canadian but includes companies from the US and India, some of the members are the Canadian offices of international companies.[5] Not all members are diamond traders, for example the Ontario Ministry of Northern Development & Mines is a member. In addition to providing a market, the bourse also offers other value added services such as gem lab services, deposit boxes and a customs bonded warehouse. The trade in Canadian sourced diamonds is governed by the Canadian Diamond Code of Conduct a voluntary standard that provides assurance of the authenticity of Canadian diamonds. The code establishes a record of origin for each diamond sold as "Canadian" from one of the four Canadian diamond mines.

2.3 Diamond production and trading

Canada was the fifth largest diamond producer in the world by volume in 2012 and the third by value, producing US$2.1 billion of diamonds and has been a significant producer for a number of years now. Despite this, Canada is not one of the primary global trade centres for rough diamonds of which there are five; Antwerp, London, New York, Tel Aviv, Dubai in the United Arab Emirates ("UAE") India and China are also growing quickly. These centres provide a link between diamond producers and the cutting and polishing centres.[6]

The Diamond Bourse of Canada was established in 2008, in Toronto, in response to the dramatic growth of diamond production in Canada over the past decade. It joined 28 other bourses around the world. The national bourse, located in Toronto's financial district, is entirely dedicated to the business of diamond trading, merchants now use the bourse to meet for the purpose of buying or selling rough and polished diamonds, and take advantage of other services and amenities such as the Kimberley Process certification.

In 2012, Canada issued 280 Kimberly Process Certificates ("KPCs") for exports to 11 locations with the European Community comprising 53% of the total. India, Israel and the USA accounted for a further 33%. Canada also

[4] The London Bullion Market Association - http://www.lbma.org.uk
[5] Diamond Bourse of Canada - http://diamondbourse.ca/
[6] FATF – Money Laundering and Terrorist Financing Through Trade in Diamonds, October 2013 - http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

received 269 foreign KPCs in 2012 from 10 locations, once again the European Community led with 46% and the US, with 35%.[7] The complete table for diamond production is at Appendix A.

The statistics for 2012 for Canada look like this:[8]

	Volume (carats)	Value (USD)
Production	10.45 Million	$2.01 billion
Import	0.76 Million	$0.16 billion
Export	11.12 Million	$2.16 billion

The United States is the top exporter of jewellery to Canada and the trade has increased significantly, but other countries such as China, India, Israel and Italy are also major exporters of jewellery and silverware to the Canadian market.

Canada does not feature on tables displaying the top rough diamond import, export and trade figures or those relating to diamond export, import, cutting and polishing. Canada is not a major diamond cutting and polishing centre, this work is now mainly concentrated in India and China although Belgium and some African countries are still significant players. Despite this, the development of the Canadian diamond mining industry has been followed by early efforts to stimulate activity in this segment. The agreements which led to Ontario's first diamond mine opening also included clauses allocating 10% of its production for cutting and polishing in Ontario, and centres were established in Vancouver and Sudbury which produce high end loose polished diamonds. See charts at Appendix A.

Canada now has only one remaining diamond cutting and polishing company still in operation, Crossworks Manufacturing which is headquartered in Vancouver and has production facilities in Yellowknife and Sudbury, close to two significant diamond mines. The Sudbury facility is one of the largest in North America with 32 employees.[9] Canadian mined and polished diamonds, especially those from Ontario's Victor, mine are of exceptionally high quality and sell at premium prices around the globe.

2.4 Jewellery

Canada does not have a major jewellery manufacturing segment, although it is a significant market for both fine and costume jewellery. Although the US is the largest global market for fine jewellery, Canadians have, for example, the highest diamond engagement ring acquisition rate in the world at 85 percent. In 2008, the total value of the jewellery industry in Canada was estimated to be $1.7 billion. This figure includes the non-PCMLTFA regulated segments such as jewellery manufacturing and gem polishing and cutting.

Statistics Canada data for 2012 identifies 890 establishments in Canada under NAICS code 33991 Jewellery and Silverware Manufacturing. A full breakdown of the NAICS code is at Appendix A.

The Canadian precious metals & minerals market experienced growth and expansion between 2009-2012 with forecasts maintaining growth in value terms between 2013 and 2017.

---

[7] Canada Report on the Implementation of the Kimberley Process Certification Scheme, 2012 - http://www.kimberleyprocess.com
[8] FATF – Money Laundering and Terrorist Financing Through Trade in Diamonds, October 2013 - http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf
[9] Northern Ontario Business – "Crossworks Manufacturing is the largest cutting and polishing manufacturer in North America", February 17, 2011

Table 2-1 - Market value
CA$ million 2008-2012
Canada precious metals and minerals (includes mining and refining)

Year	US$ million	% Growth
2008	6,557.5	
2009	5,921.3	(9.7%)
2010	7,809.0	31.9%
2011	11,554.6	48.0%
2012	10,724.6	(7.2%)

Table 2-2 - 2012 Market value
Breakdown by metal

Category	2012	%
Gold	5,664.4	52.8%
Industrial & gem-quality diamonds	3,889.0	36.4%
Silver	511.2	4.8%
Platinum	361.3	3.4%
Palladium	259.0	2.4%
Rhodium	29.7	0.3%
Total	10,724.6	100%

Source: MarketLine – Precious Metals & Minerals in Canada, October 2013

Gold is the largest segment of the Canadian precious metals & minerals market, accounting for 52.8% of the total market value in 2012. The industrial & gem quality diamonds segment accounts for 36.4% of the market.

Canada accounted for 21.5% of North America's precious metals & minerals market value in 2012[10].

[10] Ibid

Table 2-3 - Market geography segmentation
US$ million, 2012
Canada precious metals and minerals

Geography	2012	%
United States	$14,236.1	28.5%
Canada	10,724.7	21.5%
Mexico	8,930.7	17.9%
Rest of the Americas	15,999.2	32.1%
Total	49,890.7	100.0%

Source: MarketLine – Precious Metals & Minerals in Canada, October 2013

2.5 Reporting entity population

The following Statistics Canada data gives an idea of the reporting entity data for a number of relevant segments. In each case, the statistics include several key segments with no further breakdown.

- Jewellery, Watch, Precious Stone, and Precious Metal Merchant Wholesalers: 667 (Onesource)
- Jewellery & silver manufacturing: 890 organizations or individuals
- Mineral ore and precious metal wholesalers/distributors: 122
- Jewellery stores: 2,619
- Securities and commodities exchanges: 263
- Gold and silver miners: 210
- Nonferrous metal smelters & refiners: 39
- Pawnshops – NAICs is too imprecise to identify

The total organizations and individuals identified through the Statistics Canada data review is 4,810. The SIC codes for the seven relevant codes are detailed at Appendix A.

3. Economic and financial statistics

In 2011 the value of jewellery imports reached its highest level in five years, at $1.1 billion. This was partly a result of the increased cost of raw materials such as gold and silver. Retail sales of jewellery and watches in Canada in 2011 amounted to $630 million, $138 million of which was sold in December during the Christmas and New Year's holiday season.[11]

A 2011 Statistics Canada report stated that there were five importers of worked, unset industrial diamonds. The total value of these imports by these five companies totalled C$481,569. The similar figure for worked, unset non-industrial diamonds indicated 83 importers and a total value of imports for 2011 of C$404,845,700. Figures for precious stones (other than diamonds) - unworked indicated 28 importers and a total value of imported goods of C$781,366. Precious stones (other than diamonds) – worked, 62 importers and a total value of imports of C$8,785,498. Rubies, sapphires and emeralds – worked, 26 importers and a total value of imports of C$8,254,092. The report also contains figures for synthetic or reconstructed precious/semi-precious stones – worked with 22 importers and a total value of imports of C$2,676,812. The figures for gold in semi-manufactured form (non-monetary) show 4 importers and a total value of C$30,135,550 no figures for monetary gold are available.[12]

The value of jewellery and watches sold at retailers in Canada in 2012 totalled $3.34 billion. Retail sales of jewellery and watches sold at large Canadian retailers in December 2012 were $138.8 million, an increase of 18% from average monthly sales of $135.6million in 2012 and up 60% from November in the same year.[13]

[11] TFO Canada - http://www.tfocanada.ca/
[12] Statistics Canada – Canadian Importers Database
[13] Statistics Canada - http://www.statcan.gc.ca

4. Regulation of the DPMS sector

The primary legislation in the DPMS sector is the Export and Import of Rough Diamonds Act (EIRDA) which came into force on January 1, 2003. This Act provides for controls on the export and import of rough diamonds and for a certification mechanism for the trade in rough diamonds, namely the Kimberley Process Certification Scheme. The Act also has a series of regulations, the Export and Import of Rough Diamonds Regulations (SOR/2003-15).

There are also a number of other Federal and provincial laws which govern the sector:

- Metal Mining Effluent Regulations (SOR/2002-222) - http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-222/
- Precious Metals Marking Act (R.S.C., 1985, c. P-19) - http://laws-lois.justice.gc.ca/eng/acts/P%2D19/
- Base Metal Coins Regulations, 1996 (SOR/96-194) - http://laws-lois.justice.gc.ca/eng/regulations/SOR%2D96%2D194/page-1.html
- Royal Canadian Mint Act (R.S.C., 1985, c. R-9) - http://laws-lois.justice.gc.ca/eng/acts/R%2D9/page-1.html
- Ontario Pawnbrokers Act – RSO 1990, Chapter P.6 - http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90p06_e.htm

There are also a number of other voluntary compliance type guidelines such as:

- The Canadian Diamond Code of Conduct
- Canadian Guidelines for Gemstones - Canadian Guidelines with Respect to the Sale and Marketing of Coloured Gemstones & Pearls – Revised edition 2013
- Jewellery Appraisal Guidelines – Minimum Acceptable Standards – Revised Edition 2010

Other laws governing some aspects of the sector come from the municipal level such as those governing pawnbroker and precious metals trading licences. There are also a number of global agreements and treaties governing the trade in conflict minerals and diamonds etc. aimed at reducing the ability of rebel groups in war torn countries from funding their military activities through the trade in illicitly obtained supplies.

The trading of metals futures is governed under the rules of the Investment Industry Regulatory Organization of Canada ("IIROC") Regulatory Margin Requirements for Precious Metals. Dealer Member Rules 100.2, 100.20 and 400.4, and Form 1 are designed to allow gold and silver precious metals bullion to be margined like their respective certificates.

5. Constraints

None identified at this point other than the regulations as described above.

6. Description of sector associations

Our research has identified the following Canadian and International DPMS related associations:

- *World Gold Council* – "The World Gold Council is the market development organization for the gold industry. With our unique insight into the global gold market, we see unrealized potential for gold across society and intervene to create new possibilities. Working with world-class organizations across the supply chain, we stimulate demand, develop innovative uses of gold and take new products to market. As the global authority on gold, we offer comprehensive analysis of the industry, giving decision makers unparalleled information and insight into the drivers of gold demand." www.gold.org

- *World Federation of Diamond Bourses* – "The object of the World Federation of Diamond Bourses is to protect the interests of affiliated bourses and their individual members, and to further the amicable settlement or arbitration of differences and disputes between the individual members of the affiliated bourses and between the affiliated bourses. In furtherance of this object, it is the aim of the world federation to participate in the promotion of world trade and to encourage the establishment of bourses, with the view of eventual affiliation of all centres where diamonds are actively traded. Members of the bourses affiliated to the World Federation of Diamond Bourses pledge themselves to uphold the traditions, principles of mutual trust, consideration and friendship which prevail among the members of the bourses world-wide. They pledge themselves to abide by and hand down these principles and to ensure that they will forever serve as a basis in business relations between members of the affiliated bourses world-wide."

- *International Precious Metals Institute* – "… the largest and most well-known association focused on precious metals in the world. IPMI is an international association of producers, refiners, fabricators, scientists, users, financial institutions, merchants, private and public sector groups, and the general precious metals community formed to provide a forum for the exchange of information and technology. IPMI seeks and promotes the efficient and environmentally sound use, reuse, and recycling of precious metals from both primary and secondary sources." https://www.ipmi.org/about/index.cfm

- *Jewellers Ethics Association (US)* - JEA works towards promoting and supporting ethical business practices within the jewellery and gemstone industry by providing its members with information, education, conflict resolution and support to increase confidence in the products they buy and sell. - http://jewelersethicsassociation.com/

- *London Bullion Market association* - The LBMA is the international trade association that represents the market for gold and silver bullion, which is centred in London but has a global client base, including the majority of the central banks that hold gold, private sector investors, mining companies, producers, refiners and fabricators. http://www.lbma.org.uk

- *Gold Anti-Trust Action Committee* – was organized back in 1998 in order to expose, oppose, and litigate against collusion to control the price and supply of gold and related financial instruments http://www.gata.org/

- *Alliance for Responsible Mining – ARM* "…is an independent, global-scale, pioneering initiative established in 2004 to enhance equity and wellbeing in artisanal and small-scale mining (ASM) communities through improved

social, environmental and labour practices, good governance and the implementation of ecosystem restoration practices." http://www.communitymining.org/

- *Professional Numismatists Guild* - a non-profit organization composed of the world's top rare coin dealers, paper money and precious metals dealers and numismatic experts. PNG members must follow a strict Code of Ethics in the buying and selling of numismatic merchandise. http://www.pngdealers.org/

- *Numismatic Guaranty Corporation* - Coin collectors often join large coin collecting groups such as the NGC and trade coins at group meetings or at coin collecting conventions.

- *Jewelers Circular Keystone* - is the jewellery industry's leading trade publication and jewellery industry authority. http://www.jckonline.com/about

- In the mining sector, the largest and oldest group is the *Prospectors & Developers Association of Canada.* There is also a Mining Association of Canada and multiple similar bodies at the provincial level.

- *Canadian Jewellers Association* - The CJA is the voice of the Canadian jewellery industry, providing leadership in ethics, education and communication. This association has some provincial level groups as well.

- *Jewellers Vigilance Canada* - An Independent, non-profit association to advance ethical practices, establish a level playing field for the Canadian jewellery and watch industry and provide crime prevention education for our industry. In full partnership with the RCMP and Jewellers Mutual Insurance Company.

- *Canadian Diamond Code of Conduct* - The Code establishes a minimum standard based on records and a chain of warranties required to validate a Canadian diamond claim. Retailers who abide by the Code demonstrate to consumers their commitment to ensure the authenticity of Canadian diamond claims.

- *Canadian Gemmological Association* - is a non-profit, membership association and educational institute providing education in the field of gemmology and provides a forum for Canadian gemmologists to meet and share knowledge and experiences

- *American Gem Society* - American Gem Society is a jewellery association comprised of the top jewellers in the United States and Canada offering diamond education and other services to consumers. http://www.americangemsociety.org/

- *Gemological Institute Of America* - The Gemological Institute of America, GIA, is the world's foremost authority in gemmology, diamond grading, jewellery education, gemology research, diamond and gemstone grading reports and laboratory services. http://www.gia.edu/

- *National Jeweler* – the industry's only news analysis publication which covers all the topics of importance to the retail community and is the leader in conducting and disseminating trade and consumer research and identifying the trends that shape the industry. http://www.nationaljeweler.com/

7. Emerging business trends

Our research has identified a number of macro trends that are affecting this sector. In particular, as outlined above, the diamond industry is undergoing significant change with the emergence of new diamond producers and the migration of diamond cutting and polishing centres to China and India. The DeBeers' monopoly has been significantly degraded and its market share fell from as high as 90% in the 1980s to less than 50% in 2012.[14] The development of the Canadian diamond industry played a role in this change.

Similarly, the global movement to stamp out the trade in conflict diamonds and minerals, especially the Kimberly Process, has significantly altered the global market place for the sector. Although in theory, trade in these materials is decreasing, in reality, it has been driven underground and this factor alone has significantly increased the risk of money laundering in the sector globally. As a more current example, there are media reports involving dealers in Dubai who have apparently been involved in significant numbers of cash transactions which does not allow for any effective monitoring as to the origin of the metals (gold). Strict standards for requirements to determine the sourcing of the metal (similar to the Kimberly Process) are now starting to be applied/called for. Articles related to this are attached at Appendix B.

Formation of wealth management type companies focused on investments in precious metals and stones is another emerging trend. The trend is that these organizations are presented to the public more along the lines of securities firms. However, these organizations appear, given the sector they focus on, to be unregulated with respect to investor protection regulations. An example is the following: http:/ s.20(1)(c)

The retailing of diamonds and jewellery has also begun to see significant changes over the past few years with the internet and mass merchants such as Walmart beginning to gain market share. Although the numbers here are changing, there is little doubt that the high end of the market is still dominated by the traditional sector participants such as specialty jewellery stores. Research indicates that specialty jewellery stores now account for only about 40 percent of all jewelry sales in the US. It is reported that Wal-Mart's success in selling jewelry stems partly from consumer perception that it has the lowest prices.

- *Synthetic Diamonds* – In the past the processes which had been developed for the synthetic creation of diamonds could only produce very small gems that were suitable only for industrial processes such as drill bits and cutting blades. In the last 20 years, a number of different technologies for creating diamonds have been developed and gemstone quality synthetic diamonds are now a reality. Although chemically identical to geological diamonds, their physical properties are different and they can be distinguished using optical analysis techniques. Despite this, the traditional diamond industry has in the past few years reacted strongly to the discovery of synthetic diamonds in parcels of geological stones. The full impact of these developments is not

[14] Kitco – "A diamond market no longer controlled by DeBeers", June 6, 2013

yet apparent but the traditional industry is pushing for laws preventing the identification of synthetic diamonds as genuine, an act they see a fraud.

- *3D Printing* – Market research reports indicate that more jewellers and jewellery designers are turning to 3D printers to give customers a greater number of customization options and a quicker turnaround time; that the 3D technology may allow designers to bring more affordable versions of their products to customers and that the printers could increase consumer demand for custom-designed jewelry and allow jewelers to provide a level of customization previously not possible.[15][16]

- *Public Mistrust of Jewellers* – research of the sector also indicates that the public is wary of, and intimidated by, jewelers, a perception "not unfounded given the average 100 percent price markup in the industry and the difficulty consumers have assessing product quality." These factors may be behind the trend towards retail internet jewellery sales.

There are some indications of a consolidation in the Canadian retail jewellery market. One example of this is the recent merger of two of the biggest diamond sellers in the US, Signet Jewelers Ltd and Zale Corp. Zale Corp, is the owner of Canada's People's Jewellery and Mappins, the new combined entity is now therefore the leading jewellery retailer in Canada. The deal was described as: "The latest sign of industry consolidation as chains and mom-and-pop shops increasingly battle on-line upstarts for customers."[17]

[15] First Research Industry Profile – Jewellery Stores, February 2, 2014
[16] First Research Industry Profile – 2-10-2014
[17] Financial Post February 20, 2014

8. Products and services offered

The products and services offered in the DPMS sector have remained stable over time although some delivery methods have changed as outlined above. At the production end of the spectrum, the mining and refining of both precious metals and stones is largely unchanged but the participants in these aspects have seen considerable change. Canada is a major player in the global mining industry and has become a major diamond producer. The jewellery manufacturing segment in Canada is not large and is a net importer of finished jewellery.

At the wholesale level, Canada has participants who refine and trade in both precious metals and gems and are traders of both bullion and coins and finished diamonds. Bullion dealer services include assaying, storing and shipping.

At the retail level, polished stones, metal and jewellery are sold both through traditional bricks and mortar retail establishments and a growing internet market. Online, the public are able to purchase bullion products, gems and jewellery from a range of companies. For bullion, players like Sprott, Kitco and the Bullion Exchange are examples. For gems and jewellery, examples range from the largest, Blue Nile and industry leaders like Tiffany's to smaller players such as budgetdiamondsonline.com. There is also an informal portion of this market where individuals sell such items for cash. Other sector products include:

- *Bullion Investment Funds* – an alternative way to invest in physical gold, platinum and silver bullion, on a Canadian dollar-hedged basis. Investors hold an interest in physical gold, silver and platinum bullion by buying units of the Fund directly on the TSX. Like any other exchange-traded securities, fund units are traded through investment dealers. (Examples in Canada include Brompton Precious Metals Bullion Trust, Sprott Physical Gold Trust, and Royal Canadian Mint Exchange Traded Receipts.)

- *Precious Metals certificates* – can be bought and sold at the prevailing spot price for the metal. Certificates carry no storage charges and bar charges are only applicable if the certificate is exchanged for physical bullion.

- *Exchange Traded Funds* – allowing consumers to purchase shares in a fund which purchases and holds physical precious metals or future contracts.

- *Stock market investments*- Investors can invest directly in mining and exploration companies by purchasing stocks or bonds or investing in mutual funds that purchase tangible precious metals.

9. Type of customer(s)

To a significant extent, the products included in this sector are personal items. With the exception of bulk purchases of precious metals by businesses and governments for investment purposes and the jewellery industry itself, customers are individuals buying jewellery and precious metals or stones for investment.

Institutional precious metals and base metals dealers like ScotiaMocatta are international buyers and sellers of gold, silver, platinum and palladium. The company acts as a clearing house to move billions of dollars of gold to settle daily trades. The company is also a conduit for gold going into India, the largest market for physical gold in the world, and is also one of the largest purchasers of metal from South Africa, the world's number one gold producing country. ScotiaMocatta connects industrial users and the big investors and the producers of precious metals. The company also stores vast amounts of metals in their vaults which can be shipped around the world at a moment's notice.[18]

[18] ScotiaMocatta - http://www.scotiamocatta.com/

10. Geographic considerations

The geographical picture behind the DPMS sector is a complex one for a number of reasons. Although there is local supply of both precious metals and stones in Canada, most of the product sold here has been sourced or manufactured overseas. As outlined above, Canada does not have significant assets or participants in the diamond trading and polishing segments or in the supply of precious metals from this country.

The diamond trade itself is a very global one and although Canada has become a significant supplier, only approximately ten percent of this product is destined for the local market. As a new player in this market, Canada is still developing the systems and controls to ensure adherence to the global set of laws and agreements that keep the industry clean. The nature of both the products and the global trading system through which they are sold both represent significant risk factors for money laundering and terrorist financing.

11. Any other relevant information on the sector

11.1 Product characteristics

As pointed out in the 2013 FATF paper on the diamond industry, diamonds have a number of inherent properties which make them especially useful for money laundering and terrorist financing. Although the same applies to other gemstones, their relatively small market as compared to the vast scope of the diamond industry makes them a less important tool for the money launderer. Diamonds have the ability to earn, move and store value, they are a liquid and transferable asset with unique physical and commercial properties which carry value in small, easily transportable quantities allowing their easy movement and therefore their suitability for the concealment and storage of the proceeds of crime. Diamonds are:

- Very high value
- Low weight/mass and size
- High value to mass ratio unlike metals
- Highly durable
- Stable prices and can retain value of long periods
- Hard to detect and therefore easy to smuggle
- Untraceable
- Easy to buy and trade outside the formal system
- Mostly unmarked (Many Canadian diamonds are an exception to this)
- Diamonds range significantly in a number of ways and therefore cover a very wide range of prices allowing price manipulation
- Diamonds can also be a useful tool for fraud as substitution of different quality products or synthetic diamonds can be hard to detect.
- Diamonds can also be used as a currency in themselves and have characteristics similar to cash

A number of aspects of the diamond trade also provide similar benefits for money laundering and terrorist financing:

- The global nature of the trade.
- The varied nature of participants from large to small and from modern and sophisticated to traditional and informal trading.
- Significant parts of the diamond trade are undocumented, unaudited and untraceable.
- The combination of the factors outlined above make diamonds an ideal tool for trade based money laundering. "The Financial Action Task Force (FATF) has recognised misuse of the trade system as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other ML techniques have become

increasingly effective, such abuse of the trade system is expected to become increasingly attractive". This statement is very relevant to the trade in diamonds. One of the main methods through which trade based money laundering is conducted is by way of over or under valuation. The diamond industry is tremendously vulnerable to this primarily because of the high subjectivity in the valuation of diamonds, the ability of diamonds to change their form, the trade based and global nature of the diamond market, and the long production chain involving many actors.

11.2 Business challenges

- *Influence of De Beers* - World diamond supply and pricing are strongly affected by De Beers, the South African group, which controls 40 percent of the world's rough diamond supply. However, De Beers faces increased competition from Canada, Australia, Angola, and Russia, and has encountered legal obstacles in the US and the EU because of its business practices.

- *Crime Exposure* - The small and expensive nature of the merchandise makes jewelry a target for potential thieves. The Jewelers Security Alliance of the USA reported 1,478 crimes against the jewelry industry in 2011, with losses totaling $85 million. Crimes include thefts in stores and off premises, such as robberies of traveling salespeople.[19]

11.3 Industry opportunities

- *Private Credit Cards* - Jewelers offering private credit cards have targeted promotional materials to customers to enhance connection with the store; some have also been able to sell other types of merchandise to them. Zale Corporation markets insurance and credit insurance to its credit card customers, about 35 percent of whom buy some form of insurance product from the company.[20]

- *Internet Sales* - Luxury jewelry giant Tiffany and many other jewelers have set up websites to sell jewelry. Internet sales accounted for 5 percent of Zale's revenue in fiscal 2012,[21] and the company has added e-commerce capabilities to its various brands to boost online sales. Tiffany markets its products through catalogs as well as its website.

- *Branding* - To increase consumer confidence, retailers and manufacturers are trying to establish brand names. While branding has been successful for signature pieces from famous retailers like Tiffany, gemstone branding has so far had little impact. Branding has been most successful for watches.[22]

[19] First Research Industry Profile – Jewellery Stores, February 2, 2014
[20] Ibid
[21] Ibid
[22] Ibid

12. Key points from interviews

12.1 Sector Background

1. One viewpoint was that there was ease of entry to the market and that this was an opportunity for criminal funds, "…entry costs are no different than opening a restaurant for example".

2. Another view was that there was a cost of getting in and out, and that it is within the range of 30 to 50%. This was thought to be significant, "too large a drop", and that the legitimate mark-ups and profit margins are low. In the past few years, there has been a trend towards diminished margins; diamond prices have become more transparent due to the internet. For retailers however, there are lower barriers to entry due to use of consignment sales.

3. Huge range of players within the sector; there are many one man shops, an individual who has a connection to source of diamonds/gems for example, who then sells to their own personal network, minimal to no oversight on any of these transactions. Then there are the other players: jewellery manufacturers, dealers and retailers; metals dealers, refiners; bullion dealers, suppliers, refiners; diamonds; some pawn shops. In major cities there are thousands of 'dealers' from small to large.

4. Subdividing the sector, one way to look at it:

   a) Buying jewellery from the public
   b) Buying and selling physical bars
   c) Retail jewellery sales
   d) Precious stones

5. Is there a high proportion of cash transactions? Yes.

6. Bullion Supply: if you are sourcing in Canada, this Canadian source is normally from the US and likely has come through at least a couple of wholesalers. When are buying from the US you are buying closer to the source. Unless you are one of the distributors that the Royal Canadian Mint works with for bullion.

7. Established and reputable bullion/metals dealers are selling "recognized bars", this means that the source is from a certified refiner. What does it mean to be certified? There are several listings… one is the London Bullion Market Association and if a refiner is on their list this means it is recognized, follows certain guidelines, is subject to testing etc. It was noted that these guidelines were not about AML but that they were some form of industry regulation.

8. All reputable dealers sell "recognized bars" and they do not go underground.

9. The Royal Canadian Mint has a distributor list: it is short and no more are being added to the list. The Mint has two sides: Numismatics (collector coins) and the Bullion side (The Mint has a FAQ section on its website).

10. The Mint relies on their distributors to distribute to the smaller shops. These distributors though, also have a retail side so they are in essence also competing with the smaller shops. In Canada, there are no non-retail distributors; the market is not big enough. In the US for example, there are distributors who do not have a retail presence; usually these are private companies.

11. The Mint does not regulate their distributors; it is a partnership. For example, when they buy from the Mint they are not asked any questions about the source of the money they bring forward; their business has never received a question from the Mint about whether or not they have an AML compliance program in place and if their dealer activities are reviewed for example.

12. There are metal bars in the market which are made from smaller (not certified) refineries, these are not "recognized".

13. Dealers will buy in gold, silver (in whatever form) from the general public or whatever source they have, they will either melt themselves and/or send to a refiner to do (this could result in bars which are not "recognized"). Then, for example, Royal Canadian Mint will take this refined "unrecognized" metal and will then process it and put out to market as "recognized". It was noted by this dealer that they were not aware of any AML procedures applied to any of this.

14. The Mint does refine gold for others as a service, putting it into any form they request.

15. If a dealer ships 100 ounces to a refinery, the refiner comes back and says 98 ounces of it was pure gold. Do you want it back, pay the refiner fee or do you want to swap? Swap means I take equivalent value in whatever bullion product I want and they supply. Anyone can be a refiner, but there are groups that provide certifications, so some refiners are certified and others are not.

16. Gold and silver metals are always traded in US dollars and always settle in US dollars. So, even if buy from the Canadian Mint, you pay in US price in US dollars. Would some distributors accept other currencies? Maybe, doesn't know, this particular dealer would not.

17. Retailers who are exposed to the public are seen as having a higher risk of exposure to money laundering, they do not really know their client. Wholesalers, and KYC is done at this level, have a better understanding of who the clients are. Typically there is an established client relationship at the wholesale level and transactions are not with one time clients.

18. When purchasing diamonds, this stones dealer looks for an originating invoice from a Debeers sightholder. It is estimated that 80 to 85% of the market originates this way. The secondary market, diamond producing which is non-DeBeers, is where it is thought that illegal transactions may exist. The secondary market can be riskier; the Debeers sight holders have more to lose, more to protect.

19. The industry is based on trust and that customers act honestly.

20. Metals don't actually move that much anymore particularly in large quantities. There is a very strong chain of custody at the higher levels and they doubt that conflict metals are getting into the system in North America. More likely it is going to markets much nearer to the original source.

21. In relation to the Dubai case, this proves that the global auditing process is working and this supplier has now been exposed, there is not risk of the metal entering Canada from this source as it is too far

away and the cost of moving it here is too high. Also believes that if you shut one door another one opens and they will always find a way.

22. Experience at the top end of the industry where dealing with most reputable dealers, there are lots of prohibitions. The background checks done are extensive and very thorough. This has been strengthened in the last few years by new OECD rules.

12.2 AML Compliance

23. There are minimal KYC requirements. Are there procedures being done to 'know your client'? Some dealers perform procedures but that is almost entirely because this dealer has an MSB business as well and are therefore aware and have been trained, have implemented a program because "it is the right thing to do". Generally, there is not much if anything done in the sector in this regard.

24. Industry players are not really at all in any way attuned to the AML rules, the rules have been in place only since 2008. Rules are very loose, most don't care. Has been no education.

25. Where does the industry need to get to? Needs to start by applying the MSB rules to DPMS. Need to think about supply/source as well, not just customers.

26. Some larger organizations deter cash from coming in, they promote bank drafts, but this comes with AML awareness and deciding to not accept cash off the street.

27. The new legislation came in in 2008 and at first it was very difficult to get people to understand why it was important to practice KYC due diligence and the learning curve was steep. Took a lot of effort to get people to understand and get on board.

28. In Canada the AML thinking is now there and there are good compliance processes. People are asking the right questions except at the retail level where they are still a bit reticent. The effort now needs to be on training and getting it out there to help them understand why it is important. Sharing knowledge, learnings and intelligence can help with this process.

29. There are global groups that meet with others in the industry and related groups to discuss what is going on in the market and share knowledge. One such group is the responsible metals forums. Some of these information exchanges are helping to bring AML standards up to the level of the securities industry.

30. The regulators could do more to share information and intelligence with industry to help educate them.

12.3 Trends

31. Do players in this sector ever get into securities type transactions (hedging using metals trading) and do these transactions receive any securities regulation type oversight? Yes, this happens. Not aware of any securities oversight.

32. Companies selling precious metals and stones for investment purposes, wealth management services, such as [redacted] was communicated as a trend. **s.20(1)(c)**

33. In regards to whether or not this type of business is currently or should be regulated by securities regulators: If the client takes possession of the specific bars or stones than securities registration is probably not required as there is no security, it is simply the sale of the underlying asset. If the client receives an 'interest' in unspecified bars or diamonds, then registration is probably required because those interests would be securities. Generally speaking, securities regulators have not seen registration from these types of businesses.

12.4 Risk areas

34. Need to consider the sourcing side of the business as well as the sales side.

35. Cash transactions.

36. Retail sales as the client and the source of funds is basically unknown. Also, if the main business is buying jewellery/gold product from the public, this is seen as very high risk. How does the dealer do any checks on where the jewellery came from? Or the silver? Possibly are feeding cash to organized property theft groups and/or groups that move money this way.

37. The non-Debeers diamond market; more risk for illegal activity here.

38. There is a lot of shadiness in the sector. Hard for the smaller shops to stay in business and stay clean. If are larger and of size, can manage the costs of choosing clean business. Pawnshops are the shadiest out there.

39. Online businesses are seen as risk area; not sure about the source of the diamonds. Diamonds identified as investments, such as [redacted] which was communicated as a trend (above), are seen as a risk area as the source of the diamonds is not clear.

40. The North American market for bullion is very well controlled and believe that the risk of any conflict metals getting into the system is low to moderate.

41. It is the other end of the supply chain where there could be problems, 3 to 7 layers down from the mint as the refineries and the wholesalers are very reputable and are doing a lot of compliance work, due diligence and KYC work to ensure the quality of their sources.

42. The mom and pop stores are a bigger risk because the due diligence efforts and the training are just not there. Anyone dealing with the larger entities is forced to maintain high standards in order to do so.

43. Gold lends itself to money laundering because its form can be changed very easily making it hard to trace.

44. Is aware of cases where the criminals use metals to launder funds and in many cases, gold and gold jewellery are found in police raids but they have been bought as finished products rather than being evidence of money laundering in the production system or supply chain.

45. Everyone in the industry has to do their part including the low end retailers.

13. Risk factors

It is essential to understand for this sector, that because all activity is trade-related, both the supply of the product and the sale of the product must be considered when assessing risk.

13.1 General Market

13.1.1 Ease of entry to the market

There appears to be relative ease to enter parts of the sector, e.g. metals trading, the requirement simply being sufficient initial capital outlay. During some interviews, it seemed that the only measure preventing dealing with illegally sourced funds was reputational. For specific segments, e.g. jewellery, there appears to be lots of competition, low margins and AML compliance is not an issue or seen as a concerning risk area for companies.

For other segments, e.g. diamonds trading, research indicates that there are barriers to entry including that the market is significantly reliant on trust and established relationships.

13.1.2 No cross border controls/reporting

While there is currently a declaration required for the transport across border for currency or monetary instruments this is not required for precious metals or stones.

Smuggling of precious metals and stones across borders; on February 3, 2014 a woman arriving from Trinidad and Tobago was arrested at Toronto's Pearson airport for smuggling over 10,000 diamonds hidden inside her body.[23]

13.1.3 Fragmentation of the sector/minimal regulation

No formalized industry oversight or regulation. Traditionally the sector has regulated itself, e.g. DeBeer sightholders, bourses, reliance on trust and established relationships. The lack of formalized oversight and regulation makes the sector vulnerable to money laundering and terrorist financing. Research indicates that markets have formed outside of away from and broadening beyond the traditional markets as more players become established.

13.1.4 Trade Based Money Laundering (TBML)

Manipulation of the prices of specific shipments of stones; sometimes combined for example with transnational smuggling to effect trade based money laundering. This is one of the most common methods used by criminals to launder illegally gained funds. The specific characteristics of diamonds as a commodity and the significant proportion of transactions related to international trade make the diamonds trade vulnerable to the different laundering techniques of TBML in general and over/under valuation in particular. This should be viewed in light

[23] Globe and Mail – "Woman arrested at Toronto airport had 10,000 diamonds hidden in body" Tu Thanh Ha, February 21, 2014

of the significant world annual trade volume which includes rough diamonds, polished diamonds and diamond jewellery[3].

13.1.5 Level of awareness of law enforcement and AML / CFT authorities (including FIU awareness)

Research indicated that the awareness of potential ML/TF schemes through trade in diamonds is low in most countries and trade transactions. The opaque and closed nature of the diamond industry are also obstacles to investigations of ML/TF by law enforcement agencies, which in many cases are unaware of the benefit and the possibilities for money laundering which diamonds may allow.

13.2 Products and Services

13.2.1 General product characteristics

Precious metals, precious stones, and jewels are easily transportable, highly liquid, highly concentrated bearer forms of wealth. They serve as international mediums of exchange and can be converted into cash anywhere in the world. In addition, precious metals, especially gold, silver, and platinum, have a readily, actively traded market, and can be melted into various forms, thereby obliterating refinery marks and leaving them virtually untraceable.

Criminal use of diamonds and gold as a form of currency due to the product characteristics; provides anonymity to transactions.

Apart from the retail sector, trade in diamonds, jewels and precious metals is traditionally private, as a matter of commercial protection or security. Dealers have traditionally protected their counterparties, their materials, and their business practices from public knowledge, in the interest of protecting themselves from criminal activity, and from potential independent interaction by competitors with their customers and counterparties or suppliers. Trust based on personal contact is an essential element of conducting business, and such trust and personal contact can assist in lowering counterparty risk. Each industry has trade resources, such as trade associations and directories, with which to establish some background and credit information and these can be consulted. Checks should be made of any new counterparty that is unknown. A counterparty, who proposes a transaction, should have the knowledge, experience and capacity, financial and technical background, to engage in that transaction, if not than the risk for money laundering and/or terrorist financing is assessed as higher.

Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. However, we need to be aware that values are volatile depending on supply and demand. The relative values of some materials can vary dramatically between different countries, and over time.

The physical characteristics of the products are also a factor to consider. For example, products that are more easily transported (e.g. jewellery) and which are unlikely to draw the attention of law enforcement, are at greater risk of being used in cross border money laundering.

Stolen or fraudulent products- as with all valuable objects, precious metals are attractive to thieves, and dealers need to be aware of the risks of trading in stolen product.

13.2.2 Product characteristics – precious metals, primarily gold

While not easy to transport in large quantities due to weight, the gold and silver markets are attractive due to the market stability and the international standard of measure. There is a relatively ready market for gold in Canada and internationally. While some bullion has serial numbers, this is not used to monitor and track source.

Depending on the nature of the transaction, counterparties, and quantities, gold is seen as the higher risk metal. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself, e.g. by hawalas. Gold is available in a variety of forms, e.g. bars, coins, jewellery, or scrap, and trades internationally in all of these forms. We have seen a number of cases where funds stolen in frauds and other cases were used to purchase gold and exported, see articles at Appendix B.

Unrecognized bars are at higher risk for illegal funds. Interviewees reported that reputable dealers deal in "recognized bars". Although interviewees also identified instances where "recognized bars" purchased with fraudulent funds were liquidated into cash to hide the origin of the funds.

13.2.3 Product characteristics – diamonds

While traditionally there is the primary market for stones from DeBeers sightholders (and this is changing as more diamond producers establish themselves in the market), there is more risk in the non-DeBeers market as it is less regulated. This was confirmed by interviewees who stated that the non-Debeers diamond market was more at risk for illegal activity in part because there was no originating invoice available from a Debeers sightholder.

- *High value* – cases show that the trade in diamonds can reach tens of millions to billions of US dollars. This has bearing on the potential to launder large amounts of money through the diamond trade and also on the level of risks of the diamond trade. The value of diamonds is high and their source is hard to trace; source of stones can be easily masked through recutting.

- *Pricing* – there is no standard valuation of precious stones, including diamonds; while in principal pricing is based on several determinant factors, the value of precious stones can be highly judgmental among experts and also depending on the purpose of the value – i.e. whether the precious stone is wholesale, market, appraised value. Accordingly, the declared value of precious stones is vulnerable to deliberate under or over valuing for trade-based money laundering on a larger scale. Mitigating factors to consider is the lack of local marketplace in Canada to liquidate diamonds and there is a large loss in margin (30% to 50%).

- *Terrorist Financing* - There are cases, even though relatively few, indicating that the diamonds trade has also been used for TF during the last 10 to 15 years.[24]

According to the RCMP's 2009 Project SHYNE report[25], Canada's diamond industry is at serious risk for money laundering by organized crime and terrorists. "The Canadian diamond industry remains largely unregulated," and leaves dealers vulnerable to money laundering and a law enforcement system ill-equipped to handle the problem. There are 6,500 dealers of precious metals and stones in Canada's highly fragmented market. The jewellery business is often a family affair and fuelled by personal contacts, and as a result it is so much harder for police to access. A major problem is the "value manipulation" of diamonds. Dealers can alter the jewellery's price by falsifying documents, or by not declaring the nature of diamonds at the point of sale. As well, retailers now often buy more diamonds from underground markets than from legitimate wholesale dealers, perhaps partly due to more jewellery store robberies across Canada, which has helped lead to "the growth of a parallel, illicit market among dealers."

[24] FATF – Money Laundering and Terrorist Financing Through Trade in Diamonds, October 2013 -
[25] Financial Post – "RCMP issues warning on Diamonds", August 10, 2011

13.2.4 Uncertified stones and metals

Primarily gold and diamonds entering the legitimate production and sales pipeline e.g. blood diamonds or conflict minerals.

13.3 Delivery Channels

13.3.1 Size of the dealer

Interviewees indicated that it was harder for the smaller shops to stay in business and stay clean. Larger operations are of size and can manage the costs of choosing 'clean' business.

13.3.2 On-line sales

The source of product for some of these groups was questioned by interviewees.

13.3.3 Pawnshops

Many of the transactions are understood to be mainly cash based. Some research indicates that up to 90% of the items pledged are gold. Interviewees indicated that they considered significant risk to be attached to many of the higher value transactions.

13.4 Geography

13.4.1 Global nature of trade

The supply and customer markets are transnational and complex, thus convenient for ML/TF transactions that are, in most cases, multijurisdictional in nature. This, in turn, creates difficulties for national law enforcement to conduct investigations and necessitates international cooperation between law enforcement agencies across countries in which the trade is taking place.

Research indicates that this industry, while there have been efforts to reduce such trade practices, is based on traditional ethics of trust and that this is an integral part of the trade culture and that record keeping is minimal.

More recent reports around major centres, e.g. Dubai, indicate that their ability to monitor and prevent the infiltration of conflict stones and metals into the legitimate market is weak/vulnerable and published examples show this. See Appendix A.

13.5 Business relationships/linkages with other sectors

13.5.1 Dealer customer risk

Retail customers are typically individuals purchasing gold and silver bullion as a safekeeping asset and for investment purposes. Transactions with individuals where purchases are shipped to addresses outside of Canada and/or to PO Boxes are seen as higher risk; also higher volumes and possibly structured transactions.

Purchases of bullion (or diamonds) back from retail clients and non-clients (rather than traditional supply sources); particularly where the origin of the product is unknown is seen as higher risk.

Research indicates that retailers dealing with the public really did not know their clients or the source of the funds and that accordingly, are seen as having a higher risk of exposure to money laundering. Wholesalers were understood to perform 'KYC' procedures and to have a better understanding of who they were dealing with. Typically at the wholesale level there is an established client relationship and transactions are not one-offs.

13.5.2 Dealer supply/counterparty risk

Level of transparency around gold (or diamonds) origination.

Supplier or counterparty that is not knowledgeable of the applicable local laws, regulations and rules, as well as the structure and extent of regulatory oversight is seen as high risk. The level of government regulation of counterparty's business and accounting practices is also relevant. Companies and their wholly owned subsidiaries that are publicly owned and traded on a regulated exchange, or that have publicly issued financial instruments, generally pose less money laundering risks. We note that this is not always true; some publicly traded companies may be established by money launderers.

The nature and extent of banking involvement. In general, a lower risk level is present where a transaction is entirely financially settled, both at the side of the dealer and the counterparty, through a banking institution that is situated in an FATF member country and that is known to be actively involved in payment flows and financing arrangements in the particular trade, provided the transaction is generally routine (including payment that closely follows routine trade flows) and that the documentation contains adequate identification of all parties concerned.

Higher risk counterparties/transactions include:

- Does not understand the industry in which they propose to deal, or does not have a place of business or equipment or the finances necessary and appropriate for such engagement, or does not seem to know the normal financial terms and conditions.
- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
- Has significant and unexplained geographic distance from the dealer in precious metals.
- Uses banks that are not specialized in or do not regularly provide services in such areas, and are not associated in any way with the location of the counterparty and the products.
- Makes frequent and unexplained changes in bank accounts, especially among banks in other countries.
- Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose.
- Will not identify beneficial owners or controlling interests, where this would be commercially expected.
- Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries.

13.5.3 Dealers providing wealth management services

Emerging trend was reported that there were some dealers in precious metals and stones who were positioning themselves to the public market more along the lines of wealth management and/or securities advising services. While this is perhaps less a risk factor for money laundering, it is an important public protection risk factor.

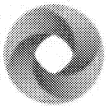
Securities firms are highly regulated with significant focus on investor protection and suitability requirements for the advisor and representatives. Dealers in the DPMS sector have no such regulation.

13.6 Transaction methods/types

13.6.1 Cash transactions

Interviewees reported that there continues to be a high level of cash transactions in this sector within Canada.

Recent media on case in Dubai for example, report on high volumes of cash transactions which effectively mean that the origin of the product (gold) is unknown.



Grant Thornton

Reporting Entity Sector Profile: Securities dealers

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

Canada's security sector is an integral part of the financial services industry and plays a key role in the capital markets. It serves investors, businesses and governments by providing expertise to raise debt and equity capital and allows investors to trade with confidence in open and fair capital markets. Brokers and investment dealers act as intermediaries by matching investors with the users of capital.

The securities sector is regulated at the provincial and territorial level and the securities regulators are assisted by self-regulating organizations ("SROs"). The regulators collectively monitor the markets to ensure fairness and transparency and they also enforce the rules that govern market activity.

Canada has no national securities regulator and this has frequently been identified as a weakness and a hindrance to the Canadian markets. Several provincial bodies are currently working on an agreement to operate together in simulation of a (semi) national entity and all of them cooperate through the Canadian Securities Administrators (CSA).

The products and services offered by the sector cover a very wide scope, and range from straightforward retail offerings to complex instruments and services for specialist traders and investors. The regulatory environment is therefore complex with both geographical and product/service based requirements and implications. Accordingly, securities firms are often regulated by multiple organizations.

The Canadian market is relatively small with a total of approximately 200+ firms operating in the primary segment of brokerage firms and investment dealers and over 2,000 reporting entities in other segments. The entire Canadian securities industry is eclipsed in size by several individual U.S. and Japanese securities firms. In spite of its comparatively small size, the industry has provided Canada with a capital market that is one of the most sophisticated and efficient in the world. These qualities are measured in terms of the variety and size of new issues brought to the market and the depth and liquidity of secondary market trading.

Securities firms vary in size and assets under management and generally comprise of the following three structures:

- Integrated firms that serve institutional and retail clients and offer a full spectrum of investment products and services. There are eight in Canada.
- Institutional firms are usually smaller, boutique-style operations that serve institutional clients such as pension funds, insurance companies, mutual fund organizations, banks and trust companies, endowments, charitable foundations, family trusts/estates and corporate treasuries.
- Retail firms serve retail investors and include both full-service firms and discount brokers.

The eight largest Canadian securities firms follow the integrated model and are mainly represented by the securities divisions of domestic tier one banks. They offer full investment services and discount brokerage services. Other firms in the securities industry range from boutique firms that specialize in a particular niche to firms that cater to high net worth clients providing a range of services. Differentiation within the industry is generally accomplished through three factors: investment approach and performance, quality of service, and pricing. (Seamark AIF)

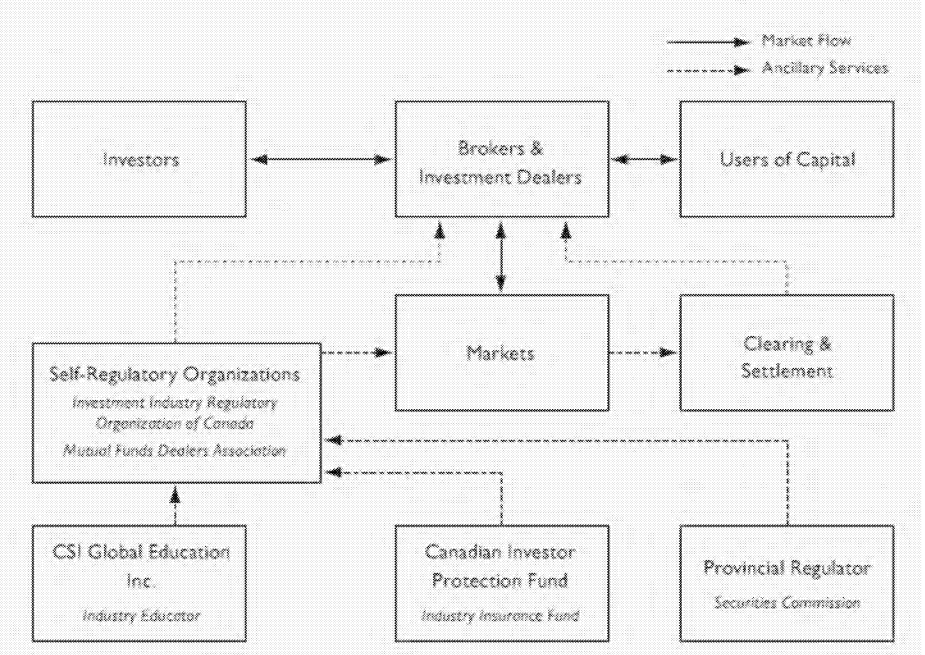
While the industry is highly regulated, the following key risk factors for money laundering have been identified:

- An environment that is highly focused on profitability and investor protection/suitability as opposed to money laundering and terrorist financing risks;
- Securities fraud as a vehicle to generate potential proceeds of crime. This would include market manipulation by clients, manipulation by securities professionals;
- The exempt market and off book transactions; and
- Fragmented industry that services high net worth clients and the involvement of international sources of funds.

2. Structure, size and segmentation, reporting entity population

Many securities firms operate in multiple jurisdictions and provide services that are regulated by more than one regulator. In total, the CSA identifies over 2,000 registrants that operate in the securities industry. The following diagram identifies the primary participants and their roles and interdependencies in the industry.

Figure 2-1 - Securities Industry Flowchart



Source: CSI Global Education Inc. (2013)

2.1 Brokerage firms and investment advisors/dealers

In 2013 there were just over 200 firms registered with IIROC that facilitate the buying and selling of financial securities for retail and institutional clients. The member firms range from full service firms to discount brokerages. Large full service brokers of banks and credit unions provide securities services through multiple divisions including private client services, institutional services, corporate finance and economic research. In 2013, the ten largest firms, eight of which belong to banks and credit unions, conducted 85% of the industry's sales in Canada.[1]

Client transactions are driven either by client-directed orders or by discretionary management – where investment decisions are made by portfolio managers. Compensation for brokerages includes a fee for transaction, as a percentage of the size of the portfolio or a fixed fee.

2.2 Mutual fund dealers

The members of the MFDA are organizations that distribute mutual funds and represent over $300 billion in mutual fund assets under management. The MFDA has 100+ member firms. Data from Investor Economics indicates that the value of assets under management in the mutual fund industry grew from less than $100 billion before 1993 to $920 billion in May 2013. It is estimated that the mutual fund industry directly contributed $5.8 billion to Canada's economy in 2012, up from an estimated $4.5 billion in 2005. Research by the Conference Board reveals that the total economic footprint of the mutual fund industry—including supply chain and induced impacts—was $17 billion in 2012. Directly and indirectly, the industry supports 192,600 jobs while creating $12.6 billion in primary household income and $2.3 billion in corporate profits.[2]

2.3 Exempt market dealers (EMD)

EMDs are securities dealers which trade in securities that are exempted from the rigorous requirements of the public capital markets by specific provincial exemption rules and some national instruments. EMD's are registered under provincial securities legislation in one or more jurisdictions in Canada and may act as a dealer or an underwriter for any securities which are prospectus exempt. They may also act as a dealer for any securities, including investment funds which are prospectus qualified (mutual funds) or prospectus exempt (pooled funds), provided they are sold to clients who qualify for the purchase of exempt securities.

The exempt securities market products are alternative investments that are not available through typical stock exchanges or mutual funds. Products may only be sold to a specific category of investors who are generally financially well off and knowledgeable about the products they invest in. There are approximately 880 registered EMDs in Canada belonging to the two primary associations.[3] The industry is still developing and varies province by province as the provincial exemption rules are not harmonized nationally.

---

1 Source: Retirement Quebec
2 Conference Board of Canada report
3 Canadian Securities Association/ Ontario Securities Commission; Exempt Market Dealers Association of Canada/National Exempt Market Association

2.4 Venture capital and private equity

Canada's 100+ Venture capital (VC) firms typically invest in early-stage or pre-revenue companies that do not have ready access to funding and receive investments through capital for equity deals. In 2012, $1.5 billion was invested by venture capitalists in Canada. As in other regions around the world, Canada's VC investment is mostly placed in its largest urban areas and in technology sectors with 49% invested in the IT sector, 25% in life sciences firms, and 10% in the energy and environmental technologies sector.[4]

Private equity (PE) firms typically invest in mature companies utilizing capital and debt. Through restructuring and reorganization, PE firms operate and manage the company to be more profitable. The PE fund management industry oversaw a capital pool that Thomson Reuters estimates to be $105.4 billion at the end of 2012. By far, the largest portion of this capital pool ($87.7 billion or 83 per cent of total assets) was managed by 172 Canadian firms active in buyout, mezzanine, and related PE segments of the market.[5]

2.5 Portfolio managers

These firms are registered with securities commissions as portfolio managers and are regulated by them. Most portfolio managers in these firms hold the Chartered Financial Analyst designation and abide by a strict code of ethics. Their only business is the discretionary management of investment portfolios for individuals, estates and trusts, charitable foundations, corporations, pension funds and endowment funds. Investment counsel fees are limited, in most cases, to a percentage of the assets under management. Investment counsel and portfolio managers also offer pooled funds to clients with smaller amounts to invest than the minimum for segregated accounts. These firms provide segregated accounts, usually with a minimum account size of $500,000 to the several million dollars range. They also provide pooled funds which require a minimum investment of $150,000 and disclosure is in the form of an information circular as opposed to a prospectus. Portfolio managers are also known as: Investment counsel or Investment Counsellors, Asset managers, Investment managers, and Wealth Managers.

2.6 Hedge funds

Hedge funds are commonly described as lightly regulated pools of investment capital that have greater flexibility in their investment strategies. They are a form of alternative investment that utilize advanced investment strategies in order to deliver higher returns and generally cater to sophisticated investors. Some hedge funds are conservative, others are more aggressive. Despite the popular name, some funds do not hedge their positions at all and they are best thought of as a type of fund structure rather than a particular investment strategy. Popular awareness of hedge funds in Canada is recent and has grown since 2001, despite several high-profile hedge fund failures, hedge fund assets continue to grow.

Hedge funds are less regulated, less controlled and less standardized than the majority of investments, but they also offer significant opportunities including flexibility compared to the more heavily regulated other types of fund. Other investment types are also not able to replicate the complex and sometimes expensive strategies that hedge funds use. Hedge finds differ in size but the primary differentiator is the strategy that they employ. Canadian hedge funds are estimated to have grown from approximately $12 billion in 2004 to over $30 billion in 2012.

Despite highly publicized failures in Canada and elsewhere, in recent years, significant progress has been made in the industry, especially in operations, governance, risk management, separation of duties and transparency. A

[4] CVCA/Industry Canada
[5] Conference Board of Canada

number of Canadian managers are ranked on a global basis as top quality managers – from both an infrastructure point of view and a return/risk point of view.[6]

2.7 Statistics

Statistics Canada provides some high level information on the major segments in this industry:

- Investment banking and Securities Dealing: 2,529
- Securities Brokerage: 1,619
- Securities and Commodities Exchanges: 263
- Portfolio Management: 18,830
- Investment Advice: 8,124

Statistics from industry and other relevant sources also provide some statistical information on the sector which has been included in the segment description sections of this report. Full details are at Appendix A.

[6] AIMA Handbook

3. Economic and financial statistics

In 2011, more than $320 billion in new financing was issued through Canadian securities markets, including more than $201 billion in new federal, provincial and municipal debt securities, $77 billion in corporate debt securities, and $42 billion in corporate equities. In 2011, more than $2,380 billion in equity securities and more than $9,340 billion in debt securities changed hands in Canada's secondary markets.[7]

In 2012, Canada's investment industry raised $32 billion in equity capital and helped the federal and provincial governments raise $161 billion to build infrastructure and provide services to Canadians. In the first nine months of 2013 operating profit in the securities industry grew 27% to $4.8 billion in 2012, with the eight integrated firms accounting for nearly all of the earnings gains, increasing on average 43% in the last five years.[8]

The past five years have been typified by increasingly divergent results between the integrated firms and the retail and boutique operations, while the large firm increased profits by 43% the retail side is struggling to survive with their profits declining by 39%. For the 58 domestic boutique firms, profits declined 67% over this period and with capital requirements rapidly increasing this is likely to continue.[9]

[7] Investment Industry Association of Canada website, September 2012
[8] http://iiac.ca/wp-content/uploads/IIAC-Letter-from-the-President-Volume-691.pdf
[9] Ibid

4. Regulation of the securities dealers sector

In Canada the regulation of the securities industry is a provincial responsibility, each province and territory is responsible for its own legislation and regulations. The bodies that carry out this mandate are all members of the CSA and are:

- Alberta Securities Commission
- Autorité des marchés financiers
- British Columbia Securities Commission
- Financial and Consumer Affairs Authority of Saskatchewan
- Financial and Consumer Services Commission (New Brunswick)
- Manitoba Securities Commission
- Northwest Territories Securities Office
- Nova Scotia Securities Commission
- Nunavut Securities Office
- Office of the Superintendent of Securities (Prince Edward Island)
- Office of the Superintendent of Securities (Yukon Territory)
- Office of the Superintendent of Securities Service Newfoundland and Labrador
- Ontario Securities Commission

Together, the provinces and territories work together through the Canadian Securities Administrators (CSA). The major provincial securities regulators also participate in various international co-operative organizations and arrangements.

The industry has also been allowed to govern its own activities to some degree and a number of SROs including the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association (MFDA) are important players in this role. SROs are private industry organizations that have been granted the privilege of regulating their own members by the provincial regulatory bodies. SROs are responsible for enforcement of their members' conformity with securities legislation and have the power to prescribe their own rules of conduct and financial requirements for their members.

SROs are delegated regulatory functions by the provincial regulatory bodies, and SRO by-laws and rules are designed to uphold the principles of securities legislation. The provincial securities commissions monitor the conduct of the SROs. They also review the rules of the SROs in the province to ensure that the SRO rules do not conflict with securities legislation and are in the public's interest. SRO regulations apply in addition to provincial regulations. If an SRO rule differs from a provincial rule, the most stringent rule of the two applies.

When the Investment Dealers Association and Market Regulation Services were combined to create IIROC in 2006, the professional association was separated from the SRO function and a new association was created, the Investment Industry Association of Canada (IIAC). The IIAC is a member-based professional association that

represents the interests of market participants. The IIAC provides support and services that contribute to the success of their members. It also represents the investment industry's views and interests to federal and provincial governments and their agencies, and to other SROs.

4.1 Investor protection funds

The securities industry offers the investing public protection against loss due to the financial failure of any firm in the self-regulatory system. To foster continuing confidence in the firm customer relationship, the industry created the Canadian Investor Protection Fund (CIPF) in 1969 and the Mutual Fund Dealer Association Investor Protection Corporation (MFDA IPC) in 2005.

4.1.1 Canadian Investor Protection Fund

The primary role of the CIPF is investor protection and its secondary role is overseeing the self-regulatory system. The secondary role provides a mechanism to help CIPF contain the risk associated with its primary role. The Fund protects eligible customers in the event of the insolvency of an IIROC dealer member. The CIPF is sponsored solely by IIROC and funded by quarterly assessments on dealer members.

4.1.2 Mutual Fund Dealers Association Investor Protection Corporation

The MFDA Investor Protection Corporation (MFDA IPC) provides protection for eligible customers of insolvent MFDA member firms. The IPC does not cover customers' losses that result from changing market values, unsuitable investments, or the default of an issuer of a mutual fund. The coverage provided is limited to $1,000,000 per customer account for losses related to securities, cash balances, segregated funds, and certain other property held in the account of an MFDA member firm. The MFDA is not recognized as a self-regulatory organization in the province of Québec; consequently, the MFDA IPC coverage is not currently available to customers with accounts held in Québec MFDA member firms.

4.1.3 Other Regulations

Other forms of regulation relating to global efforts to combat corruption and bribery such as the Corruption of Foreign Public Officials Act and the Extractive Industries Transparency Initiative are impacting the sector. These are particularly relevant when a securities form is involved to underwrite a new issue, particularly where there are foreign operations.

5. Educational and licensing requirements

5.1 Brokerages

- Members of stock exchanges and regulated by IIROC
- Securities Commissions
- CSA
- Independent brokerage firms have very little representation with IIROC

5.2 Portfolio Managers

- IIROC
- CSA

5.3 Mutual Fund Dealers

- MFDA – The Mutual Funds Dealers Association

5.4 Investment Dealers

- Members of stock exchanges and regulated by IIROC
- Securities Commissions
- CSA

5.5 Venture Capital Firms

- The 13 securities commissions governing Canadian provinces and territories
- The CSA, the Canadian Securities Association – the association of the 13 security commissions in Canada
- IIROC – Investment Industry Regulatory Organization of Canada

5.6 Exempt Market Dealers

- The regulatory framework for EMDs is set out in National Instrument 31-103 Registration Requirements, Exemptions and Ongoing Registrant Obligations which applies in every jurisdiction across Canada.
- The qualification criteria for exempt purchasers and exempt securities are found in National Instrument 45-106 Prospectus and Registration Exemptions.

Appendix 9

6. Constraints

Because of the increasingly global nature of global commerce, including the capital markets, the Canadian industry is becoming more closely impacted by international markets and their regulations and requirements. In many situations, this means that other regulatory and compliance issues may have an impact on transactions being conducted in Canada.

Specifically, the Foreign Account Tax Compliance Act (FATCA) (US) and the Foreign Corrupt Practice Act (FCPA) (US as well as other similar international laws, particularly regarding underwriting).

Appendix 9

7. Description of sector associations

Our research has identified the following Canadian securities dealer related associations.

7.1 Portfolio Managers

- *PAC – Portfolio Management Association of Canada* - is a forum for Investment Management Firms to share best practices and industry knowledge.
- *Exempt Market Dealers Association of Canada* - a not-for-profit association whose members firms are active in the exempt securities market. Recently this group has changed their name to PMAC, the Private Market Association of Canada.
- *National Exempt Market Association* – based in Calgary, the NEMA works with both regulators and stakeholders on developing a practical regulatory framework that fosters development of the exempt market by allowing entrepreneurs to efficiently raise capital and investors to participate in a broader range of investment options while being adequately protected.
- *AIMA Canada - National Group of the Alternative Investment Management Association in Canada* – AIMA members include hedge fund managers, institutional investors, pension fund managers and consultants, administrators, auditors, lawyers, prime brokers and other service providers
- *Managed Funds Association* - The Managed Funds Association (MFA) represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets.
- *CVCA – Canadian Venture Capital Association* - represents the majority of private equity companies in Canada, with over 2000 members. The CVCA is a leading source for advocacy, networking, information and professional development for venture capital and private equity professionals.
- *VCMA – Venture Capital Markets Association* - The VCMA represents public companies seeking a Canadian regulatory environment offering access to speculative investment opportunities and capital through fair securities markets that warrant public trust. It seeks to influence improvement in regulations to ensure that they are clear and easily understood and that they allow for effective policing and enforcement.
- *Federation of Mutual Fund Dealers* - is an association of Canadian mutual fund dealers and affiliates whose members have been working to be the voice of independent mutual fund dealers.
- *IFIC – Investment Funds Institute of Canada* - IFIC members include fund managers, distributors and the many professional and back office firms that support the sector. IFICs principal role is to advocate on behalf of the industry and its investors – ensuring their voices are heard by regulators and public policy makers considering the framework of rules that govern investment funds.

- *IIROC- Investment Industry Regulatory Organization of Canada* - is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada.

- *IIAC – Investment Industry Association of Canada* - is the national association representing the investment industry's position on securities regulation, public policy and industry issues on behalf of our 166 IIROC-regulated investment dealer Member firms in the Canadian securities industry.

- *Joint Forum of Financial Market Regulators* - includes representatives of the CSA, the Canadian Council of Insurance Regulators (CCIR) and the Canadian Association of Pension Supervisory Authorities (CAPSA). The mandate of the Joint Forum is to coordinate and streamline the regulation of products and services in the Canadian financial markets. One of the latest Joint Forum initiatives is the development of the Point of Sale Framework.

8. Emerging business trends

Recent years have seen heavy financial pressure on smaller brokerage houses resulting from market conditions and significant loss of profits as well as increasing capital needs for regulatory compliance and capital requirements. This has seen the demise of some firms and the transfer of others to different market segments such as the exempt market.

In 2012, during a review of 87 EMDs and Portfolio Managers by the OSC, it was found that only a quarter had sufficient recordkeeping, including suitability requirements. This development dovetails with indications that Canada's securities regulators are under pressure to follow their international counterparts in imposing a fiduciary duty regime on all financial advisors and dealers that would require them to act in the best interests of retail clients at all times.

The Ontario Securities commission has been exploring the possibility of allowing Crowd Funding where small amounts of capital are raised from large numbers of people over internet based market portals. The methodology is used in other countries by start-ups and small and medium-sized businesses and provides easy access to funds. This is part of the exempt market and there are low barriers to entry as there are no expensive prospectus requirements and no scrutiny by regulators. There is risk of fraud because there are no regulator vetted prospectus requirements and minimal consumer protection. The OSC is currently reviewing and expected to provide guidance.

Restrictions on EMD's: The CSA recently proposed rule changes that would limit the services that EMDs offer; specifically, EMDs may not trade any listed security (on or off an exchange). Accordingly, EMDs would be only able to offer prospectus qualified or prospectus exempt securities. As a result of the proposed rule changes, EMDs may not establish omnibus accounts with any investment dealers.

In March 2014, the OSC agreed to allow "no contest" settlements: The OSC has also recently approved a number of innovative enforcement tools to allow them more flexibility and therefore to manage more cases. In limited circumstances, alleged wrongdoers may be sanctioned and pay a fine without an admission of facts or liability. This will permit the OSC to focus investigations where there are allegations of serious violations.

Increasing counterparty risk: Organizations are becoming more exposed to increasing risk when risk mitigation fails as a result of counterparty failure (e.g. AIG, MF Global)

9. Products and services offered

Investment dealers serve a number of functions, sometimes acting on their clients' behalf as agents in the transfer of instruments between different investors, at other times acting as principals. Investment dealers sometimes are known by other names, such as brokerage firms or securities houses.

Investment dealers play a significant role in the securities industry's two main functions. First, investment dealers help to transfer capital from savers to users through the underwriting and distribution of new securities. This takes place in the primary market in the form of a primary distribution. Second, investment dealers maintain secondary markets in which previously issued or outstanding securities can be traded.

Integrated firms offer products and services that cover all aspects of the industry, including full participation in both the institutional and the retail markets. Most underwrite all types of federal, provincial, municipal and corporate debt and corporate equity issues, actively trade in secondary markets including the money market, trade on all Canadian and some foreign stock exchanges, and provide many ancillary services to securities issuers and large and small investors. Such services include economic, industry, corporate and securities research and advice, portfolio evaluation and management, merger and acquisition advice, tax counselling, loans to investors with margin accounts and safekeeping of clients' securities. Many smaller securities dealers or "investment boutiques" specialize in such areas as stock trading, bond trading, research on particular industries, trading only with institutional clients, unlisted stock trading, arbitrage, portfolio management, underwriting of junior mines, oils and industrials, mutual funds distribution, and tax-shelter sales.

More than 70 foreign and domestic institutional firms serve institutional clients exclusively. Foreign firms account for about one-third of total institutional firms and include affiliates of many of the major U.S. and European securities dealers. Retail firms account for the remainder of the industry. Retail firms include full-service firms and discount brokers. Full-service retail firms offer a wide variety of products and services for the retail investor. Discount brokers execute trades for clients at reduced rates but do not provide advice. Discount brokers are more popular with those investors who are willing to research individual companies themselves in exchange for lower commission rates.

10. Type of customer(s)

The securities sector services a full range of customers and the different types of vehicles used to hold investments. Customer types include individuals, corporate entities both public and private, charities, not-for-profits, pension funds, and institutional accounts which are other securities firm type clients.

Often clients have multiple accounts with one securities firm. The different vehicles used to hold investments includes estates, accounts held in trust, private investment companies, other private companies and organizations e.g. joint ventures and partnerships. Customers are primarily Canadian residents but do include individuals and companies outside of Canada, both Canadians and foreigners.

11. Geographic considerations

In terms of geography, there are licensing requirements for some of the segments of the sector, requiring that registrants be licensed in the jurisdiction where they sell to (where the targeted clients live). Notwithstanding this, some securities firms do have foreign clients and need to manage the risk of whether or not they are registered with the securities regulator in that foreign jurisdiction.

Research indicated that while some firms are cautious (do not accept clients from foreign jurisdictions) others are more aggressive (they do take on foreign clients and may or may not be registered in that foreign jurisdiction). Examples were cited including Canadian securities firms taking on clients from China and Germany.

Appendix 9

12. Key points from interviews

12.1 Sector background

1. There are three regulatory platforms for the securities sector: IIROC, MFDA (mutual funds) and CSA (for portfolio managers and EMDs); this fractured regulation is not helpful for the sector. The oversight regarding jurisdictional and other issues- IIROC reports back to the commissions, the provinces audit IIROC.

2. What is the right regulatory model? There is lots of controversy and discussion over the self-regulating model (IIROC and MFDA) vs the other model (CSA and provincial regulators).

3. The basis of the securities system is disclosure – is everything appropriately disclosed? The OSC for example does not look at the quality of the investment.

4. Inside a registered dealer there is a daily focus on investor protection. There is significant regulatory obligation and this is part of the operations of the firm; e.g. regular reporting to the regulator, subject to regulatory reviews. AML generally is not a part of this, it is done separately. It is only some of the larger organizations that are of sufficient size that they have dedicated AML teams.

5. Dealers are set up to deal with each area of regulation: Business conduct, Trade Conduct and AML (for larger firms). But these groups are not integrated, so need to ensure that the dots are connected between the teams. Some firms have these teams meet weekly; cross training etc. There is a structural issue currently that inside dealer firms, the focus and execution of compliance is on areas other than AML – need to work to make this integrated.

6. Exempt market products (EMPs) come with a significantly lighter disclosure burden than other products and are accordingly less transparent. EMPs are not available to the general public. Exempt market Dealers (EMDs) are required to file an Offering Memorandum with the regulators if there has been a subscription/purchase, but it's unclear to what extent the regulators vet the document and the product. If one were to offer a fictitious product through which illicit funds could be laundered, it would be easier to do it through an EMP than a mutual fund or security, which is more heavily regulated. Similarly, EMDs are not regulated by IIROC or the MFDA. The oversight is detailed and extensive in an IIROC or MFDA firm, something EMDs do not have to contend with.

7. EMDs generally target accredited/high net worth investors who can afford to lose their entire investment, so the typical analysis of whether it makes economic sense to invest in an EMP can't really be used as a factor in assessing the reasonability of the transaction. Also, because the typical amount invested is much larger than the average retail client, if there were illicit activity, the magnitude would generally be greater on a transaction by transaction basis.

8. EMDs often have a small number of very large clients. The EMD may therefore be seen as beholden to each client to a much greater degree than the average retail client, increasing the risk that they may bend the rules in favour of a client.

9. While not specific to EMDs, many EMDs are smaller firms, and where a firm has limited staff and the President also acts as Chief Investment Officer and CCO, there is not necessarily a segregation of duties that allows for independent monitoring of ML. This could lead to heightened AML risk.

10. More of the industry is good at taking care of client money. The industry is not so good at assessing broader risks and the industry needs to start getting at this.

11. Doesn't think the Canadian securities industry is that good at analyzing risk, the requirements are so prescriptive and detailed today it is hard to stand back. It is not a principals based approach today at all. Believes that the risks today are not met with the prescriptive approach, need principals based. How will people learn this if we don't start doing it? This is quite a sensitive topic amongst the peer group. It is the regulators that need to change the approach and thinks they should start in a less sensitive area like financial management. Today there is much just doing (ticking the boxes) vs. really thinking about the risks and mitigating.

12. Some dealers are not that good at identifying risk, the smaller firms don't have the resources, smaller firms have inherent risk, independence issues. Agrees that there is a size tipping point, lets larger dealers manage risk. However, a larger dealer could miss risky things due to volume of transactions. Example: Brokers from Bolivia looking for relationships with Canadian firms. This has come up and does happen. A firm may be desperate to keep the doors open, looking at the good, no eyes for AML risk.

13. Another individual did not believe that a principals (versus a detailed prescriptive rules) would work in this sector, thinks we need the rules – 'greed has no conscious'. A huge busy brokerage, things move too fast throughout the day, operations are too bureaucratic to run on principals. Compliance is seen as a department that stops them from making money.

14. Processing work in the back – they know how to follow the rules – but generally these are younger, less experienced, not credentialed people. Does not believe that they can be expected to apply a principals based approach. Rules are needed because the trades can't fail, this is the market.

15. Each jurisdiction wants to protect its own citizens. Always look at how and where clients came to the firm – usually there is a relationship. If a person/client just came out of the blue – many dealers wouldn't take that file.

16. If investment dealers wanted to do business with foreign persons: If the person came from a well regulated jurisdiction – the firm should be registered there. If this is not so obvious – need to use a risk based approach. If person is from China? Client from Germany? If the client is well known, if there is anything mitigating, then the firm may take a risk but often the larger firms decide not to. This does happen though– China, Germany, Zimbabwe. There is a business risk to dealing in foreign jurisdictions; don't know the rules of the foreign jurisdiction, unregistered dealing. Usually requires more due diligence. Some firms are not concerned with foreign regulators; some would not allow any foreign clients – others would; there is a wide spectrum – and more firms are paying less attention to this rather than more.

17. IIROC does look at the directors of its registrants, have to have a 'registered executive'. IIROC approves and could disprove. Not sure that the provincial commissions monitor the governance, directors/ownership of the registrants in the exempt market. There is an ease of access to the EMD

registration. To become an exempt market dealer must follow the CSA rules. This is all within the purview of the CSA, the rules, the process, and the sufficiency requirements.

18. Many firms only provide Delivery Against Payment (DAP) services, meaning that these are all settlements of the transaction and it is the bank that receives the funds locally with a prime broker:

    a) Omnibus account – usually a big bank securities arm – this is used for the trades.
    b) The dealers just settle the trades – not any cash; they don't hold money for purposes of future trades – prime brokers do this.
    c) Both are agents to the client; one provides trade execution only, other has custodian and possibly trade execution as well.
    d) Prime broker can see more than the broker dealer, prime broker needs to monitor at these many levels.

19. Generally, the trader wants to make more money, more points – this is what this business is all about. Registered representatives (RR's) make all their money on commission, so the regulators have made specific things offences to try and keep it fair. The business is about making money.

20. Believes that compliance is not as lily white as they should or could be. Regulators have to make the pain of doing the wrong thing so intense in order to deter/prevent illegal activity. And the probability of being caught has to be high. But the question today is, even if they are caught, what happens? The regulators are challenged with proving knowledge, proving intent to get a fraud conviction. Insider trading is so hard to prove, and people know this.

21. Provincial regulators, OSC for example, can have jail terms for some charges, and are working with IMET/police groups and so are seeing more charges laid now; this information is contained in press releases.

22. Fraud involving securities – there are many, many jurisdictional issues, so it does not get attention even though there are laws, hard to get police authority attention.

23. Exempt dealers, believes that these individuals have very limited backgrounds. Requirements include a Canadian Securities course, it is done on computer, believes that course can be passed without having to do the number/calculations parts. They get their exempt dealer licences and then can sell whatever they have; exempt market does not have to give offering memorandums as are only selling to accredited investors. Note though that if an exempt market dealer is also an IIROC dealer, they must sell all product through the IIROC dealer license. This is a good rule, principals based.

24. The thresholds for an accredited investor (Ontario): Financial assets - $1M, Net worth - $5M, Family income $300K.

25. Believes that brokers are thinking about making money within the rules, not so much about investor protection. The Securities Act is not written considering all of the bad activity – it assumes good faith and this is often not the case anymore.

26. This stuff (illegal activity in the securities industry) is going to happen; the trick is to keep the balance between useful markets and fraudsters.

27. One belief that 70% of illegal activity in the sector is "I can make money illegally in the market" and 30% is "I can use the sector to hide/cleanse my money".

28. There are always excuses and technicalities that challenge enforcement (MRS case, limelight case). What can a provincial commission do? Commission can issue a cease trade order – but then they (fraudsters) just find another way in from behind the scenes. Cease trade order would only matter to the larger firms. Other groups, change titles but still continue the activity. Bad guys know the law better than we do.

29. Believes illegal activity is 'rampant'; there are opportunities for RRs to make $50,000 to $100,000 per month, and what really is their risk? A commission does not have criminal authority, the defendants have too many excuses, hard to prove intent to fraud unless have wire taps. Crowns rarely touch these files.

30. They see cases where IIROC or a securities commission have detailed knowledge of the full pattern of a target's trading but the individual firms see only part of the picture which on its own is not suspicious. In earlier times, there were mechanisms for the exchange of information on such matters, but now strict rules mean that they will only discover such cases when the regulator visits. A better (secure) warning system for such trends would prevent such problem clients from getting in the door at all. The changes really happened when IIROC became the regulator and the roles were split.

31. There are no cash transactions anymore and some suspicious customers, for example those wishing to trade in closely held companies or deposit OTCBB shares, find it hard to open accounts because no one will take them as clients.

32. The dealer industry is small and there are only a few firms who will even get approached now with problematic deals because of the compliance programs at the larger firms. The smaller firms have fewer compliance resources and may be targeted for this reason.

33. From their point of view, the risk and cost of a regulatory compliance investigation is just not worth it. They are aware of securities dealers who are still willing to turn a blind eye. They have the resources to try and find out what is going on with clients and where the money comes from, but others with the same skills and resources are wilfully blind. They are also not able to discuss any of their findings on a refused client with other firms and the IIROC cooperation rules do not give them the protection/coverage they need. They risk a lawsuit if they provide background to another firm.

34. They saw a lot of Chinese companies going public on the Canadian market but since Sino Forest this has been curtailed. Their industry is generally poor at submitting STRs because of all the other compliance requirements and regulators they deal with. They themselves submit about 10 to 30 a year.

35. They feel that their attempts to alert authorities regarding suspected criminal activity often falls on deaf ears e.g. RCMP IMET teams and FINTRAC.

12.2 AML Compliance

36. The exempt market is not fully compliant in a number of areas including AML. This is the combination of several factors, including:

    a) 'Until someone really forces me to, I might not comply.'
    b) Some "dealers" don't see themselves as part of the securities industry – they see themselves as working for the companies. The regulators are kicking them a bit on this to get them into shape.
    c) While some are now beginning to accept that they need to be regulated, they don't see themselves as gatekeepers yet for the investment industry.

37. It is the view of the compliance officer that the AML paper trail in their industry is easy to manage and that competent money launderers are completing it all with believable and supportable stories and then taking a modest approach to trading so that no red flags are raised. They are not in a position to determine the true source of the funds in any detail in these cases, even if they suspect money laundering.

38. If money laundering is suspected, an STR is submitted and this firm has, more than once, delayed clients from removing money after an STR has been filed (or multiple STRs) to allow the authorities to take action. In this respect they do not believe that broader detection and enforcement systems are effective (in some cases).

39. AML systems focus on the source of funds from PEFPs but not really from others which means that with a suitably developed story, low profile laundering can proceed undetected.

40. They are aware of organized crime money laundering schemes tied into pump and dump schemes "out west". This is a combination of new crime funded by old proceeds i.e. laundering them through the scheme producing new proceeds.

41. The key indicator of money laundering for them is trading patterns and they monitor this closely, when they see a problem they shut down the accounts quickly.

12.3 Trends

42. Business is migrating to the exempt market. What is causing this? Formalization of the category, starting to recognize the EMD sector as legitimate, that it can be successful. Could there be other reasons, like it is an easier segment to operate in because there are fewer rules? While the IIROC member rules do not apply, the fundamentals still do apply. Who is reviewing to make sure rules are followed? Not IIROC it is supposed to be the commissions at the provincial level across the country.

43. The picture on the use of nominees has changed, they still have clients using offshore nominees but they are legacy clients they are very comfortable with and they don't take new ones. They see fewer people using secretarial and junior staff to open trading accounts but more people using junior lawyers and accountants who need the work and are not experienced enough to understand the risks.

12.4 Risk Areas

12.4.1 Exempt market:

44. While not specific to EMDs, many EMDs are smaller firms, and where a firm has limited staff and the President also acts as Chief Investment Officer and CCO, there is not necessarily a segregation of duties that allows for independent monitoring of ML. This could lead to heightened AML risk.

45. If one were to offer a fictitious product through which illicit funds could be laundered, it would be easier to do it through an EMP than a mutual fund or security, which are more heavily regulated.

46. Ease of entry into the EM market is an AML risk. The regulators would be in the best position to actually assess how easy it is to enter the market. As with all business sectors, AML is made easier if there is collusion with someone inside the institution.

47. How to track the exempt market? Look at examples of when the exempt product is bought by a public company. This might allow for some tracking. Pick a higher risk business, e.g. payday loans. If this company is lending out money to consumers at say 17%, the financing for this is not from banks, it is likely from private EM sources, and perhaps they pay 14% and they keep the 3% difference. Where does the money come from? This is the question.

48. The exempt market has lots of good players but there are also a number who are bad. They do take EMD clients but are aware of the risk in some of the deals and with some players.

12.4.2 Off Book Transactions or Unregistered Activity:

49. The concern with potential ML in the sector is with unregistered/off book activity. Each regulator has put out guidance on off book transactions- look for the IIROC paper on this. How prevalent are off book transactions? 'Where the potential is there, it represents a serious problem.' Non-brokered private placement, this is jargon for 'off book'.

50. Example: An individual lines up a group of investors for a high risk product which provides liquidity to businesses who can't get money from banks. This activity is supposed to be run through an EMD. However, they are seeing much activity done unregistered and off book, which means that there are likely no compliance procedures done at all, nothing done in this regard. Clients are happy to put money up, they receive 14% as long as the business stays alive (these are high risk, and this is why often they cannot get bank financing) the investor can often get their whole principal back. No scrutiny of how this is being done. This activity is stuff that the CSA is supposed to watch out for via the provincial regulators. There are many reported disciplinary cases posted on the IIROC website. For sure money laundering activity is occurring.

51. Another example provided by a different individual: 100 clients are brought together to provide 'off book' funding. $30M is invested with a high risk business, the clients receive a high rate of return and they have contractual rights (limited partnership, debentures). This is rife for money laundering because the transactions are not subject to any scrutiny. Contrast this to private placement by an EMD for a high risk business by accredited investors- this would be legitimate and subject to all appropriate regulations/compliance and oversight.

52. The following is also happening: a representative who says these are my clients, I facilitate the connection to the exempt market products, I don't need to put this on the books, it is personal, says it is not a problem and it is just done as unregistered activity.

53. Sector needs to be more vigilant regarding unregistered activity, and this needs to be done by the regulators.

12.4.3 Registered Representatives (RRs):

54. The registered representatives within the broker firms themselves, this is the weakness in the securities sector for fraud and money laundering. A company called Firestar, organized crime figures were involved, four main street brokerage houses raided, the RR had a separate book for stocks he was selling, they pulled emails & taped cell phones. Basically, the trade looks like it was being made, the private book was for the RR to get paid, the buy/sell prices were instructed. Criminal money buys a company, the company creates or has options, these are what gets traded, the buy and sell of the options is controlled by the criminal money and they use the RR to do this. The criminal money uses the RR to set a price of say $10.25 and then they tell the RR who is going to buy. The price goes up in the market, the RR pushes the product to other representatives, then the criminal money makes money in the market on the options.

55. The RRs make money, a lot of money. One individual said that the above example is just that, an example of activity that is going on, is not an isolated case. One organized crime figure who recently died in the US and was sent back to Canada – they were involved in this activity, in Ontario. It is just a matter of connecting the dots, private placement is where the risk is and these are highly regulated firms where this activity is going on. Other cases to read up on: Da Selva, MRS sciences, limelight, Maple Leaf – Henry Chau – Carousel Islands - $21 million from Canadian Chinese investors. Look at the IIROC notices.

56. Considering the level of ethics and integrity at the front lines (low, vulnerable), it is easy to compromise these people. There are so many RRs; the chances of being caught are very slim, at least 80% chance of not getting caught, only a few examples are made.

12.4.4 'Nested accounts'

57. These have a similar structure to correspondent banking; one interviewee agrees that there is risk. Basically, there are exemptions for institutional clients. A corporation is viewed differently, less risk vs. an individual. Usually there are more exemptions for institutions as the institution is registered with the foreign jurisdiction (banking or securities registration), the idea being that that authority is monitoring them. What due diligence does a firm do regarding these accounts? Generally nothing more than checking that the institutional client is registered and in good standing with that jurisdiction. Dealers are generally not looking at beneficial ownership.

58. There is a reason though for "nested accounts", securities firms must transact using a registered dealer in that jurisdiction, this is required. Example: CIBC provides services to Barclays bank offshore who wants to trade in RIM; CIBC relies on Barclays to do all of the know your client work, and CIBC is allowed to. Institutional clients are defined within the IIROC rules.

12.4.5 Offshore accounts:

59. 'You can pick up an offshore company very easily', so the securities industry should not be accepting these clients without scrutiny; this is perhaps where the institutional client exemption rules provide vulnerabilities to the regime.

60. They have seen accounts where the "client" is an offshore bank in Western Europe e.g. Switzerland or Liechtenstein dealing with a German or British asset manager who's ultimate client is in London and has a UK passport even if they were not born there. They try to document fully but the financial establishments refuse to identify the ultimate clients or alternatively state that the trading is for the "house account" but it may well be for a nominee. They have declined clients like this. The key indicator is trading on the US Over The Counter Bulletin Board ("OTCBB").

61. Other than above example, they have not seen an influx of foreign clients or money in their space.

12.4.6 Use of Nominees

62. The picture on the use of nominees has changed, they still have clients using offshore nominees but they are legacy clients they are very comfortable with and they don't take new ones. They see fewer people using secretarial and junior staff to open trading accounts but more people using junior lawyers and accountants who need the work and are not experienced enough to understand the risks.

12.4.7 Smaller firms

63. The dealer industry is small and there are only a few firms who will even get approached now with problematic deals because of the compliance programs at the larger firms. The smaller firms have fewer compliance resources and may be targeted for this reason.

12.4.8 Trading in Closely Held Companies or OTCBB Shares

64. There are no cash transactions anymore and some suspicious customers, for example those wishing to trade in closely held companies or deposit OTCBB shares, find it hard to open accounts because no one will take them as clients.

12.4.9 Trading strategies that are neutral

65. Some of the trading strategies are so complex these days that it is hard to understand why clients are undertaking them. One interviewee shared that one of the ones they had become aware of was an 'Iron Butterfly' which is basically a neutral trading strategy so that a maximum loss amount is set through four different trades of the same security (depending on movement of the underlying stock it is possible to make money, but the maximum loss is fixed). These types of trades are going on and they are often quite complex. There are significant commission charges on setting up these complex trades, so unless it is an investor doing these trades on their own, under low cost discount brokerages (trying to earn a conservative return and not beat the market) they really make no sense unless perhaps money laundering was the objective.

13. Risk factors

13.1 General market

13.1.1 Regulatory Fragmentation of the Securities Industry

The securities sector is highly regulated; and the focus of this regulation is on investor protection. Interviewees shared that securities firms often do not see themselves as gatekeepers for the industry in regards to money laundering/illegal money and simply follow regulations on a prescriptive basis. Accordingly, the approach to AML compliance is often not based on principles but on simply following the prescribed rules.

Securities sector regulation is seen as fractured and siloed. Anti-money laundering procedures are usually considered separately/independently rather than part of a firm's integrated approach. Research indicates that the risks of funds being illegally sourced, if considered, are not integrated with the rest of the firm's regulatory compliance procedures. For example, firms are required to monitor for trading manipulation, however this same activity when being monitored for this purpose is likely not being monitored for any indicators of money laundering. As another example, investor suitability is a key requirement which receives significant compliance oversight and monitoring, but how this integrates with what the risks are for money laundering is not known or executed on in any detailed way within most firms.

Fragmentation of the Canadian regulatory environment exposes the financial system to at best, over-regulation of certain segments and at worst, little to no regulation – for instance, there are no Canadian regulators that have determined that the potential manipulation of 'Cdor' – the Canadian Dealer Offered Rate – is under their jurisdiction.

13.1.2 Quality and Ethics of Firms/Sales Individuals

Research indicates that there is high pressure and competition to complete deals and earn commissions; and at the same time, a low chance of being caught (if they do something wrong) and even if caught, the penalties are not seen as high.

Several examples provided by interviewees of registered representatives (RRs) being compromised with illegal money to provide assistance to criminals.

Interviewees shared that they are aware that organizations, understood to have the capability and resources to identify problematic situations, are wilfully blind and take on the client accounts; including larger organizations.

13.1.3 Inability to Share Information Within the Sector

Interviewees reported that they are not able to discuss any of their findings on refused clients with other firms; citing that the IIROC cooperation rules do not give them the protection/coverage they need. Firms risk being sued if they provide this background to other firms.

Interviewees reported that they had seen cases where IIROC or a securities commission had detailed knowledge of the full pattern of a target's trading but that the individual firms saw only part of the picture, which on its own was not suspicious. Apparently, in the past, there were mechanisms for the exchange of information on such matters, but now strict rules mean that they would only discover such cases when the regulator visits and provides the information. Desire was expressed for a warning system for such trends so as to prevent such problem clients from getting in the door at all.

13.1.4 High Level of Fraud Within the Sector

The securities industry is prone to being used to generate illicit funds through stock market manipulation, insider trading, and fraud. All of these are "predicate" offences for money laundering and thus the movement of the funds after these frauds results in money laundering in addition to illegal funds entering the securities industry from others sources. While the risk of fraud and manipulative trading is inherently high, current regulations require securities firms to monitor trading activity for these risks.

"While the RCMP Proceeds of Crime Program rarely focuses on securities infractions, it is safe to assume that much of the revenue that is generated through such breaches as insider trading is at least initially or partially laundered through the capital markets, taking advantage of the same processes and vehicles utilized in the original crime. A particular challenge is determining when the securities offence ends and the money-laundering offence begins."[10]

13.1.5 Ease of Entry into the Exempt Market

Interviewees reported that the requirements to become an exempt market dealer are not as onerous as other securities registration categories. The requirements include a Canadian Securities course done electronically. Once their exempt dealer licence is obtained, they can sell whatever they want. Some exempt market products do not require offering memorandums as they are only selling to accredited investors. Some interviewees believed that these individuals had very limited relevant experience.

As per National Instrument 31-103 the registration requirements for an exempt market dealer – dealing representative are as follows:

A dealing representative of an exempt market dealer must not act as a dealer on behalf of the exempt market dealer unless any of the following apply:

a) the individual has passed the Canadian Securities Course Exam;
b) the individual has passed the Exempt Market Products Exam;
c) the individual satisfies the conditions set out in section 3.11 [portfolio manager – advising representative].

[10] Money Laundering in Canada, Beare and Schneider

13.2 Product and service

13.2.1 Unregistered Trades and Deals

Non-brokered, private placement deals represent very high risk – these can be through securities brokers (EMDs or other) or non-brokers. This basically is activity that should be regulated under securities laws, but the securities professionals involved do not subject these transactions to any scrutiny. These deals can be used to perpetrate fraud or as part of activity to launder funds. The risk is seen as very high as there is no scrutiny by regulators or the compliance departments in securities firms.

13.2.2 Off Exchange Securities or Penny Stocks

Over the counter (OTC), Bulletin Board (BB) and Pink Sheet trades as well as thinly-traded securities are considered higher risk of money laundering due to less scrutiny applied and the potential for market manipulation.

Interviewees reported that those wishing to trade in closely held companies or to deposit OTCBB shares are finding it harder to open accounts because no one will take them as clients because the risk is seen as high.

13.2.3 Accredited Investor / Exempt Market Products (EMPs)

Products in the exempt market are generally less regulated, are subject to less scrutiny and should only be sold to accredited investors. Exempt market products come with a significantly lighter disclosure burden than other products and are accordingly less transparent. EMPs are not available to the general public. EMDs are required to file an Offering Memorandum with the regulators if there has been a subscription/purchase, but it's unclear to what extent the regulators uniformly vet the document and the product.

Interviewees indicated that if one wanted to offer a fictitious product through which illicit funds could be laundered, it would be easier to do it through an EMP than a mutual fund or other type of security, both of these areas being more heavily regulated.

Interviewees reported that the typical amount invested in EMPs was generally much larger than the average retail client, so if there were illicit activity, the magnitude would generally be greater on a transaction by transaction basis.

13.2.4 Emerging New Investments and Technologies

New investments and technologies that are not within the regulations of traditional investments will evolve and grow quickly, challenging the resources of regulators and exposing the market to fraud risk. For example, precious metals and stones dealers providing these products to the market as wealth management type service, securities advisors.

13.2.5 Specific Trading Strategies e.g. 'Iron Butterfly'

While interviewees did not identify some of the more well-known methods of money laundering through the securities sector as risk factors, e.g. establishing multiple accounts to trade one-for-one, the use of more complex, neutral trading strategies was identified as a risk that is occurring within the sector.

13.3 Delivery Channel

13.3.1 Exempt Market Dealers (EMDs)

Many EMDs are smaller firms, and where a firm has limited staff and the President also acts as Chief Investment Officer and CCO, there is not necessarily a segregation of duties that allows for independent monitoring of money laundering.

Research indicates that the exempt market is generally comprised of smaller organizations that traditionally have fewer resources to spend on compliance. Clients of these firms tend to be accredited with a higher net worth and accordingly no suitability review is required. The OSC identified in a 2012 report that often EMDs were not properly ensuring that clients met the accredited investor thresholds.11

Smaller securities firms and representatives in the exempt market are presented with the opportunity to earn higher commissions and therefore there is the potential for greater willingness to bend the rules for these investors. EMDs often have a small number of very large clients; the EMD may therefore be seen as beholden to each client to a much greater degree than the average retail client, increasing the risk that they may bend the rules in favour of a client.

13.3.2 Off Book Transactions or Unregistered Activity

Also may be referred to or conceptually similar to 'rogue employees' in some of the authoritative AML literature. Interviewees stated that there was significant concern with unregistered/off book activity conducted by securities registrants and that this was vulnerable to money laundering. 'Where the potential is there, it represents a serious problem.'

A search of the IIROC website for disciplinary notices and decisions regarding 'outside' business activities identifies many cases involving registrants (individuals) who had engaged in outside business activity without the knowledge of their IIROC Dealer member firm and without their consent. Appendix A includes some of these notices.

13.3.3 Size of the Securities Firm

Interviewees stated that the dealer industry was small and that there are only a few firms who get approached with problematic deals because of the compliance programs at the larger firms. And that the smaller firms have fewer compliance resources and may be targeted for this reason.

---

[11] OSC Staff Notice 33-738; 2012, OSC Annual Summary Report for Dealers, Advisers and Investment Fund Managers

13.4 Geography

13.4.1 Clients from Foreign Jurisdictions

Firms servicing foreign clients from jurisdictions where the firm is not registered are seen as significant risk, not only because of the securities industry investor protection rules (e.g. Canadian firm should be licensed to deal in all of the jurisdictions they have clients and should not deal in jurisdictions where they don't have licenses) but also due to the red flag of why a foreign individual needs to access the Canadian securities sector directly and not transact through local securities firms.

13.4.2 Offshore Companies

Research indicates that the use of offshore companies to invest in Canadian securities is a risk factor. Regardless of whether or not these companies are institutional clients (registered with off shore regulators) they should not be accepted without scrutiny, as beneficial ownership is easily hidden, and trading / funds flow should be monitored.

Interviewees reported that they have seen accounts where the "client" was an offshore bank in Western Europe e.g. Switzerland or Liechtenstein dealing with a German or British asset manager who's ultimate client was in London and had a UK passport even though they were not born there.

13.5 Business Relationships / Linkages with Other Sectors

13.5.1 Sector Reliance on other Jurisdiction Regimes

Generally, within the sector in Canada, there are more exemptions for 'institutional' clients than individual clients. Institutional clients are generally understood to be entities which are registered with securities or financial regulators. These regulators could be Canadian, but they could also be foreign; distinctions in the industry are made between foreign FATF countries and non-FATF countries. When these clients provide proof of registration, many Canadian securities firms exempt these clients from their KYC processes and the level of due diligence becomes minimal e.g. there are cases where nothing additional is done. Some interviewees reported that a risk based approach was applied so that in higher risk cases more KYC procedures were done. It appears that generally beneficial ownership is not being determined. Complicating these relationships is the concept of 'nested accounts'. Once the institutional account is set up, the account has a similar structure to correspondent banking and the Canadian securities firm often would not know the identities of the underlying clients.

One interviewee provided the following example: CIBC provides services to Barclays bank offshore who wants to trade in RIM; CIBC relies on Barclays to do all of the know your client work, and this is allowed.

The above relationships are also understood as the relationship between introducing and clearing broker–dealers.

13.5.2 Lack of Clarity in the Sector as to Who is Monitoring Transactions When Omnibus Accounts Used

An omnibus account is an account which has been established when an entity is acting as an intermediary on behalf of multiples parties or entities. Often in the securities sector firms only provide DAP transactions, meaning that they take delivery-against-payment and they do not hold any customer funds on account. Customer funds are maintained with a custodian, usually the brokerage arm of a major financial institution, a prime-broker' and often

this is in an omnibus account. The risk in these situations, as reported by interviewees, is that it is not clear how and who is monitoring for money laundering risk. The broker-dealer who only transacts on a DAP basis, has the client relationship but may be (and this was generally communicated to be the case) viewing these transactions as low for any money laundering risk because it is the prime-broker who actually receives the client funds and holds money on account.

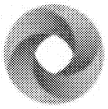
13.5.3 Use of Nominees:

Research indicated that the use of nominees has changed. Clients may still use offshore nominees but these were more likely legacy clients (established relationships, level of comfort on transaction and money flow) and that new ones (off shore nominees) were not being taken on. Fewer people are using secretarial and junior staff to open trading accounts but more people are using junior lawyers and accountants who need the work and who are not experienced enough to understand the risks.

13.6 Transaction Methods and Types

13.6.1 Transactions which are conducted using physical or bearer securities

The anonymity and easy transferability of bearer securities presents significant vulnerability at all three stages of the money laundering. While, these were not highlighted as areas of concern by interviewees, research indicates that these products are still encountered in the Canadian securities market, although this is less the case than in the past.



Grant Thornton

Reporting Entity Sector Profile: Accountants

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

For purposes of this report, we have defined 'accountant' to include persons who have demonstrated competency through professional examination and certification. In Canada, this includes accountants qualified as CPAs- Chartered Professional Accountants (formerly CAs- Chartered Accountants), CMAs- Certified Management Accountants and CGAs- Certified General Accountants.

Accordingly, we have not focused on the activities of some individuals who work in the field of accounting or provide accounting, tax, or payroll services, e.g. bookkeepers who provide these services or individuals who are not certified but who may work in the accounting departments of companies[1].

The segments making up the sector include public accounting firms and accountants who work in industry. The large accounting firms are the largest employers of accountants worldwide, and this is true for Canada as well. However, most accountants are employed in industry, working with commercial businesses, not for profits or with the public sector.

The market is dominated by the larger "big four" accounting firms; Deloitte, PwC, KPMG and EY, as well as two other global accounting firms, Grant Thornton, and BDO. There are many other firms including national ones which are affiliated with other firms internationally, regional firms and then smaller, one office firms and sole practitioners. Other than the differentiators of size and specialisation, there is no real further segmentation in the market.

The professional services market in Canada is self-regulating, one of the few in Canada, and has been this way since inception. Historically, the sector has been quite fragmented, including the three major certifications (CA, CMA and CGA) each having their own independent associations and each with their own provincial self-regulating organization. A unification initiative is currently underway by the three main groups. There are estimates that if/once national unification is achieved, that there would be over 125,000 individual members and approximately 20,000 students.[2] Approvals and agreements must be obtained and undertaken by all three bodies on a province by province basis to achieve unification.

CPA Canada (Chartered Professional Accountants of Canada) states that it represents a total membership of over 70,000 professional accountants in Canada.

[1] Note that the statistical data and charts provided do include some of the activity/segments of non-certified accountants, e.g. bookkeepers.
[2] "Uniting the Canadian Accounting Profession", May 2011 - http://unification.cpacanada.ca/wp-content/uploads/2011/12/Position_Paper.pdf

A significant number of risk factors have been identified, including as listed below, and these are detailed further later in this document:

- Smaller accounting firms and independent practices are seen as more likely to provide services to illegal/unethical activity, whether wittingly or unwittingly. There is often very little quality monitoring infrastructure and the practice is dependent on the ethics of the specific individuals involved;
- Provision of higher risk services including complex tax planning and structuring, wealth management and corporate finance services;
- Referrals made to offshore affiliates and/or clients located in higher risk jurisdictions;
- Conflict of interest issues, as the advisory services practices of firms extends, there exists more opportunity for conflicts impacting the independence of the auditor/accountant from the underlying client. Recent regulatory cases highlight how seriously regulators are treating these issues; and
- Accounting services provided when third parties are involved, including the use of lawyers for legal privilege.

2. Structure, size and segmentation, reporting entity population

Our review of the NAICS codes for the sector identified two relevant codes; "Accounting, tax preparation, bookkeeping and Payroll services" (NAICS 541211), which has a total of 9,917 establishments. A second code for "Other accounting services" (NAICS 541219) has a further 2,214 establishments.

Included at Appendix A is a table of 'Canada's Top 30'. This is data on the top 30 accounting firms (by revenue) in the country and is published annually in the Bottom Line, an accounting sector focused publication. The data provided for April 2014 shows that the top 30 firms had:

- Revenue of $7.420 billion with the top four firms reporting $5.158 billion or 70%;
- 25,898 professional staff, with the top four firms reporting 16,366 or 63%; and
- 582 office locations across the country.[3]

These accounting firms are generally limited liability partnership organizations with practices led by the individual partners. The larger firms tend to have more integrated practices with a higher degree of national infrastructure, supports and monitoring of individual partners providing services to clients and accordingly have built and maintain a higher level of 'brand' recognition in the market. The medium and smaller firms tend to be partnerships which are less integrated; more the sum of the individual partner practices and success is based on the individual partner client relationships.

The largest six firms are understood to all be Canadian partnerships which are member firms of international networks that operate under the same name globally. So while each country is an independent partnership providing services to the public, the firms within each international network cooperate and provide support to deliver to clients who operate multi-nationally. One of the emerging trends is that some of the larger firms in the US and Canada are beginning to open offices in overseas locations (e.g. India) and this office is owned and managed by the US or Canadian partnership.

[3] The Bottom Line – Canada's Accounting Top 30, April 2014

The top 30 accounting firms would include accountants from all three major groups as well as uncertified accountants; however the majority of professionals employed would be ones with the CPA (formerly CA) designation.

As is the case with the CPAs, most CGAs and CMAs work in industry. However there are many CGAs and CMAs who provide services to the public. An online directory of CGAs and CGA firms provides data on 2,322 across the country[4]. And while a directory of CMAs providing services to the public was not identified, all CMAs providing services to the public are required to register their practice with the appropriate provincial group (e.g. in Ontario this is CMA Ontario) and to adhere to regulations which set out criteria for members who independently offer their services to the public[5].

[4] http://www.needanaccountant.org/
[5] http://www.cmaontario.org/CMACandidates/Post-CMADesignationCredentials/CertifiedManagementConsultant/ConsultingCMAs.aspx

3. Economic and financial statistics

The Canadian accountancy market has seen low to moderate growth since 2008 and the market is forecast to continue performing this way through to 2017.

As indicated, the Canadian accountancy market is characterized by the presence of four large firms and these firms exercise significant influence, particularly at the upper end of the market, regarding services provided to public companies.

The Canadian accountancy market had total revenues of $11.9 billion in 2012, representing a compound annual growth rate ("CAGR") of 1.2% between 2008 and 2012. In comparison, the US and Mexican markets grew with CAGRs of 0.7% and 5.7% respectively, over the same period, to reach respective values of $132.0 billion and $16.2 billion in 2012.[6]

Audit services are the most significant component provided in the public accounting market, with total revenues in 2012 of $5.2 billion, equivalent to 43.7% of the market's overall value. The advisory segment contributed revenues of $3.6 billion in 2012, equating to 30.3% of the market's aggregate value.[7]

The performance of the market is forecast to follow a similar pattern with an anticipated CAGR of 1.2% for the five year period 2012 - 2017, which is expected to drive the market to a value of $12.6 billion by the end of 2017. Comparatively, the US and Mexican markets are forecasted to grow with CAGRs of 3.7% and 7.9% respectively, over the same period, to reach respective values of $158.6 billion and $23.6 billion in 2017.[8]

Table 3-1 - Canada accountancy market value: C$B, 2008-2012

Year	C$ Billion	% Growth
2008	11.3	
2009	11.6	1.9%
2010	11.6	0.5%
2011	11.9	2.2%
2012	11.9	0.2%

Source: Accountancy in Canada – August 2013 – MarketLine Industry Profile

[6] MarketLine Industry Profile - Accountancy in Canada, August 2013.
[7] Ibid
[8] Ibid

4. Regulation of the sector

As indicated, the accounting profession is self-regulating and while there are unification efforts underway, accounting certification and regulation is done by each of the ten provinces and two territories and is divided between the three main national accounting groups (the CPAs, CMAs and CGAs). So for example, currently the provinces of Quebec and Ontario are the only jurisdictions in Canada able to certify members as CPAs.

All other provinces and the territories must award CAs. Legislative change must occur in each jurisdiction and until legislative change is complete, each provincial and territorial CA institute will continue to grant the CA designation. Once the unification efforts are complete, each jurisdiction will then be able to issue all CAs the CPA designation and to issue all new members with CPAs.

The sector self-regulation means that each group/association that advocates for the profession also regulates its members. Details of the groups and their mandates/membership are provided below in the Description of Sector Associations report section.

As a self-regulating profession, the provincial institutes are responsible to protect the public interest by ensuring that all Members, Students and Firms observe high professional and ethical standards. Generally, this is done by a program of interrelated activities that includes:

- High standards of qualification, involving both a demanding education program with a rigorous final examination, and a significant period of prescribed practical experience under authorized supervision;
- A comprehensive professional development program;
- An internationally-recognized, mandatory practice inspection program directed to ensuring that members and firms engaged in public practice maintain prescribed professional standards;
- Practice and ethics advisory and counselling services; and
- A comprehensive and well-resourced disciplinary process that, through experienced members of the profession and public representatives, deals on a timely basis with complaints and other matters concerning the professional conduct of members, students and firms.

A professional conduct committee or similar body investigates written complaints received. Once a decision is reached in the matter, both the complainant and the respondent have an opportunity to be further heard, after which, depending on any change to the decision, the matter is generally forwarded to a discipline committee. In Ontario for example, the Discipline Committee has powers to make specific orders, including the following: fines, charges for costs of the investigation, suspension, expulsion, training and/or examinations, period of supervised practice, reinvestigation, and/or that an accountant's practice be restricted for a specified period of time. There is then an appeals process available.

- *Canadian Public Accountability Board* – CPAB is Canada's audit regulator for reporting issuers as defined and it functions to assess audit quality through the inspection of selected high-risk sections of audit files and assessment of the six elements of quality control. The Canadian Securities Administrators' National Instrument - 52-108 Auditor Oversight, requires auditors of reporting issuers to be registered with CPAB, as CPAB participants, and requires Canadian reporting issuers to issue financial statements audited only by CPAB participating firms.
- *Public Company Accounting Oversight Board* – PCAOB was established by the US Congress to oversee the audits of public companies in order to protect the interests of investors and further the public interest in the preparation of accurate and independent audit reports. The PCAOB also oversees the audits of broker-dealers, including compliance reports filed pursuant to federal securities laws, to promote investor protection. The PCAOB has a significant influence on a number of Canadian accountants as many Canadian companies are listed on US exchanges or are affiliated with entities listed on US exchanges.

Other laws and regulations are increasingly having an impact on the sector. Public accounting firms are experiencing not only civil litigation from commercial interests as they intersect with these laws but also questions and expectations from regulators. Both groups are looking at the firms as 'gatekeepers' when audit and other types of services are being provided. Our research has identified specific statements to this effect in both Canada and the US, and we have identified examples relating to frauds and company failures, breaches of anti-corruption laws, AML regulations and the emergence of the newer FATCA (Foreign Account Tax Compliance Act) regulations out of the US.

5. Educational and licensing requirements

In order to become a CA/CPA one must first obtain a university degree. Following graduation the student must gain work experience under the supervision of experienced CA's within organizations (CA firms, corporations or government organizations) that have recognized CA training programs in place. All candidates must ultimately pass an exam in order to obtain the CA designation. The profession works to develop and maintain a uniform standard for qualification process throughout Canada.

To earn the Certified Management Accountant designation in Ontario, for example, a prospective candidate must meet CMA Ontario's General Admission Requirements and complete the five basic steps of the CMA Accreditation Program which include: earning a degree from a recognized university or recognized college, completing the CMA Required Topics which are specific accounting and management studies at the university level, pass the national CMA Entrance Examination unless granted a waiver by CMA, complete the two-year CMA Strategic Leadership Program (including the CMA Case Examination and CMA Board Report) and simultaneously complete 24 months of qualifying practical experience.

There are also alternative paths to earning the CMA designation based on the prospective candidate's education and work experience.

The requirements to become a Certified General Accountant in Canada are somewhat different. The candidate can enter into the CGA program without a degree or a degree in a discipline outside of accounting. The candidate must successfully complete 4 levels of CGA courses before being eligible for the two-year PACE certification program. Up to 36 months of supervised work experience in increasingly senior responsibility is also required for certification.

6. Constraints

Accounting independence rules require that auditors avoid conflicts of interest. This is generally the case with the profession around the world and recent cases are emphasizing that accountants are becoming more involved in situations where their independence could be impaired.

7. Description of sector associations

Our research has identified the following Canadian accounting related associations:

- *Chartered Professional Accountants Canada* – A national organization established to support unification of the Canadian accounting profession under the Chartered Professional Accountant (CPA) designation. CPA Canada provides services to all CPA, CA, CMA and CGA accounting bodies that have unified or are committed to unification.
- *The Canadian Institute of Chartered Accountants* represents Canada's CA professionals both nationally and internationally. This organization is now CPA Canada.
- *Certified General Accountants Association* - serves CGAs and students in Canada and nearly 100 countries. CGA-Canada establishes the designation's certification requirements and professional standards, offers professional development, conducts research and advocacy, and represents CGAs nationally and internationally.
- *CMA Canada* - grants a professional designation in management accounting and regulates its members under the authorization of provincial legislation. CMA Canada, a self-regulating body, maintains the highest standards, practices and professional conduct in management accounting to protect the public interest. CMA Canada's partnership structure consists of the CMA provincial, territorial and national jurisdictions working together.
- *Society of Professional Accountants of Canada* - is a professional organization established for the on-going education and setting of qualifying standards to ensure professional competence of its members in the practice of accountancy. "The Society has members across Canada and internationally with proven capability in their chosen profession. The Society proudly exudes the singular distinction of being the premier professional accounting organization in Canada offering a unique perspective with a special emphasis on small business."
- *Guild of Industrial, Commercial and Institutional Accountants of Canada* – an association of business accountants, financial managers, tax preparers and accounting executives with members in every province of Canada. It promotes and supports interest in vocational accountancy; encourages acceptance of modern methods and procedures and gives recognition to the individual's skills and practical experience.
- *Provincial institutes and bodies:* for example in Ontario there is the Institute of Chartered Accountants in Ontario, now CPA Ontario, there is CMA Ontario and also CGA Ontario. There is a similar structure across all of the other provinces and territories. For further example, each of the 10 provincial chartered accountants' (now CPAs) institutes/ordres has the responsibility and authority to admit members and student members, and to determine practice requirements and the discipline of members and students.

8. Emerging business trends

- Increasing focus by regulators and the authorities on issues of independence and conflicts of interest.
- Discussion and debate internationally as to the extent to which accountants may legitimately advise clients on tax planning.
- Some of the larger firms in the US and Canada are beginning to open offices in overseas locations (e.g. India) and this office is owned and managed by the US or Canadian partnership.
- Audits of foreign companies which are publicly traded in Canada and the audits of foreign branches of Canadian clients have come under significant scrutiny after a number of large frauds and issues with access to information in foreign locations.
- In the UK, accountants are lobbying for limited form of privilege especially regarding the provision of tax services. Canadian accountants are monitoring this closely.
- The profession is undergoing a unification process and is setting new national standards.

Appendix A contains a number of examples of these different trends.

9. Products and services offered

Accountants provide a broad range of financial, management accounting and advisory services, ranging from the audit, tax and general financial advisory services provided by the public accounting firms to specialist/boutique tax, valuation, forensics and general consulting services firms. As well, individual accountants provide services within industry; often the most senior finance positions, as well as staff in the finance and accounting departments, within private, public and public sector organizations, are certified accountants.

Many certified accountants across the profession are involved in non-profit, charitable organizations as members on volunteer boards; e.g. most non-profit, charitable, public sector organizations have a volunteer accountant involved in some way if not as a member of the board.

The table below provides a breakdown of available data of the three main service areas of the public accounting firm:

Table 9-1 - Canadian accountancy market services: C$B, 2012

Service	2012 C$B	%
Audit	5.2	43.7%
Advisory	3.6	30.3%
Tax	3.1	26.0%
Total	11.9	100%

Source: Accountancy in Canada – August 2013 – MarketLine Industry Profile

Generally, the public accounting firms provide the following types of services in each of the three areas:

1. *Audit:* includes financial statement audits of public and private companies, non-profit and charitable organizations, government and related; also includes reviews (lesser level of assurance provided than audit) and accounting services.

2. *Advisory:* includes valuation services, internal controls and business risk services, corporate finance and valuation services, bankruptcy and reorganization services, forensic and investigations. Many of the larger firms have practices which provide corporate finance services to the market and accordingly require registration with provincial securities regulators.

3. *Tax:* includes notice to reader financial statement tax preparation, compilation of annual tax filings, complex tax planning and structuring services, for both Canada and other jurisdictions. Many Canadian firms have US and International tax practitioners providing services in the larger centres. Commodity tax services, scientific research and experimental development tax claim services, expatriate tax planning and filings.

The range of advisory services offered by accounting firms is becoming broader, many general business consulting services e.g. retail operations, IT security and systems, industry specializations, productivity improvements and others are now offered. The nature of these services, although within the broad business area, is moving further away from the core training and competency of accountants, increasing the likelihood of possible conflicts. This is emphasized by recent media articles including: "Advisory revenue (excluding tax) at Deloitte LLP, Ernst & Young LLP, PricewaterhouseCoopers LLP and KPMG LLP last year surged to $36 billion for their global networks, a rate four times the 3.4 percent gain in audit fees, according to Monadnock Research LLC in Gloucester, Mass. KPMG's audit revenue, the smallest of the Big Four, actually fell."[9]

The larger firms generally are not involved with clients to provide financial intermediary services (PCMLTFA "regulated activity"). Smaller accounting firms generally focus on audit and accounting services, with most no longer involved in public company or larger audits, as well as the tax services and are understood to more likely be involved in financial intermediary type services on behalf of clients.

Services provided by accountants that are potentially useful to a money launderer:

- *Financial and tax advice* – Accountants regularly provide these types of services in the market. Criminals with a large amount of money to invest may pose as individuals hoping to minimize tax liabilities or desiring to place assets out of reach in order to avoid future liabilities. The request for these services is not itself any kind of red flag, you would only get at this by understanding the background of the individuals involved, the source of funds, business activities.
- *Creation of corporate vehicles or other complex legal arrangements (trusts, for example)* – such structures may serve to confuse or disguise the links between the proceeds of a crime and the perpetrator. Also provision of advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seal or other complex group structures). Accountants, especially experienced tax professionals, are often asked to advise on these types of situations. Usually and most often the client is involved with legal counsel and the accountant may be hired by the law firm or the client directly.
- *Performing financial transactions* – Sometimes accountants may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.) These are not understood to be typical services provided by accountants, but research indicates that they do happen; tends to be the smaller firms, independent accountants (though not always). There is risk when the accountant has a relationship beyond being the independent financial advisor.
- *Gaining introductions to financial institutions-* accountants could be and are called upon to make these kinds of introductions; this is general business networking and referrals and happens often. A mitigating factor is

[9] Crain's Chicago Business, THE BIG FOUR'S NEW MATH; A decade after Sarbanes-Oxley forced them to scale back consulting work, accounting giants are beefing up the business of dishing out advice, October 7, 2013. Copy included at Appendix B.

that most professional accountants would value the relationship with the banker as much as the relationship with the client.

- *Buying or selling of property* – Accountants could be involved to assist property transfers between parties, whether this is the provision of financial advisory services to the parties involved, presentation of the relationship with the accountant to the other parties involved, provision of valuation and tax services regarding the details of the transaction etc.

10. Type of customer(s)

The Canadian accounting industry is significantly focussed on business clients. Although they also serve a significant number of individual clients, these are by the nature of the services offered, higher net worth and business owners who need tax advice or assistance with more complex issues that their positions involve.

The majority of clients in the sector are Canadian residents although there are certainly elements of the accounting business where overseas clients are common. The scope of the countries from where such offshore clients originate is very broad indeed and limited only by the scope of Canadian business activity and immigration trends.

11. Geographic considerations

The accounting firms have offices located in major centres across the country, with regional and smaller firms generally located in the larger as well as smaller centres.

The larger accounting firms either are part of an international network of firms under the same brand name or, for the smaller larger firms, part of an international affiliated network. These networks serve to assist each firm to support one another in the provision of services to multi-jurisdictional clients and enjoy cross referrals.

There are no jurisdictional rules (as for example there are in the securities sector) about which jurisdictions an accountant can work in or not when the accountant provides services to the private sector except in the case of auditing. Auditors must obtain a public accounting license and be licensed to provide audits in the respective jurisdiction. In Canada, an accountant obtains their designation and a public accounting license from a provincial body and is then licensed to provide services. There are no jurisdiction rules for services other than audit. The market manages this by demanding that the experience and expertise of the professional accountant be relevant for the local market. So for example, Canadian accountants with Canadian US tax filings experience would not easily be able to provide services in the US regarding US tax filings. In other cases, it is less the jurisdiction and more the specialized industry expertise that the market demands, so a Canadian accountant with significant financial services industry expertise may provide services to financial services all over the world in regards to their transaction processing systems for example.

As well, as has been noted, one of the emerging trends is that some of the larger firms in the US and Canada are beginning to open offices in overseas locations (e.g. India) and this office is owned and managed by the US or Canadian partnership.

12. Any other relevant information on the sector

As indicated, unification of the accounting bodies over the last few years is significant, relevant information on the sector within Canada. The unification initiative was started in 2011 and undertaken by the three main Canadian accounting bodies to work towards merging the relatively fragmented Canadian accounting profession. The ultimate aim is to ensure that the accounting profession becomes "the pre-eminent, internationally recognized Canadian accounting designation and business credential that best protects and serves the public interest."[10]

Unification of the accounting profession took place in May 2012 in Quebec. On February 3 2013 it was announced that the Certified Management Accountants of Ontario, the Certified General Accountants of Ontario, and the Chartered Professional Accountants of Ontario (The Institute of Chartered Accountants of Ontario) signed a Memorandum of Understanding in support of unification of the accounting profession in Ontario. As of October 9, 2013, CGA-Canada entered into an Integration Agreement with CPA Canada.

Recent regulatory and litigation cases involving accountants, further details provided at Appendix B:

- In December 2013, the Dutch authorities fined KPMG €7 million for failing to provide reasonable assurance that the books and records of their client accurately reflected reality. In a settlement, three KPMG accountants were alleged to have helped their client disguise suspicious payments to foreign agents and knowingly failed to verify the payments.
- The SEC has ruled that the Chinese affiliates for all the Big Four accounting firms had "wilfully" failed to provide the audit work papers of certain Chinese companies under investigation for accounting fraud to US regulators. The Chinese arms of KPMG, Deloitte, PwC and EY now face a six-month ban on practicing in the US, January 2014.
- New York State fined Deloitte $10 million for services provided to Standard Chartered Bank regarding anti-money laundering compliance program review work. Standard Chartered was fined US$667 million for allowing hundreds of billions of dollars to be laundered through its US branch by clients from Iran, Burma, Libya and Sudan, in violation of US sanctions on the countries. Deloitte's financial advisory services arm was also banned for one year from taking on new work in the state, June 2013.
- PwC was fined £1.4 million by the Accountancy & Actuarial Discipline Board in the UK for failures concerning reports on client-money accounts at JPMorgan Chase & Co, January 2012.
- KPMG was fined $8.2 million in the US by the SEC to settle allegations of independence violations. Accounting independence rules require that auditors avoid conflicts of interest that could compromise their ability to audit a company's financial statement impartially and rigorously. According to the SEC, KPMG provided non-audit services to affiliates of two of its audit clients. KPMG also hired a recently retired senior-level tax counsel of a third audit client's affiliate only to loan him back to the affiliate to do

[10] http://unification.cpacanada.ca/a-framework-for-uniting-the-canadian-accounting-profession/

the same work. In addition, KPMG employees owned stock in one of the clients and in affiliates of another; January 2014.

- Deloitte was found to have disregarded professional standards when arranging two deals for the Rover employees known as the Phoenix Four. The British carmaker collapsed in 2005 with debts of £1.4 billion and the loss of 6,000 jobs. Deloitte was given a severe reprimand and fined £14 million. Deloitte is planning to appeal the fine imposed by the Financial Reporting Council in the UK, September 2013.
- Deloitte was fined $2 million by the PCAOB to settle civil charges that it violated federal audit rules during the 2003 audit of the financial statements for a unit of Navistar International Corp., August 2012.

13. Key points from interviews

13.1 Sector background

1. Nature of services provided: Audit and valuation and tax compliance, these are the more "traditional", less risk associated, more core services provided by firms. Other services provided include wealth management (offered by some but not all accountants), more complex tax planning, trust account services (some firms will say that they won't provide trust account services in Canada, but they do provide through international affiliates in Cypress for example) and a range of advisory services.

2. Public Accounting: Accountants doing public accounting work (usually the core services as described above) are subject to their firm's rules and to institute inspections. Independents and smaller firms have to have another firm review, a quality monitoring process and the institute inspects this.

3. Accountants in business (e.g. not public accounting), these are usually professionals working inside organizations (public, private, government, not-for profit and charities). There are difficulties, these individuals usually do not have the same provision of services mentality, they are surrounded by others who are not professional accountants, and they don't have the same ethics, professional and quality monitoring structures.

4. Accountants are a self-regulating profession; it has always been this way in Canada. In some other jurisdictions the regulators set the rules for accountants. For CPAs, there are provincial bodies that have responsibility for ethics. This is believed to be the same for CGA's and CMA's.

5. Acceptance of candidates for the profession: Does the profession look at the background of the individual who is applying to go through the process to obtain their professional designation? No, not for the CPA designation. Provincial institutes can however take away the designation if the individual does not follow the rules, but this is based on activity once designation obtained not any prior history. Could not recall there ever being an issue with an individual obtaining the designation and then finding out afterwards that they had criminal history. The process for professional designation is significant and therefore a barrier to entry for anyone not legitimately pursuing.

6. Members of the profession must report to their provincial Institute after having been, in any jurisdiction, convicted of an offence of fraud, theft, forgery, money laundering (and the list continues).

7. The profession regulates itself through the provincial institutes which advocate & regulate across the country. Is not aware that any other industries or sectors are allowed to do this. CPAs are allowed because of the high quality of services provided to the market.

8. CPAs must and need to act in the public interest. Regarding the more recent moves to merge and consolidate the profession, with the CGA's and CMAs it was seen as better to bring them in with the CPAs and regulate to a consistently higher standard, rather than to let them regulate and self-discipline. This has been allowed by governments because of the quality provided by the profession in the past/to date.

9. The self-regulation and discipline processes maintained by the CPAs is graded an 'A'. CGAs are seen to have a weak process, a 'C' grade. Note that only CPAs (as CAs) and CGAs had public licenses to give opinions. The CMAs never had public licenses; their process is seen as weak, a 'C+' grade. CMA process is really focused on situations where a member might have had a bad association with client. The job now is to bring everyone up to the A standard/grade and this will happen through the inspection processes. There will be a mid-tier certificate coming as part of this process. View is that it will not take too long for this to be done, moving from 'C' to 'A' grade.

10. The profession does have a hotline/ whistle-blower line. The public will complain if they lose money etc. The hotline is used, there are active complaints and also newspapers/the media is the flag for the profession as to what situations need to be investigated.

11. Does the profession have a strong enough investigation process? Once all the groups (the CPA, CGA and CMAs) come together, the profession will be double the size of what the CA (now the CPA) used to be. Investigation is executed provincially, it requires co-ordination amongst complaints, conduct and discipline committees.

12. When firms undertake mergers there is massive amounts of due diligence done on the principals and there is due diligence done on key clients as well. In this professional services sector, reputation is everything and so this risk is actively managed.

13. It does happen however, that partners and accountants cross the line, and get involved in unethical or illegal/fraudulent activity. How do 'good' partners get trapped in bad situations? It happens. Firms need to ensure that the culture of the firm supports the professional to come forward, that there is professional support and that this is clearly the tone from the top. "Need to make it safe to come out".

14. CPA supports the implementation of international standards. The International Ethics Standards Board for Accountants (IESBA) – CPA is a member and then uses influence to get each of the provinces to adopt these rules consistently.

15. An exposure draft has been put out by the IESBA on illegal acts (exposure draft is in essence a discussion paper on new standards for the profession). If an illegal act is discovered, who does this need to be reported to? The profession internationally is having three roundtables/ discussions (including in the US and Europe, and Canadian representatives will attend the discussions) on this topic. Currently in Canada there is no reporting requirement and situations are usually governed by client confidentiality rules.

16. The CPA profession currently has no requirement for ethics training, just simply that all professionals are required to follow the rules of professional conduct. This is understood to be the same for CMA and CGA. Note that for the smaller segment of accountants who practice as forensic and investigative accountants and who also carry designations such as CFE and/or CFI, they are required to annually complete ethics training. Some firms have ethics training in place though; this is part of managing and protecting against reputational risks. Accounting professionals are required to have on-going training in their area of expertise on an annual basis.

17. Independence for example, this is a significant requirement for the profession, for certain services, the accountant/auditor must be independent from their client, and this is a part of ethics, an execution of objectivity. This has lately garnered much attention.

18. Independence: the rules of professional conduct which are harmonized across the provinces, supposed to be identical and are close (most provinces have council interpretations, maybe a few don't) say that you cannot take on an engagement which is contrary to a client(can't act for two parties in a dispute with each other for example). How is this applied, does this apply to current relationships? Relationships over the past client 6 months? Over up to 5 years ago?

19. Individual partners complying with rules? How about individual partners who are 'playing on edge', what does a firm do? For example, an auditor must be independent of their client. If a client file is taken on but there is significant question as to whether or not the client can pay, the auditor loses independence. Should the file be taken on? Will the file be taken on? Ethics of the firm and the individual come into play. Some would take on the file even if there were risks/warnings/issues that could impair independence; others would not.

20. Do firms have international bank accounts? Yes, firms in North America have international accounts. See notes below re outsourced and offshore activity trends.

13.2 Professional Standards

21. There are no 'rules' around client acceptance in the profession other than (for CPAs) that we must maintain the good reputation of the profession, don't associate with anyone of 'poor character', can't be associated with false or misleading activity etc. These are principals based rules, which have served the profession well. But one can understand that in a competitive market, with many different sizes of firms, as well as independents, that there is a spectrum as to how the rules of professional conduct are adhered to. The profession has a professional conduct committee and disciplinary committee.

22. How strong is the public accounting client acceptance process? There are no specific rules. It really depends to what extent the facts are known, really comes down to judgment/business decision.

23. What does the profession actually require / what are the rules of professional conduct? CPAs are required to not associate themselves with someone of "poor character". Members of the profession must 'conduct themselves at all times in a manner which will maintain the good reputation of the profession and its ability to serve the public interest', 'maintain the profession's reputation for competence and integrity'; 'professional duty prohibits a member or firm from being associated with financial statements or other information, whether written or oral, which the member or firms knows, or should know, to be false or misleading'.

24. There is a whole spectrum of how this is executed. Generally, standards are quite high and this is due to the desire of the profession's members to maintain highly regarded reputation. Public accounting firms require background checks for public companies and at least a google search for private companies. What is public though? What if a private company is registered with say the OSC, is that public?

25. Quality control systems: 10 years ago the focus was on the Quality Control system framework for assurance (audits and reviews) engagements –this system does make sense for all public practice service (not just audits); quality control includes client acceptance, human resources practice, independence, file reviews, ethics, quality monitoring etc. So many firms now are in process (varying degrees of completion) of applying quality control system to other areas (other than audit) of the practice (tax and advisory type

services). Larger, national firms have internal inspection processes and if they are part of an international network they have further inspections done through this network.

26. Quality control standards focus is really is on the provision of audit services and this in large part is due to legal liability of the profession in regards to audit opinions. Since the Castor case, audit & accounting standards are more robust; there are quality control systems within the firms and the independent standards say that you can't be an advocate for your client. Also in Canada, this started with 80's financial institution failures; in late 90's, the Asian crisis – needed more global consistency for audit/accounting standards and for ethics.

27. Standards around provision of audit services: mandatory partner rotation is required on public company files only; must assess the threat of longer association for non-public company files; public files must have a concurring partner; private files require a concurring partner but only if assessed as higher risk. Need to look at the dollar amount of fees from a client to see if others should have involved (if fees are ≥ 15% fees of a firm, this is an international rule and if fees are ≥ 50% fees of the partner). Also, staff are required to report up more than they ever have before if they see something they don't think the partner has dealt with properly.

28. At the provincial level there are conduct inquiry committees, usually non-accountants are on the committee, key areas they focus on are: Integrity, objectivity, independence; professional competence and due care; confidentiality; and professional behaviour.

29. Litigation matters against/involving accountants keep expanding; this gets fed back into the system and drives inspections and quality.

30. Audit of public company file inspections by CPAB; this results in standards improvements and will get applied across all areas of the practice over time. CPAB is focused on public company audits to make sure that auditors meet standards and that any other services provided do not impair or conflict the auditor.

31. Who monitors the accountants' work with private companies? The provincial institutes monitor this work and they tend to look more at core services vs. other services (e.g. advisory services). They might get to look at other services if these were being provided to an audit client; so, advisory services don't get the same level of oversight.

32. At the international level, the regulators are very involved. Groups like the CSA's, OSC's, CPAB, OSFI, World Bank, IMF all looking over the accountants' shoulders. The International Ethics Standards Board for Accountants (IESBA) has a Canadian member and this person is chosen by the CPA. Each of the committee meetings has a person from an oversight board present and this person helps monitor that all of the accountant members (from around the globe) have contributed in the best interests of the public (no country, firm, or self/profession-bias).

33. There is a committee composed of the Independence Officers of the 'Big 4' firms, Grant Thornton, and BDO. They meet two to three times per year. What do they discuss: independence issues, CPAB – inspections, findings, areas of focus / PCAOB – SEC registrants (more stringent) and conflicts of interest. It is not known if the smaller firms meet or have any similar types of discussions.

34. Recent relevant cases:

- MG Rover Group, recent case in the UK, resulted in a significant fine against Deloitte, Deloitte was found to have not acted in the public interest in regards to provision of corporate finance services.
- KPMG – fined in the US by SEC/PCAOB for $8.2M regarding independence violations, January 2014

35. Nobody within the profession is really looking at/monitoring the provision of tax services. This is done more so by market forces, e.g. CRA and provincial tax authorities assess tax filings and organizations then (if filings are found to be wrong, amounts owed) look to make litigation claims against the accountants who provided the tax services. The Alberta institute is starting to talk about using their inspection process to look at the tax work done on files.

13.3 Trends

36. Globally, firms are exiting the Wealth Management services business section of the market. This is due to the liability risks around being a trustee for a client and also because of potential conflicts. Is there money laundering risk? Not sure, but there is practice risk. Some accounting firms manage the family offices of high net worth individuals.

37. What is gaining traction internationally? Out sourced practices. Some firms are providing the back offices, including flow of funds/bank accounts, to corporations. This has been going on internationally for some time and now smaller/regional firms in Canada for sure are getting into this.

38. Both Canadian & US accounting firms have cross border practices, meaning that they have an office of the Canadian or US firm in an offshore location, e.g. work is being done in India. This is separate from the firm in that offshore location by the same name which is part of the same international network. Having an offshore office (versus another firm within the same international network) helps deal with the privacy laws & data security challenges. So, firm X LLP in Canada uses their Indian office to do personal tax returns versus using the firm X LLP in India.

39. There is quite a debate currently on tax avoidance (which used to be widely accepted). Is this unethical today? There is a whole profession built around tax planning.

13.4 Risk areas

40. China is seen as a huge risk, the SEC has banned American firms from doing work there – not enough regulation to support audit. Also jurisdictional risk in other international areas, Russia for example.

41. Smaller firms and independents are seen as more vulnerable, more likely to provide services to groups undertaking illegal/unethical activity as there is no quality monitoring infrastructure, practice structure is less robust, more dependent on the ethics of the specific individuals involved, more inherent risk. The market considers this before loaning money; e.g. banks look at the quality of the firm signing the audit opinion. They often require a larger, national firm when they assess any kind of risk.

43. Usually the larger, national firms are not involved in the PCMLTFA 'regulated activities' on behalf of clients. Independents and smaller firms are understood to more commonly be providing these services to clients.

44. Is it possible that the larger firms have inherent risk as they are approached more by groups desirous of the credibility the larger firm provides to illegal activity? Possible, not known.

45. Larger firms have the risk that an individual partner or staff provides services to the market without others knowing, without the firm monitoring systems identifying. How do firms monitor for this? Have to get at what are people doing, how are they spending their time. Very difficult to monitor these things with regards to professionals and sometimes can only monitor after the fact by looking at e-mails, monitoring phone calls from clients etc.

46. Clients/services referred to international affiliates in offshore centres.

47. When accounting firms and accountants provide complex tax planning and tax structuring services, wealth management and corporate finance services.

48. As financial experts, accountants can be sought after by those desiring to launder funds; and because money laundering is a financial process, accountants can be involved in the process both wittingly and unwittingly. Some of the key areas that we want to guard against are:

49. Providing assurance or other services where we would be used to provide some legitimacy to operations which are, or are attempting to, launder funds;

50. Providing accounting, consulting, tax services or assistance to set up complex corporate organizations and structures (e.g., shell companies) which could assist individuals who are seeking to launder funds or conduct terrorist financing activities; and

51. The use of our services in any way to assist the payment or transfer of funds between parties when this is not related to legitimate commercial transactions.

52. Our firm generally and specifically prohibits activities which involve the handling of client monies on their behalf. This prohibition applies to all clients in all of our service lines regardless of the type of expense or remittance. Any attempt to extend these types of courtesies to our clients is not worth the substantial financial and legal risk to the firm. The firm has covenants to various third parties (bankers, insurers, etc.) by which such transactions are in breach of contractual terms and conditions.

53. Our firm, we expect like most of the larger and regional firms, focuses more broadly on the risks for accountants. The most relevant, when considering money laundering and these types of risks for illegal activity, is to make sure we know well the individuals we are dealing with. The client acceptance process is pretty important. We do not want to be involved with providing or being seen to provide services to individuals involved with money laundering or terrorist financing activity.

54. Some of the areas, functions that could be performed by accountants that are most useful to a potential launderer:

55. Financial and tax advice – Accountants regularly provide these types of services in the market. Criminals with a large amount of money to invest may pose as individuals hoping to minimize tax liabilities or desiring to place assets out of reach in order to avoid future liabilities. The request for these services is not itself any kind of red flag, you would only get at this by understanding the background of the individuals involved, the source of funds, business activities.

56. Creation of corporate vehicles or other complex legal arrangements (trusts, for example) – such structures may serve to confuse or disguise the links between the proceeds of a crime and the perpetrator. Accountants, especially experienced tax professionals, are often asked to advise these types of situations… usually and most often the client is involved with legal counsel and the accountant may be hired by the law firm or the client directly.

57. Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seal or other complex group structures). Same as above.

58. Performing financial transactions – Sometimes accountants may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.) I have seen this occur on investigations I have worked on. We don't allow this activity in our firm, need to manage and monitor through culture and awareness of the firm. It certainly happens, tends to be the smaller firms, independent accountants (though not always), there is risk when the accountant has a relationship beyond independent financial advisor.

59. Gaining introductions to financial institutions- accountants could be and are called upon to make these introductions. A mitigating factor is that most professional accountants would value the relationship with the banker as much as the relationship with the client.

13.5 Discussion with senior tax accountant professional

60. New immigrants/Canadians – tend to keep assets offshore – currently, the system is based on self-assessment so therefore is a weakness. Not necessarily proceeds of crime but do not want government involved. There is reliance of bank privacy laws to not disclose information.

61. There is offshore planning to protect assets with assets held in foreign trusts. Have also heard of instances where use of offshore entities in order to repatriate assets back into Canada.

62. For tax professionals – would provide legitimate tax advice but there is better understanding in system of tax professionals' role. Would advise client if tax treatment is overly aggressive. However, some clients would opinion shop amongst several accountants to find right accountant that will help with setting up structure.

63. One example of structure would be to create residency (or cancel citizenship, as in the US) – however, clients would utilize both domestic and foreign tax professionals, especially if involved in foreign jurisdiction.

64. Areas seen to be higher risk for accounts include offshore gambling as uncertain about controls and abuse of native reserves to take advantage of preferential tax treatment.

65. Canadians are sometimes seeking services from lawyers in conjunction with accountants to get/maintain privilege. In the UK, accountants are lobbying for limited form of privilege so Canada monitoring this closely.

66. In Canada, lawyers within accounting firm cannot offer privilege. Lawyers are bound by ethical rules and reputation risk to not assist clients with potentially illicit activity.

14. Risk factors

14.1 Products and services

14.1.1 Nature of services

Accountants, through the various services they provide and their areas of financial expertise are sought after by those desiring to launder funds. Because money laundering is a financial process, accountants can be involved in the process both wittingly and unwittingly. Interviewees shared that higher risk areas included complex tax planning and tax structuring services, wealth management and corporate finance services.

14.2 Delivery channels

14.2.1 Accountants who provide services outside of their areas of expertise

This is potentially an indicator that the accountant, client relationship is not service driven, e.g. the accountant is less or not independent and the client obtains value in another way.

14.2.2 Size of firm/independent accountants

Smaller firms and independents are seen as more vulnerable, more likely to provide services to groups undertaking illegal/unethical activity as there is often limited quality monitoring infrastructure; the practice structure is dependent on the ethics of the specific individuals involved, and thus there is more inherent risk. Interviewees reported that the market considers this before loaning money; e.g. banks look at the quality of the firm signing the audit opinion. They often require a larger, national firm when they assess there is more risk around the potential debtor.

Client acceptance processes are where these larger firm resources really come into play, e.g. to really understand the backgrounds of the persons involved with new client relationships.

Usually the larger, national firms are not involved in the PCMLTFA 'regulated activities' on behalf of clients. Independents and smaller firms are understood to more commonly be providing these financial intermediary services to clients.

14.2.3 See provision of services under legal privilege (below)

14.3 Geography

14.3.1 Referrals to offshore affiliates located in higher risk jurisdictions

Research indicates that sometimes, when accountants are unable to provide services locally, they may refer the client to offshore affiliates where the provision of services receives less scrutiny.

14.3.2 Clients located in high risk international locations

Research indicates that countries such as China and Russian are significant risk areas for public accounting firms. The SEC has banned American firms from doing work there and Canadian firms communicated that they are very aware of the risks.

14.4 Business relationships/linkages with other sectors

14.4.1 Conflict of interest issues

As accountants, and particularly larger accounting firms, grow and expand the breadth of their services there exists more opportunity for conflicts of interest, impacting the independence of the accountant from the underlying client. Recent cases and examples are included at Appendix B and they highlight how seriously regulators are treating these issues.

14.4.2 Accounting services provided under legal privilege (lawyers)

When accountants provide financial advisory services to businesses under legal privilege there is significant risk. This is true except in the case of litigation/dispute resolution wherein it is quite common for expert accounting services to be engaged to assist a dispute resolution process between parties (e.g. parties are in dispute over the valuation of a business and each side hire their own valuator). Legal privilege provides a protection, makes the underlying financial or business data less transparent, and could mean that the parties are seeking a degree of confidentiality beyond business norms which is not easily understood. Interviewees suggested that they were aware of instances when tax planning services were provided this way.

14.4.3 Higher risk real estate transactions

Accountants who provide financial services to clients around higher risk real estate transactions have opportunity to understand the client and the source and use of the funds.

14.4.4 Clients who opinion shop

Interviewees shared that some clients will opinion shop amongst several accountants to find an accountant to help set up the structure they desire, e.g. tax planning.

14.4.5 When engaged to perform work through third parties

Other than when engaged by external legal counsel (discussed above), when accountants are engaged by parties other than the ultimate subject or beneficiary of the work, there is higher risk. This is primarily because the accountant does not deal directly with the underlying party(s).

Potential indicators of this include:

- Does not understand the nature of the work requested, is not familiar with standard terms and requirements, or does not have a place of business.
- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
- Has significant and unexplained geographic distance from the parties involved.
- Is associated with questionable business practices.
- Involves third parties in transactions without apparent legitimate business purpose.
- Will not identify beneficial owners or controlling interests, where this would be commercially expected.
- Seeks anonymity by conducting ordinary business through other accountants, lawyers, or other intermediaries.
- Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
- Is a politically exposed foreign person (PEFP).

14.5 Client type and characteristics

14.5.1 Client characteristics

Given the nature of accounting services, it is believed that there is less relevance to trying to identify transaction type and method factors and more relevance in the identification of client type and characteristic factors. While many of these factors are relevant to all sectors, they have particular relevance for the accounting and legal profession due to the nature of services provided:

- Unsolicited business and not requesting a vendor competitive process
- Beneficial ownership/directors unclear
- Position of intermediaries is unclear
- Company activities are unclear and/or no apparent business reason for transactions/business activity
- Inexplicable changes in ownership
- Legal structure of client has been altered numerous times
- Management appear to be acting on instruction
- Customer's business, source of revenue is not clear
- Known criminal/questionable reputation
- Third-party involvement with obscure details
- Politically exposed foreign persons (and association)
- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
- Has significant and unexplained geographic distance from operations that are not reasonable.
- Changes consultants, accountants frequently or engages a number of consultants, accountants, lawyers at the same time.

- Has a complex business structure, multiple shell companies
- Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose.
- Will not identify beneficial owners or controlling interests
- Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries.
- Client is involved in online gaming or business activities which are illegal in some jurisdictions
- Reason for choosing firm is unclear, given the firm's size, location or specialization
- Sudden activity from a previously dormant client
- Client starts or develops an enterprise with unexpected profit or early positive results.
- Client does not wish to obtain necessary governmental approvals/filings, etc.
- Client offers to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures).
- Transactions being done on behalf of a third party
- Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
- Investment in real estate at a higher/lower price than expected
- Large international payments with no business rationale
- Misuse of introductory services, e.g. to financial institution
- Client paying unusual consultant fees to offshore companies
- Company shareholder loans are not consistent with business activity
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business
- Over and under invoicing of goods/services
- Multiple invoicing of the same goods/services
- Falsely described goods/services
- Over and under shipments (e.g. false entries on bills of lading)
- Multiple trading of goods/services
- Misuse of pooled client accounts or safe custody of client money or assets
- Client reluctant to provide all information or accountant has reasonable grounds to believe that the information provided is correct or sufficient
- Client uncertain about location of company records
- Client records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Client carries non-existent or satisfied debt that is continually shown as current on financial statements.
- The client operates in an industry, sector, category where opportunities for ML or TF are particularly prevalent.
- Lack of face-to-face contact or subsequent lack of contact, when this would normally be expected.
- Employee numbers or structure out of keeping with size or nature of the business
- Client living beyond their means

- Company acquires large personal or consumer assets (i.e. boats, luxury automobiles, personal residences or cottages) when this type of transactions is inconsistent with the ordinary business practice of the client or industry.

Grant Thornton

Reporting Entity Sector Profile: Life insurance

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

The Canadian life insurance sector is significant in Canada, with over $320 billion in life insurance premiums for approximately 21 million Canadians. In total, Canadians own approximately $3,900 billion in insurance.[1]

There are approximately 90 active life insurance companies, with the largest three controlling about 75% of the market.[2] These three conglomerates – Great-West Lifeco Inc., Manulife Financial Corp. and Sun Life Financial Inc. – are considered amongst the largest life and health insurance companies in the world with significant operations internationally in the US, Europe and Asia in over 20 countries.

The remaining companies are smaller and service niche markets or are subsidiaries of international conglomerates.

The composition of the life insurance industry is as follows:

- Life insurance companies which hold individual policies for clients;
- Reinsurance companies, which sell insurance to life insurance companies;
- Managing General Agents (MGAs), which are provided contracts from life insurance companies; and
- Insurance agents/brokers which sell insurance contracts to individual clients.

The insurance industry is heavily regulated. Insurance and reinsurance companies are federally regulated and supervised by the Office of the Superintendent of Financial Institutions ("OSFI"), with the exception of Quebec, and insurance agents and brokers are regulated by provincial and self-regulatory organizations ("SRO"), depending on the province.

In Canada, only companies that sell life insurance are required to meet AML regulations whereas property and casualty (P&C) insurance companies do not have to. The P&C insurance sector is fragmented, consisting of a number of co-operative organizations, subsidiaries of life insurance companies and Canadian banks.

Some evidence of the use of life insurance products for money laundering has been identified in Canada. A number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Fragmented regulation of brokers
- Market competitiveness at agent level/commission based compensation
- Life insurance products with single premium payments and/or high cash values upon surrender
- Premium payments by third parties
- Surrendering of large value policies early
- Use of offshore policies and professional advisors

[1] Canadian Life and Health Insurance Association – Key Statistics (data for 2012)
[2] Ibid

2. Structure, size and segmentation, reporting entity population

Segmentation of the sector is as follows:

2.1 Life insurance companies

With a maturing industry, the life and health insurance companies have consolidated from 290 companies in 2008 to 264 at the end of 2012. In 2012, total assets held by life insurance companies totaled almost $615 billion.[3]

Outside of Canada, foreign branches and subsidiaries of Canadian life insurance companies earned premiums of $48 billion, which accounted for 40% of the worldwide total. These same branches and subsidiaries held assets of $597 billion, representing approximately half of the worldwide total.[4]

In February 2014, the International Monetary Fund ("IMF") performed solvency stress tests on the three largest life insurance companies – evaluating based on a projected five year outlook as well as a hypothetical severe financial crisis from outside Canada – the results determined that the companies were strong, well above supervisory targets. Insurance companies that want to reduce their risk will typically reinsure their policies with reinsurance companies.

Premiums from life insurance, account for approximately 30% of total earnings in 2012[5], the remaining 70% of earnings were from pension and annuity investments, which are outside of the life insurance sector.

Smaller insurance companies survive in the market place by being innovative and faster to launch new products, which generally do not require regulatory approval prior to sales.

2.2 Reinsurance companies

Reinsurance companies are insurance companies that sell policies to other insurance companies, allowing them to reduce their risk and protect themselves from very large losses. The reinsurance market is dominated by a few very large companies, with huge reserves. A reinsurer may also be a direct writer of insurance risks as well.

3 International Monetary Fund (IMF) – Canada: Report on the Observance of Standards and Codes, February 2014
4 Source
5 MarketLine Industry Profile – Life Insurance in Canada, January 2014

2.3 Managing General Agents (MGAs) or Associate General Agents (AGAs)

Managing General Agents have contracts with one or more insurance companies and act as the middlemen, managing the administration process of deploying agents that sell insurance. There are no specific financial regulations regarding MGAs and there are no clear regulations as to who is responsible for the independent agent.

Associate General Agents are similar to MGA's but unable to obtain an MGA contract due to low volume and therefore, an independent agent may work for an AGA that is used by an MGA.

2.4 Insurance Agents and Brokers

There are approximately 154,000 insurance agents and 45,000 brokers serving the insurance industry.[6] Insurance agents are generally divided between independent and career agents.

2.4.1 Independent Agents

Independent agents work with one or more insurers, selling life insurance. While the specific numbers are not available, it is believed that a large number of independent agents work with one or more MGAs.

2.4.2 Career Agents

Career agents work exclusively for one insurance company, which is responsible for their training, monitoring and mentoring. While use of career agents was initially popular for insurance companies, using independent agents is now preferred by the insurer as there are less expenditures, and for the consumer, it precludes the need to shop around with multiple insurance companies.

6 IMF Report – data as at the end of 2012,

3. Economic and Financial Statistics

In Canada, there are a total of 77 OSFI regulated life insurance companies; 42 are Canadian and the remaining 35 are foreign. Statistics Canada provides some high level information on the major segments.[7] The Statistics Canada breakdown of the major segments is as follows:

- Direct Life, Health and Medical Insurance Carriers: 727
- Direct Individual Life, Health and Medical Insurance Carriers: 558
- Insurance Agencies and Brokerages: 12,994
- Direct Group Life, Health and Medical Insurance Carriers: 169

See detailed charts and statistics at Appendix A

The Canadian life insurance industry's net income for 2012 increased 75% over 2011 but reportedly remains volatile. Total net income for federally regulated life insurance companies and branches for 2012 was $7.4 billion, with 73% coming from the three large conglomerates. This compares to 2011 when there was $4.3 billion in net income with 50% coming from the three large conglomerates. The return on equity for the industry was 9.8% in 2012 compared to 5.9% in 2011.[8]

7 OSFI
8 OSFI 2012-2013 Annual Report - http://www.osfi-bsif.gc.ca/eng/docs/ar-ra/1213/eng/print-eng.html

4. Regulation of the Insurance Sector

Insurance is one of the most highly regulated industries in Canada, with the regulations for life insurance divided between the federal, provincial and territorial governments. OSFI supervises the federally incorporated insurers as well as foreign insurers from a safety and soundness perspective, the AMF does the same for companies incorporated in Quebec. The provincial regulators regulate market conduct and the licensing and supervision of insurance intermediaries such as agents, brokers and adjusters. The provincial regulators together comprise an umbrella group called the Canadian Council of Insurance Regulators ("CCIR").

In some provinces, insurance brokers and agents are regulated by the same regulator. In other provinces, for example Ontario, agents are regulated by a government regulator, while brokers are regulated by a self-regulatory organization. In some provinces, all regulation of intermediaries is carried out entirely by self-regulatory organizations with delegated powers.

The insurance regulatory laws of the provinces, other than Québec, are generally uniform and based on common law principles. The laws of Québec are based on the civil code system.[9]

Government of Canada: Insurance Companies Act (S.C. 1991, c. 47) - http://laws-lois.justice.gc.ca/eng/acts/i-11.8/ Each province has passed insurance legislation, e.g.:

- Ontario Registered Insurance Brokers Act - R.S.O. 1990, CHAPTER I.8
- British Columbia - Insurance Act - [RSBC 2012] CHAPTER 1 - Part 3 — Life Insurance
- Newfoundland and Labrador – Life Insurance Act - RSNL1990 CHAPTER L-14 - Chapter L-14 - An Act Respecting Life Insurance
- Nova Scotia Insurance Act – Chapter 231 of the Revised Statutes, 1989
- Quebec – An Act Respecting Insurance – Chapter A-32
- Alberta Insurance Act - O.C. 325/2011

In September 2012, OSFI released a framework document identifying the regulatory initiatives for the life insurance sector up to the year 2016. The document outlined OSFI's priorities to address issues in order for the market to continue serving Canadians. Some of the issues the framework identified included insurance companies' corporate governance and risk management, evolving regulatory capital requirements, and financial transparency.[10]

9 Source: http://www.stikeman.com/en/pdf/insurance_reinsurance_Canada.pdf
10 Source – OSFI Annual Report 2012-2013

5. Educational and licensing requirements

Agents are required to be provincially licensed before being permitted to sell insurance. Licensing generally requires completion of a training program, applying for a provincial license, joining an insurance provider and clearing provincial background checks.

The Life Licensing Qualification Program ("LLQP"), an entry level exam which does not provide a designation, is valid in all provinces and territories except Quebec, which operates under a separate system. Applicants in Quebec must satisfy minimum qualifications and pass an exam operated by the Autorité des Marchés Financiers ("AMF").

In addition to the training and background requirements, applicants must obtain compulsory errors and omissions insurance; a form of professional liability insurance.

6. Constraints

Insurance cannot be bought by an unrelated party; there must be an 'insurable interest'. Insurance companies monitor who makes premium payments to determine if there is an 'insurable interest'.

Appendix 9

7. Description of Sector Associations

Our research has identified the following Canadian life insurance related associations:

Canadian Life and Health Insurance Association (CLHIA) - a voluntary non-profit association with member companies accounting for 99 per cent of Canada's life and health insurance business.

Canadian Council of Insurance Regulators (CCIR) - is an inter-jurisdictional association of insurance regulators. The mandate of the CCIR is to facilitate and promote an efficient and effective insurance regulatory system in Canada to serve the public interest.

Canadian Association Of Independent Life Brokerage Agencies – a voluntary association of independent agencies, including MGA's that lobby government on industry issues and promote uniform standards.

Insurance Bureau of Canada (IBC) - is the national industry association representing Canada's private home, car and business insurers.

Advocis, the Financial Advisors Association of Canada - the largest not-for-profit association of professional financial advisors in Canada. Representing its members' interests with all levels of government, regulators, and industry.

Canadian Insurance Self-Regulatory Organization (CISRO) - is a national organization of licensing and regulatory authorities for insurance intermediaries. Members consist of representatives from British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Newfoundland and Nova Scotia.

Registered Insurance Brokers of Ontario (RIBO) – is the self-regulatory body for insurance brokers in Ontario. Established in October 1981, RIBO regulates the licensing, professional competence, ethical conduct, and insurance related financial obligations of all independent general insurance brokers in the province.

Financial Services Commission of Ontario (FSCO) - is a regulatory agency of the Ministry of Finance that regulates insurance, pension plans, loan and trust companies, credit unions, caisse populaires, mortgage brokering, and co-operative corporations in Ontario. Other provinces have similar bodies.

OmbudService for Life & Health Insurance (OLHI) - is a national independent complaint resolution and information service for consumers of Canadian life and health insurance products and services

Alberta Life Insurance Council – regulatory body which is responsible for licensing and discipline of insurance agents, brokers and adjusters in the Province of Alberta

Alberta Insurance Council - provides investigation and administrative services to the Insurance Adjusters' Council, the General Insurance Council and the Life Insurance Council.

International Association of Insurance Supervisors (IAIS) - the IAIS represents insurance regulators and supervisors of more than 200 jurisdictions in nearly 140 countries. Its objective is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders

Reinsurance Administration Professional Association (RAPA) is the primary educator of the industry on reinsurance administration principles, issues and best practices, the industry's leading voice for the development, implementation and maintenance of life reinsurance data standards, the driving force behind improved data quality, and the place where reinsurance administration professionals establish and maintain important business relationships.

8. Emerging Business Trends

Regulating MGAs – During September 2012, the CCIR published a position paper on the issues identified with respect to the supervision and activities of MGAs as well as recommendations. The Financial Institutions Commission (FICOM) in British Columbia has also issued a draft guideline for using MGAs.

9. Products and Services Offered

There are two main categories of life insurance in Canada: term life and permanent life insurance:

Term Life Insurance: Insurance premiums paid by the client are smoothed out over the expected life of the term and marginally increase every year. Insurance is renewed but usually not past age 70 or 75.

Permanent Life Insurance: Permanent life insurance calculates premiums that remain level over the lifetime of the policy, without increases. Accordingly, premiums at the beginning are used to subsidize the premiums paid in later years, when the risk is higher. Permanent life is comprised of the following subcategories:

Whole life, which has a guaranteed cash surrender value (or cash value) and a 'participating' component on eligible policies;
Term to 100, which is similar to whole life but has no cash surrender value and the policy is covered up to age 100; and
Universal life, which has two components; a fixed insurance component, with a defined death benefit; and an investment component, the value of which fluctuates depending on market performance.

The cash value is the guaranteed amount that is available to the policy holder to be borrowed against the policy or if the policy is cancelled prematurely.

Some policies will also have a participating component and receive 'dividends'. While not guaranteed, the policy holder will benefit when the insurance company estimates there to be a surplus of premium over future expenses.

As noted above, life insurance can be purchased from independent and career agents. In addition to those methods, individuals can also obtain life insurance through their place of work – some employers offer it through group benefits plans (note that this type of insurance usually ends when the individual leaves employment) – or through affinity programs such as clubs, associations or alumni groups.

Insurance through group benefit plans are usually issued without medical examination on a group of people under a master contract. It is usually issued to an employer for the benefit of employees. The individual members hold certificates as evidence of insurance. For employers, or sponsors of a group plan, offering group life insurance as part of the benefits package is sold as a way to attract and retain employees.

Often insurance companies are selling insurance along with other policy products including health components such as critical illness insurance, disability insurance, accident insurance, accidental death and dismemberment insurance.

10. Type of customer(s)

10.1 Business vs. Individual

Generally there is a wide reach and policies are sold to individuals. Most customers are the individual being insured, the spouse or a corporation with an insurable interest.

In Canada group insurance is usually purchased through larger brokerage firms because brokers receive better rates than individual companies or unions. There may be slight differences in terms of administration and market related practices worldwide, even though the concept may be the same. For example, in India, broker procured group term insurance, unlike Canada, does not intrinsically have any price advantage to the buyer i.e. the Master Policy Holder.

10.2 Canadian residents/non-residents

Life insurance policies sold to Canadian residents should only be sold by licenced Canadian agents. It is possible for a Canadian life insurance policy holder to move overseas but a Canadian resident living overseas who wishes to buy from one of the major Canadian firms would have to buy it from one of their local agents who is licensed in that jurisdiction.

10.3 Geographic area

Sales agents are licensed by province and as such, sales agents may only sell in certain provinces only.

11. Geographic considerations

The big three insurance companies are generally established and provide services throughout Canada and across 20 countries around the world.

In Canada, the provinces with the most insurance agencies and brokerages are in Ontario, Quebec, BC and Alberta, and these provinces make up the majority across Canada.

Appendix 9

12. Key points from interviews

12.1 Sector Background

1. The Canadian insurance sector is highly regulated. The big three insurance companies really set the tone for the industry.

2. Insurance companies monitor for payments made by third parties; all premium payments are supposed to be made directly to the insurance company. In limited cases, premium payments are made from the agent but these are investigated and permitted only in exceptional cases. Premium payments by third parties would also be typical when payment is made by spouse – investigators will ask for information where surnames are different – for example, in Quebec, married woman typically retain maiden name and therefore harder to determine relationship, if any.

3. Insurance is sold through insurance company employees as well as agents or indirectly through a managing general agent (MGA), the latter of which are not required to sell life insurance exclusively for any particular company. MGA's will review documentation for completeness before submitting to insurance companies as insurance company will reject if incomplete.

4. Use of MGA's reduce the administration costs of managing own sales agent network.

5. Hiring of insurance agents – agents must be provincially licensed. Licensing requires disclosure of potential suspension in other jurisdictions and falsifying the license application can be an indictable offence and fines levied. However, broker does not have ability to independently check whether an agent has had license revoked (Subsequent to the meeting with interviewee, we noted that in December 2013 the CCIR began publicly disclosing disciplinary actions against agents and firms on their website).

6. Premium payments – the life insurance premium is paid directly to the insurer, whereas premiums for property and casualty (P&C) are paid to broker. Reason for this is in life insurance, the insurer has a direct contract with the insured party. For P&C, the insured party contracts with the insurance broker and the policy is underwritten by an insurance company.

7. Premium payments for life insurance are made directly to the insurance company and usually by cheque or direct withdrawal from bank account.

8. Premium payments for P&C are directed to broker. Most brokerages will have cash limits (the interviewee indicated that their company had $500 cash limit and discouraged money orders as there would also be no money trail.

9. Amounts paid to broker go directly into a formal trust account that is audited by RIBO to ensure sufficiently capitalized and no intermingling of operational funds.

10. For life insurance, there would be instances of clients making front-end lump sum contributions. Cancellation fees within the first 2 years would typically be close to 100% of the premiums (for that

period only). Policy holders would legitimately cash out their insurance policies earlier if they have no beneficiaries. However, early cash outs within the first two years are seen as big money laundering risk.

11. Where there is a front-end, lump sum contribution, insurer deposits funds into a side account (like a trust account) and on regular basis, transfers money out for premium payment.

12. Life and P&C insurance differ in that the latter protects assets and in order to make a claim, there must be damage. In the former, the insurer underwrites the person and so the question is whether the individual's life is worth that much? For example, an insurance company will not insure a low income individual with a policy for $50M even if they were able to make the premiums. There is an assessment that takes place. Also, a central agency collects all the information so that individuals cannot buy multiple, smaller life insurance policies that total are of an unreasonable amount.

13. Insurance companies monitor who makes the premium payment to determine if there is 'insurable interest' – cannot simply buy insurance on unrelated party transaction. Therefore, payments made by spouse, business partner or corporation can be typical.

12.2 AML Compliance

14. Training and knowledge of money laundering in insurance is weak – there is no enforcement if agents/brokers are not trained. For MGA's there is lots of training but it is selective and not necessarily related to money laundering.

12.3 Risk Areas

15. Insurance companies understand the money laundering risks very well as their entire business model relies on understanding of risks. Potentially challenging areas are: front line staff – however, personal reputations are at stake and there are controls built in to process.

16. Insurance agents see potential money laundering activity – for example, where income is inconsistent with luxury assets being insured or heavily mortgaged property with insufficient income – mortgage is from private lenders and the purpose of these transactions is to limit the loss of property if seized by authorities.

17. Underwriters also assign pre-set approval amounts which trigger additional information requirements. For example, a 20 year old with a $2M property – need to understand if first time property owner, for potential loss evaluation purposes. Insurer is also concerned about potential money laundering and source of funds. There are no written rules on unacceptable, risky clients as there is concern about discrimination. Forms only ask required questions (like PEFP).

18. There are currently no mechanisms to report suspected money laundering activity as it relates to property and casualty insurance. Although, agents may be more interested in earning the commission than reporting on a client.

13. Risk Factors

13.1 General Market

13.1.1 Market Competitiveness at Agent Level / Commission Based Compensation

13.1.2 Fragmented Regulation of Brokers

13.1.3 Management of Multiple Reporting Lines

As independent agents are several steps removed from the insurance company, there is no control on the training received by agents. Furthermore, hiring practices and monitoring of initial client activity is difficult to control and monitor.

While insurance companies are responsible for providing training and ensuring compliance with AML regulations for its employees, the same responsibility when using independent agents or MGAs is not as distinguishable, especially when the independent agent acts for multiple MGAs or insurance companies.

As insurance companies increasingly reduce overhead by outsourcing the sales function to independent agents and MGAs, there may be higher risk in ensuring sufficient training and monitoring to identify potential money laundering activity at retail level.

Independent agents can be hired indirectly by an MGA or through another corporate structure, and as such, the insurance industry is exposed to not knowing the background of the independent agent.

13.2 Product and Service

13.2.1 Life insurance products with single premium payments and/or high cash values upon surrender

Whole life and universal life policies will typically provide cash values if the policy is terminated early. Accordingly, funds can be laundered when the account holder receives 'cleaned' funds from an insurance company. Interviewees we spoke to generally indicated that this was a high risk area, however, mitigating this risk is that brokers and insurance companies monitor for this type of activity.

13.2.2 Purchase of life insurance policies on terrorist fighters

Appendix A includes one article that indicates this was being considered.

13.3 Delivery Channel

13.3.1 Use of Independent Agents and Managing General Agents (MGA)

See above.

13.4 Geography

13.4.1 Offshore policies and advisors

Insurance schemes involving offshore policies or service providers. We are aware of a case where $30 million in fraud proceeds from Canadian victims was laundered using a sophisticated international life insurance scheme. The policy was issued in the Caribbean using a complex structure of offshore banks and financial advisors. A major Canadian bank was used for part of the transactions required to set it up. See details at Appendix B.

13.5 Business Relationships / Linkages with Other Sectors

13.5.1 Agents as Gatekeepers

Agents may promote themselves as trusted financial experts, offering wealth management and tax advice in addition to insurance products.

Agents have a relationship with their clients and given the nature of other insurance products sold, policies on high value assets, they may become aware of, or suspicious of, illegally sourced funds or assets. Interviewees informed that there is no mechanism right now for reporting this.

13.6 Transaction Methods and Types

13.6.1 Premium Payments by Third Parties

Premiums are typically expected to be made by the policy holder or where the payment is reasonable, for example, spouse, business partner, company. Insurers monitor for unusual payment activity and will make further inquiries where there is no reasonable explanation. In addition, insurers monitor whether the value of the policy is consistent with the background of the insured party. However, there is a risk that premium payments made by third party may be disguised in the form of a payment from an employer or corporation.

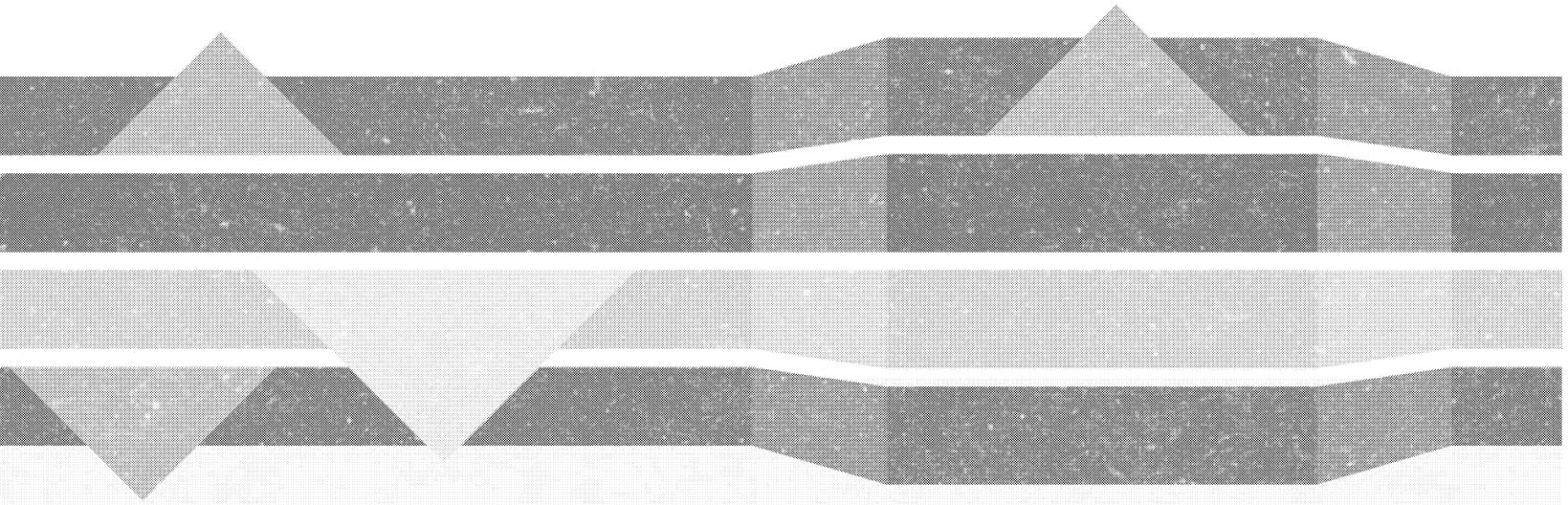
13.6.2 Surrendering of large value policies early

Grant Thornton

Reporting Entity Sector Profile: BC Notaries

Money Laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014



Appendix 9

Contents

1. General sector profile

In British Columbia, a notary public is appointed for life by the Supreme Court of British Columbia after having formally applied for the position, passing an exam and meeting the screening requirements. The Society of Notaries Public of British Columbia (the "Society"), a self-regulatory organization ("SRO"), oversees the profession and sets standards to maintain public confidence in the activities.

The Society receives over 1,600 application inquiries from the public annually; on average 20 to 25 students per year are selected. The Notary is a member of one of the branches of the legal profession and is sanctioned and safeguarded by law. BC Notaries are unique in North America, providing non-contentious legal services to the public.

BC Notaries are governed by the Notaries Act of BC (the "Act") and the discipline regulations of their professional society under the Act.[1]

BC Notaries are commissioned to provide numerous non contentious services, and in some respects the services they offer are similar to the same kinds of work undertaken by lawyers, including, for example the transfer of land, execution of wills, powers of attorney, representation agreements, and advance directives. Their primary work relates to their power to administer oaths which enables them to take affidavits, declarations and acknowledgements, and to attest instruments by seal and to give notarial certificates. Such services are required for many documents and instruments which are intended, permitted or required to be registered, recorded or filed in a registry or other public office, contracts, charter parties and other mercantile instruments in British Columbia.

Under the Notaries Act, the Lieutenant Governor in Council may also appoint other specific types of individuals to be a notary public. This clause includes a general category where the services of a Notary are required, including:

- Permanent employees of the government of British Columbia or Federal employees; or
- Registrar or person performing the functions of registrar, of a university under the Thompson Rivers University Act or the University Act.

Such appointees are not members of the Society and have only limited powers, namely to administer oaths, to take affidavits, declarations and acknowledgements, to attest instruments by seal and to give notarial certificates. Such appointees may also be limited in the geographic area in which they may practise.

[1] BC Notaries website

Notaries may operate their practice either as an individual, or as a notary corporation which means a corporation for which a permit has been issued by the secretary of the Society of Notaries Public of British Columbia. The corporate name must include the word "notary" or "notaries", and all shares of the corporation must be owned by a notary in good standing or their spouse or other specified relative.[2]

Notaries are required to post bonds on entry to the society and are also insured under a group policy.[3]

A number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Provision of financial intermediary type services- research indicated that generally, many notaries had accounting backgrounds and careers. Provision of these services by persons with both legal and accounting expertise is vulnerable to abuse by money launderers; and
- The provision of notary services to real estate transactions exposes this sector to many of the identified risks for the real estate sector.

[2] http://www.notaries.bc.ca/resources/Upload/09-12-2013-09-22-54_Society%20Rules_Revised_July%202013.pdf
[3] http://www.notaries.bc.ca/resources/Upload/28-06-2011-09-54-36_BecomingANotary-062711_ONLINE%20VERSION.pdf

2. Structure, size and segmentation, reporting entity population

There are currently 324 registered notaries in the province of BC.[4]

[4] http://www.notaries.bc.ca/findNotary/notaryRoll.rails

3. Economic and financial statistics

We have not determined any economic data for this very small sector.

4. Regulation of the BC notaries sector

BC Notaries are regulated by their SRO, the Society of Notaries Public of British Columbia. This body mandates training, runs the qualification exam program and conducts disciplinary investigations. These functions are mandated by the governing law, the BC Notaries Act. The disciplinary committee and properly appointed disciplinary tribunals have the authority to award reprimands, fines, suspension and termination. Such disciplinary tribunals are also bound by the terms of the Administrative Tribunals Act.

Notaries, like lawyers, are required to maintain trust accounts to hold and manage all money received and paid for or on behalf of others that they must handle in the course of their duties. The society by law maintains a regimen of strict rules that mandate how these accounts and all such monies must be treated and the nature of records of all transactions relating to these monies that are required to be maintained. The monies must be deposited in a savings institution in a trust account, and must be identified as a trust account in the records of the member and of the savings institution.

Notary publics generally open accounts with banks for their legal businesses. This would include operating accounts and trust accounts. Trust accounts can be general (funds are pooled) or they can be specific. In a general/pooled account there are multiple beneficiaries of the funds.

On an annual basis, banks are required to notify trustees of their responsibility regarding pooled trust accounts with the amount held for each beneficiary in the trust. This is a CDIC ("Canadian Deposit Insurance Corporation") requirement. Banks also usually respond to requests from Notaries to confirm interest owed in pooled trust accounts; these requests are commonly initiated by the Notary annually.[5]

Banks have to advise the Society of Notaries, in writing, of any banking errors that involve a notary trust account, when identified.

There is a recent case involving a BC notary who allegedly ran a Ponzi scheme using the bank accounts of her business. The banks are caught up in civil litigation now because it is being alleged by victims of the scheme that they did not do enough to identify fraudulent transactions that were running through the notary business operational and trust accounts.

[5] http://www.cdic.ca/DepositInsurance/FAQ/Pages/default.aspx#trust deposits

5. Constraints

Nothing further identified than as described elsewhere in this report.

6. Description of sector associations

Our research has identified the following Canadian sector related associations:

- *Society of Notaries Public of British Columbia* – the mission of the Society is to ensure that its members provide the highest standard of notarial services to the public.
- *Union Internationale du Notariat, International Union of Notaries (UINL)* - is a non-governmental organisation established to promote, co-ordinate and develop the duties and activities of Notaries throughout the world and ensure the standing and independence necessary for optimum service to individuals and society through close collaboration between Chambers of Notaries. It was founded in 1948 by the representatives of the Chambers of Notaries of the following nineteen countries: Argentina, Belgium, Bolivia, Brazil, Canada, Colombia, Costa Rica, Cuba, Chile, Ecuador, France, Italy, Mexico, Paraguay, Peru, Puerto Rico, Spain, Switzerland and Uruguay. BC Notaries are understood to be the Canadian member.
- *Federation of Law Societies of Canada* – is the national coordinating body for Canada's 14 provincial and territorial law societies which governs lawyers nationally and 4,000 Quebec notaries.

7. Emerging business trends

There has been tension between the British Columbia Notaries and lawyers in the Province as the Notaries have made a number of attempts to increase the scope of the services they are allowed to provide, and in doing so are encroaching on areas typically served by lawyers. A February 2012 submission[6] by the Canadian Bar Association British Columbia Branch (the "CBABC") speaks to the issues and notes that several changes to the laws of the province have already expanded the scope of Notary work. The scope at the time of writing was as described earlier in this report.

The CBABC raised the following issues in arguing against the Notaries' request:

- Negative impacts on the public;
- Negative impacts on the handling of complexities inherent in legal matters;
- Negative impact on rural communities;
- Estate planning and administration;
- Incorporation of Companies; and
- Family Law was the subject of a separate submission by the CBABC.

The CBABC expressed the view that notaries should not be giving legal advice and that any expansion of notarial services should be performed under the supervision of lawyers and accordingly, be regulated by the Law Society.

A task force was struck to deal with the issue and on December 6, 2013, the Benchers of the Law Society of British Columbia unanimously approved in principle, three recommendations from the task force report[7] as follows:

1. That the Law Society and Society of Notaries Public of British Columbia seek to merge regulatory operations;

2. That a program be created by which the legal regulator provide paralegals who have met specific, prescribed education and/or training standards with a certificate that would allow them to be held out as "certified paralegals"; and

3. That the Law Society develop a regulatory framework by which other providers of legal services could provide credentialed and regulated legal services in the public interest;[8] and

There are views indicating that if these recommendations are implemented they would have significant impact on legal services in the province.

[6] http://www.cba.org/BC/Initiatives/pdf/2012_Notaries_Submission.pdf
[7] http://www.lawsociety.bc.ca/docs/publications/reports/LegalServicesProvidersTF_final_2013.pdf
[8] http://www.slaw.ca/2014/01/24/law-society-of-bc-recommendations-may-have-significant-implications/

8. Products and services offered

An industry newsletter describes that many of the notaries have come to be a notary after at least one previous career, including that many are—or were—CAs, CGAs, surveyors, and lawyers. This is an indication that many notaries would or could provide a range of services to their clients, including financial and legal.[9]

As well, it is identified that many come from countries throughout the world and that this provides the general public the opportunity to receive the advice of experienced legal professionals from well-rounded backgrounds, many of which speak several languages and are able to serve the ethnic diversity of the province.

The services that BC Notaries can provide are mandated in section 18 of the Notaries Act and are described as follows:

a) draw instruments relating to property which are intended, permitted or required to be registered, recorded or filed in a registry or other public office, contracts, charter parties and other mercantile instruments in British Columbia;
b) draw and supervise the execution of wills
    i) by which the testator directs the testator's estate to be distributed immediately on death,
    ii) that provide that if the beneficiaries named in the will predecease the testator, there is a gift over to alternative beneficiaries vesting immediately on the death of the testator, or
    iii) that provide for the assets of the deceased to vest in the beneficiary or beneficiaries as members of a class not later than the date when the beneficiary or beneficiaries or the youngest of the class attains majority;
c) attest or protest all commercial or other instruments brought before the member for attestation or public protestation;
d) draw affidavits, affirmations or statutory declarations that may or are required to be administered, sworn, affirmed or made by the law of British Columbia, another province of Canada, Canada or another country;
e) administer oaths;
    i) draw instruments for the purposes of the Representation Agreement Act;
    ii) draw instruments relating to health care for the purposes of making advance directives, as defined in the Health Care (Consent) and Care Facility (Admission) Act;
    iii) draw instruments for the purposes of the Power of Attorney Act;
f) perform the duties authorized by an Act.

[9] http://www.notaries.bc.ca/resources/scrivener/winter2006/PDF/scrivener_winter_2006_8.pdf

The Society also provides the following list on its website;

- Affidavits for All Documents required at a Public Registry within BC
- Authorization of Minor Child Travel
- Business Purchase/Sale
- Certified True Copies of Documents'.
- Commercial Leases & Assignment of Leases
- Contracts and Agreements
- Easements and Rights of Way
- Estate Planning
- Execution/Attestation of International Documents
- Health Care Declarations
- Insurance Loss Declarations
- Letters of Invitation for Foreign Travel
- Manufactured Home Transfers
- Marine Bills of Sale and Mortgages
- Marine Protestations
- Mortgage Refinancing Documentation
- Notarizations/Attestations of Signatures
- Passport Application Documentation
- Personal Property Security Agreements
- Powers of Attorney
- Proof of Identity for Travel Purposes
- Purchaser's Side of Foreclosures
- Representation Agreements
- Residential and Commercial Real Estate Transfers
- Estate Transfers
- Restrictive Covenants and Builder's Liens
- Statutory Declarations
- Subdivisions and Statutory Building Schemes
- Wills Preparation
- Wills Searches
- Zoning Applications

Some BC Notaries provide these services:

- Marriage Licences
- Mediation
- Real Estate Disclosure Statements

9. Type of customer(s)

Because of the nature of the work of notaries, the majority of their customers are individuals. They are not allowed to offer their services outside British Columbia but they may serve anyone in their geographic catchment irrespective of their nationality or residence, provided the service is authorized by the Act.

10. Geographic considerations

The notaries are restricted to acting in the Province of BC.

Through membership in the International Union of Notaries, the BC Notaries have access to notaries practicing around the world. An industry newsletter cites that "Through this association, the BC Notary is in a position to better represent the needs of the public and to do business within a global economy that requires—with increasing frequency—the services of Notaries Public throughout the world to authenticate and verify important transactions and documentation."[10]

[10] http://www.notaries.bc.ca/resources/scrivener/winter2006/PDF/scrivener_winter_2006_8.pdf

11. Key points from interviews

1. Notary publics generally open accounts with banks for their legal businesses. This would include operating accounts and trust accounts. Trust accounts can be general (funds are pooled) or they can be specific. In a general/pooled account there are multiple beneficiaries of the funds.

2. On an annual basis, banks are required to notify trustees of their responsibility to Pooled Trust Accounts with the amount held for each beneficiary in the trust; this is a CDIC ("Canadian Deposit Insurance Corporation") requirement. Banks also usually respond to requests from Notaries to confirm interest owed in pooled trust accounts; these requests are commonly initiated by the Notary annually. See link on CDIC website.

3. Banks have to advise the Society of Notaries, in writing, of any banking errors that involve a Notary Trust account, when identified.

4. There is a recent case involving a BC notary who allegedly ran a Ponzi scheme using the bank accounts of her business. The banks are caught up in civil litigation now because it is being alleged that they did not do enough to identify fraudulent transactions that were running the notary business operational and trust accounts.

5. Generally, notaries provide much of the same services to the public as lawyers do, but do not act in contentious matters.

12. Risk factors

12.1 Products and services

12.1.1 Provision of financial intermediary transactions through trust accounts

The provision of financial intermediary type services is vulnerable to abuse by money launderers in particular.

12.1.2 Expanding scope of services

There appears to be an on-going movement by the BC Notaries to expand the scope of their services. To the extent this expansion enhances the ability of the BC Notaries to provide financial intermediary type transactions; there is increased vulnerability for money laundering and terrorist financing.

12.1.3 Breadth of services offered that potentially support financial intermediary transactions.

Research indicated that generally, many notaries had former or other careers; e.g. that being a notary was not all that they did for their career. Specifically, the profession of accounting was one area noted that a number of notaries practiced in. The provision of financial intermediary type services by persons with both legal and accounting expertise is vulnerable to abuse by money launderers in particular.

12.2 Geography

12.2.1 Access to international network

Potentially facilitates dealing with more clients and transactions that are international in nature rather than local, and there is inherent risk attached to the provision of legal services to international transactions and flows of funds.

12.3 Business relationships/linkages with other sectors

12.3.1 BC notaries and lawyers

Some research indicates that the relationship between the two groups has been strained and difficult and therefore perhaps more prone to competitiveness rather than working together, providing support for one another. More research would have to be done to understand this better and what the impacts on vulnerability to money laundering and terrorist financing are.

12.4 Transaction methods and types

12.4.1 Real estate deals and handling of funds for same

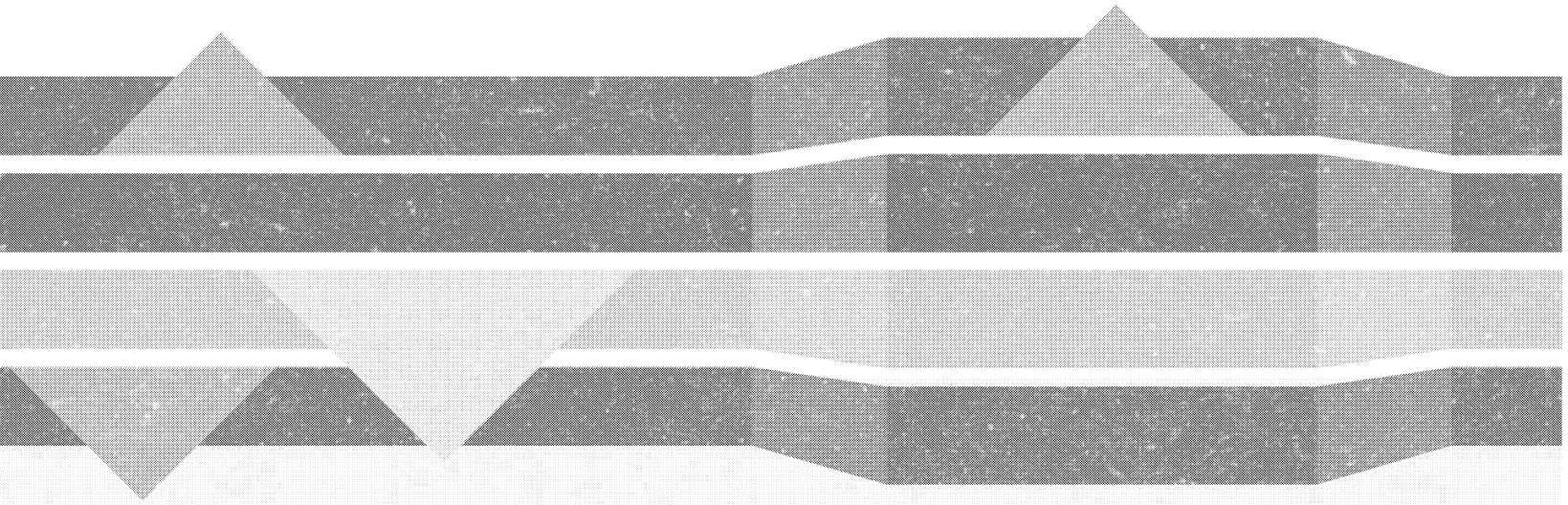
The provision of notary services to real estate transactions exposes this sector to many of the identified risks for the real estate sector.

Grant Thornton

Reporting Entity Sector Profile
Credit unions

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014



Appendix 9

Contents

1. General sector profile

A credit union (or caisse populaire) is like a bank, in that it takes deposits, makes loans and provides other financial services. Unlike banks, credit unions are co-operative institutions which are owned and controlled by their members which have a common bond and dedication to the people and communities they serve. Typically, this bond is established to serve a particular group of people based on a geographic area, ethnic background or employer. Credit unions support not only their own members, but also the other credit unions and other co-operative organizations.

Cooperative Credit Associations, usually referred to as the 'centrals' are also organized and operate based on cooperative principles. With the exception of the Credit Union Central of Canada (CUCC), the centrals provide support and services to the credit unions in their membership (usually throughout a province). OSFI is the regulator with oversight for the various cooperative credit associations. CUCC, which is federally-incorporated, functions as the national trade association for the Canadian credit union system and does not provide any financial services. Most credit unions, through their provincial central are affiliated with CUCC. There are provincial regulators in each province.

The number of credit unions is consolidating, there are approximately 340 now and the consolidation is expected to continue. However, the number of locations has not changed significantly throughout this consolidation. There are approximately 1,700 locations across the country. It is the regulatory cost burden in part which is driving consolidation.

The credit union equivalent in Quebec, with some locations in other provinces, is the caisse populaire. The caisse populaire is a cooperative, the members of which are generally people living in a given geographical sector, such as the same town or neighbourhood. Most Quebecers are members of the Desjardins caisse that is closest to their home or workplace.[1]

There are 376 caisse Desjardins in Quebec and Ontario with 897 service locations and they are all assembled under a single federation, the Fédération des caisse Desjardins du Québec.[2]

There is huge diversity in the size of credit unions (and caisse populaires[3]) size; with some being quite large and other quite small. For example, approximately two thirds of credit unions (not caisse populaires) have less than $175 million in assets.

[1] http://www.desjardins.com/ca/about-us/desjardins/governance-democracy/structure/
[2] Ibid.
[3] Note: this document uses credit unions to refer to both credit unions and caisse populaires together except where specifically identified.

While all credit unions are independent, have their own approach, and each their own strategy and policies, the network is known as the "credit union system" which works together to support one another and its members.

Credit unions differ from banks and other financial institutions in that those who have accounts in the credit union are members and owners, and accordingly these members elect their board of directors in a one-person-one-vote system regardless of the amounts invested. Credit unions are accountable to their members. Market surveys repeatedly indicate that credit unions are ranked number one for customer service.

A number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Comparative level of system risk management and monitoring sophistication
- Governance structure: requirements for board members
- Smaller sized and/or resource challenged credit unions
- Credit Union system provides access to international banking network:

2. Structure, size and segmentation, reporting entity population

There is a low level of market share concentration, with the top three credit unions accounting for approximately 14.3% of industry revenue in 2013. The remainder of revenue is split among the remaining credit unions, with the top 100 accounting for the majority of that share. Most credit unions are small and hold relatively small shares of assets.[4]

The number of credit unions (including caisse populaires) fell from 771 in 3,117 locations in 2012 to 724 in 3,030 locations at the end of 2013. As indicated, this is due to the continued consolidation in the credit union industry. Total combined membership (number of customers) reached 10.1 million across Canada at the end of 2013.

There is simplicity and complexity in the system; even the largest credit unions have smaller branches to serve their members. Each credit union has its own controls, procedures and monitoring, each has much autonomy and its own governance structure. At the same time, each credit union is part of a great whole, a member of a provincial central, member of a national trade association and there are many shared structures and operations, activities including for example shared organizations for the provision of wealth management, insurance, transaction processing, training, and marketing.

[4] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013

The following chart provides detail of the credit union system across the country:

FOURTH QUARTER 2013
CREDIT UNION/CAISSE POPULAIRE SYSTEM RESULTS

AFFILIATED CREDIT UNIONS & CAISSES POPULAIRES

($millions)

Province	Total Savings/Deposits	Total Loans	Total Assets	Total Credit Unions	Total Locations	Total Membership
British Columbia	$52,033	$50,894	$58,958	43	371	1,877,940
Alberta	19,610	18,529	21,694	33	207	646,698
Saskatchewan	15,968	14,615	18,214	53	285	490,712
Manitoba	21,050	19,368	22,730	37	190	599,284
Ontario	27,994	28,424	33,047	90	502	1,327,438
Ontario CPs	1,172	1,107	1,349	13	26	62,005
New Brunswick	829	732	909	10	30	69,301
Nova Scotia	1,870	1,605	2,077	29	76	153,979
Prince Edward Island	783	618	858	8	15	55,224
Newfoundland	949	862	1,026	10	39	52,651
TOTAL	**$142,258**	**$136,754**	**$160,862**	**326**	**1,741**	**5,335,232**

NON-AFFILIATED CREDIT UNIONS & CAISSES POPULAIRES

Caisses Populaires						
CPs outside of Quebec (MB, ON, NB)	**$7,226**	**$7,048**	**$8,440**	**34**	**141**	**329,627**
Quebec	105,007	116,851	141,106	358	1,130	4,454,480
TOTAL (All)	**$112,233**	**$123,899**	**$149,546**	**392**	**1,271**	**4,784,107**
Credit Unions						
Ontario	$338	$248	$383	6	18	37,484
TOTAL	**$112,571**	**$124,147**	**$149,929**	**398**	**1,289**	**4,821,591**

COMBINED CANADIAN CREDIT UNION & CAISSE POPULAIRE SYSTEM RESULTS

TOTAL	**$254,829**	**$260,901**	**$310,791**	**724**	**3,030**	**10,156,823**

Above Figures do not include affiliated companies of the credit union system, such as Concentra Financial Inc., The CUMIS Group Ltd., The Co-operators Group Ltd., Credential Financial Inc., and NEI Investments.

Source: Credit Union Central of Canada website, Systems Results, March 2014

Further detailed statistics are provided at Appendix A.

3. Economic and financial statistics

Canadian credit unions and caisse populaires (those affiliated with CUCC) reported an increase of 5.5% in total assets by the end of 2013 to $160.8 billion, compared to $152.5 in the 2012. Funds on deposit were reported as $142.2 billion representing an increase of 5.7% since 2012.

Non-affiliated credit unions and caisse populaires (including those located in Quebec, Manitoba, New Brunswick and Ontario), reported total assets of $149.9 billion compared to $143.4 billion in 2012. Deposits were reported as $112.5 billion, a 2.4% increase over 2012.

Further details are provided at Appendix A.

4. Regulation of credit unions

Credit unions are regulated by the provincial ministries of finance, the provincial centrals and the provincial deposit insurance corporations. In Ontario, for example, the credit unions are regulated through a comprehensive regulatory framework which involves the Ministry of Finance, the Financial Services Commission of Ontario (FSCO) and the Deposit Insurance Corporation of Ontario (DICO) and the legislation is the Credit Unions and Caisse Populaires Act, 1994 (the Act) and regulations.[5] In Quebec, the Autorité des Marchés financiers (AMF) is the body mandated to regulate the provinces financial markets including the caisse populaires. Annually, credit unions are required to have their operations audited by independent auditors.

The Centrals are provincially incorporated, and regulated and supervised at the provincial level. The supervisory approach taken by OSFI focusses on liquidity requirements as set by provincial legislation, specifically the policies and procedures that enable the Centrals to fill their statutory roles of providing sources of liquidity to, and assuming excess liquidity from, their local credit union members, to help them manage their liquidity and funding positions and hedge their risk exposure[6].

[5] Bulletin CUCP-01/09 - Important Changes to the Credit Unions and Caisse Populaires Act, 1994 and Regulations
[6] http://www.central1.com/about-us/credit-union-system

5. Constraints

Credit unions are restricted to operations within their province and are not currently able to operate federally. See emerging trends.

For new participants to the sector, an organization must receive approval from the government in the province where it plans on operating. For example, credit unions planning to operate in British Columbia must receive approval from FICOM. As well, a significant amount of capital to launch a network of branches and ABMs is required as well as reliable channels to gain funding to make personal and commercial loans.[7]

[7] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013

6. Description of sector associations

Canadian Cooperative Association - provides leadership to promote, develop and unite co-operatives and credit unions for the benefit of people in Canada and around the world.

- *Credit Union Central of Canada* - The Board of Directors at Canadian Central are comprised of 10 directors, appointed by the five provincial regional Central (Centrals) member shareholders. The principal role of the Centrals is to monitor and maintain system liquidity at the provincial level down into the grassroots of the system. The liquidity pool is shared and designed to maintain system stability by covering normal cyclical requirements. Along with provincial deposit insurance and other financial facilities, the result of all Centrals working together is the assurance that credit unions are among the soundest of all Canadian financial institutions.

- *Central 1* – is the primary liquidity manager, payments processor and trade association for member credit unions in B.C. and Ontario. It provides financial products, investment banking services, payment processing solutions and direct banking services, as well as leadership and advocacy on behalf of the credit unions represented.

- *Alberta Central* is the central banking facility, service bureau and trade association for Alberta's credit unions.

- *SaskCentral* is a financial services co-operative, providing research, support, consulting services and financial liquidity management to Saskatchewan's 53 credit unions. SaskCentral functions as a trade association on behalf of the province's credit unions and acts as the voice of credit unions in matters of common interest.

- *Credit Union Central of Manitoba* is the trade association for Manitoba's 41 credit unions, providing services in areas of capital and financial management, banking services, product and service research and development, consulting and representation and advocacy.

- *Atlantic Central* has offices in Halifax, Nova Scotia, Riverview, New Brunswick and Charlottetown, Prince Edward Island, its role is to provide liquidity management, payments processing and trade association services that support the credit unions of Atlantic Canada. The central provides leadership, advocacy and a range of support services in the fulfillment of these key functions.

- *L'Alliance des caisses populaires de l'Ontario limitée* - includes a network of 13 Caisse populaires which offer services within 29 branches in Northern Ontario.

- *Fédération des Caisses Desjardins du Québec* - The Fédération is the organization that supports the Desjardins caisse in Québec.

- *Provincial Deposit Insurance Corporations* - The deposit insurance corporations provide insurance to protect the savings of depositors to credit unions in the event a credit union is unable to repay its depositors:

- *Deposit Insurance Corporation of Ontario, DICO*
- *AMF, Quebec*
- *Nova Scotia Credit Union Deposit Insurance Corporation*
- *New Brunswick Credit Union Deposit Insurance Corporation*
- *Deposit Guarantee Corporation of Manitoba*
- *Credit Union Deposit Insurance Corporations of BC, Saskatchewan, Alberta, PEI and Newfoundland*
- *ACCULINK®* - service which provides credit union members with surcharge-free access to more than 1,800 credit union ATMs at almost 400 credit unions across the country. 'ACCULINK enables more than five million credit union members to withdraw funds, make deposits, change their PIN, transfer balances and make account inquiries at participating credit union ATMs without having to worry about paying additional fees.'
- *CUPS (Credit Union Payment Services)* – is a provider of reliable, innovative and cost effective payment services to credit unions, corporate clients and others in the financial services industry.
- *Credit Union Knowledge Network (CUSOURCE®)* - is a wholly owned subsidiary of CUCC which provides learning solutions to the Canadian credit union system, was built by and for the Canadian credit unions, also the hub for the Credit Union Institute of Canada, the strength of which is evident by the ever-growing number of graduates of its professional programs.
- *Credit Union Institute of Canada (CUIC®)* is the professional designation division of CUSOURCE® Credit Union Knowledge Network (CUSOURCE Knowledge Network), the national educational association owned by the Canadian credit union system.
- *CUETS Financial* - MasterCard credit card issuer in Canada, delivers service to cardholders through a network of 375 credit unions and caisse populaires. Headquartered in Regina, Saskatchewan with a service center in Winnipeg, Manitoba and regional sales team members in Vancouver, Calgary, Toronto and Moncton.
- *Credential Financial Inc.* - national wealth management and investment services provider owned by the Canadian credit union system. 'With over 20 years in the Canadian financial services industry, Credential Financial is a national wealth management firm providing MFDA and IIROC dealer services, online brokerage, and insurance solutions to over 225 organizations and more than 1,300 advisors.'
- *Ethical Funds Credential Asset Management (CAM)* - distributes Ethical Funds and third-party mutual funds through credit unions across Canada.
- *CUMIS Group Ltd.* - partners with credit unions to deliver competitive insurance and financial solutions. In doing so, it creates financial security and promotes the growth and success of the credit union system in Canada. CUMIS Insurance in partnership with The Co-operators offers an integrated portfolio of both organizations' insurance products and related services to credit unions.

7. Emerging business trends

The larger credit unions are working towards federal status and the smaller credit unions are grouping and working together more. In 2010, the Government of Canada introduced legislation as part of the Jobs and Economic Growth Act and this legislation amends federal acts, including the Bank Act, to allow credit unions to expand outside of their native provinces. "With their potential for growth improved, credit unions will be able to gain economies of scale and compete more favourably with commercial banks on pricing and interest rates. However, the effects will not be felt overnight because it will take many years for even the largest credit unions to increase their assets and diversify their loan portfolios to include larger loans (i.e. commercial lending)."[8]

The sector is continuing to consolidate; however this is expected to slow over the next few years due to the larger credit unions pursuing federal status.

More credit unions are providing wealth management services, either individually working with Credential or CAM, or coming together as smaller groups of credit unions to partner within their regions and work with groups like Credential and CAM.

Research with interviewees identified that credit unions have significant opportunity to target corporate, business members and that more credit unions are beginning to pursue this.

Credit unions are exploring and investigating more on-line services, mobile apps etc., they still however need to service an older population. Interviewees reported that there are really hard questions and challenges as to how to do this effectively (move to more on-line, automated methods) given the size and structure of the credit union system. Much of what happens in the credit unions system today is form based, more manual even when it is automated.

The sector is cognizant of the recent OSFI requirements around board of director changes for banks and that this needs to be considered for the credit union context.

Increased competition from commercial banks has been experienced by this sector. The banks account for over 75.0% of the consumer credit market. The size of the banks, ease of consumer access and the new technologies being introduced have made the banks more appealing to consumers. However, it is noted that consumers often benefit from more personalized service at credit unions, which is a counter balance.[9]

---

[8] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013
[9] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013

8. Products and services offered

The products available from credit unions are very similar to what is offered by banks. Most credit unions offer chequing, loans, and savings accounts. Smaller credit unions often have less complex services and/or delivery and access channels and the larger credit unions have services comparable to the larger bank offering with significant choice as to access and delivery channels.

The breadth of service offering includes: chequing, savings, foreign exchange, wire transfers, mortgages and loans and lines of credit, term deposits, TFSAs, RRSPs, RRIFs, RESPs, online and mobile banking, business banking, investment services and professionals, online trading, discretionary investment management, insurance including health and dental, disability, critical illness, long term care, life, credit cards (Visa and Mastercard).

Access and delivery channels include in-branch services, mobile and internet banking, ATMs, transactions through personal teller machines (PTMs), telephone banking, email and fax services, night deposit services, cash management services, mobile payment services (e-wallets), customer access through system network (e.g. access through other credit unions in the system).

'Accessing almost any credit union (except the smaller ones) provides access to international banking services.'

9. Type of customer(s)

The customers of credit unions are members who actually own a share in the credit union. Each member has a vote and can participate in the Board of Director elections.

Generally in the past, credit unions could not simply offer their services to anyone and were limited to working with members who shared the common bond; the bond may be the geographic community, a workplace, a religion, or other type of bond. Today, many credit unions are open bond, or not bonded. Under legislation, each credit union must ensure that any services provided to non-members are limited to a specific amount, e.g. 5%. If a credit union fails to limit their services to non-members, they risk losing their status as a credit union.

Credit unions have a wide breadth of customers including individuals and businesses of all types and background. Business clients however tend to be smaller companies and organizations rather than larger, however this is not a rule and there are many exceptions.

In terms of geography, the majority of credit union members tend to be local to the credit union location, Canadian individuals and businesses. Credit unions do however provide services to non-residents and this generally happens when a resident moves out of country.

Many credit unions have residency requirements for their members, and these requirements are determined individually by each credit union. Credit unions in Manitoba have an unlimited deposit guarantee which has resulted in a higher number of out of province members.

A market study report provided the following[10]:

- Personal members are expected to account for approximately 62.8% of revenue in 2013. Main services accessed: depository functions and often secured mortgages and automobile loans.
- Commercial members are expected to account for 33.9% of membership in 2013. Main services accessed: business and commercial loan options. It is noted that, although many large corporations deal exclusively with commercial banks because they require more capital, small businesses often choose to work with credit unions because of the personalized customer service.
- Other members are expected to account for about 3.3% of membership in 2013. Main services accessed: one-off, niche transactional services, which typically include student loan services, retirement services, auto financing and other real estate transactions and that the majority of these members have their primary accounts with commercial banks.

[10] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013

10. Interview notes

10.1 Sector background

1. The credit union system has a co-operative spirit. Credit unions have bought into this system – and there is a belief that reputational risk is the System's biggest hurdle to growth.

2. The uninformed think that credit unions are vulnerable – but this is so far off the mark.

3. Based on market surveys, credit unions have been ranked #1 for customer service for nine years in a row; this really shows that the co-operative model works.

4. The financial results of the credit union system have been very strong. There have been record profits through the financial crisis and for 2013; loan losses have been really low. The System is well capitalized and generally risk averse.

5. Credit unions are important competitors within the Canadian financial services market – and this segment (the credit unions) are starting to have resources to access outside expertise more and more.

6. Across Canada in the past 10 years there have been at most only three new credit unions and two of them did not survive. There have been no new ones for at least the last four years except through mergers. It is not that easy to become a credit union.

7. Most credit unions have residency requirements for their members. This is built and defined at the individual credit union level. In Manitoba there is an unlimited deposit guarantee and so this means there is much more out of province membership for these credit unions. The Act and regulations in each province lays out the context for membership.

8. The number of credit unions is consolidating, now 340 plus and the consolidation will continue. However, the number of locations has not changed despite the consolidations. There are still approx. 1,700 locations across the country. Regulatory cost burden in part is driving consolidation; there are still many small credit unions.

9. With the smaller ones, they tend to be community based so they know their customers – this is a protection; with larger institutions customers can obtain services with a level of anonymity. There is a protection in being small. Smaller credit unions know their customers, the tellers know their neighbours, this is the dynamic, this is face-to-face and it is hard to achieve anonymity.

10. There is a huge diversity of credit union size; two thirds of credit unions have less than $175 million in assets. All credit unions are independent, all have their own approach, and each has their own strategy, policies.

11. Credit unions are regulated and structured provincially. Each province also has a central type of association which is not the regulator. The Centrals do transaction settlement and clearing services for the credit unions as well as other services for the credit unions of the province.

12. Central 1 is the central for BC and for Ontario credit unions, acting as an operator of clearing for the system and providing switches, and services for member directly. Processing by SaskCentral is outsourced to CUPS and CUPS, which formerly outsourced wires through Travelex, now use Western Union.

13. CUPS (Credit Union payment Services), is jointly owned by Alberta Central and SaskCentral and is progressing towards other banking areas, for example, electronic signatures.

14. Deposit guarantee organizations- these organizations are concerned with protecting depositors of credit unions and caisse from loss.

15. Provincial regulation and Centrals:

    a) Ontario: FSCO – Ministry of Finance and DICO; FSCO – has delegated many of their powers to DICO, Central 1
    b) BC: FICOM, Central 1
    c) Alberta: Alberta Department of Finance, Alberta Central
    d) Saskatchewan: Credit Union Deposit Guarantee, SaskCentral
    e) Manitoba: Manitoba Deposit Guarantee
    f) Atlantic: now the government s are paying a lot of attention because of past problems; RMA New Brunswick, CUDG – Nova Scotia; Atlantic Central

16. What does the regulator do:

    a) Audits and monitors the financial viability, performs lending audits, reviews capital requirements quarterly basis, credit unions sends information in for review;
    b) Regulator would oversee any new setups – have to meet financial requirements plus co-op requirements;
    c) Does not necessarily oversee board members but does have regulations regarding how long a board member can serve consecutively. There are now maximum terms; Nova Scotia/New Brunswick/Prince Edward Island – nine years is the maximum.

17. CUMIS is a national organization that provides corporate insurance, fidelity bond, professional and liability, privacy, property & casualty financial coverage. CUMIS brings them together, the regulators and centrals, to talk about the risk in the system; at least annually. Stronger focus is on lending risk versus other risk areas. It is the Centrals or the regulator that make decisions in Newfoundland, Manitoba and Alberta around the insurance program purchase.

18. CUMIS insures against specific loss situations; deposit insurers e.g. DICO, protect the deposits and is therefore more focused on the way loans are managed. Generally, smaller credit unions are risk rated higher but do take care of their lending because they can't afford losses. There is a focus on financial stability, lending limits are given. Because of the bonding insurance they do take a look at the results of any FINTRAC audit.

19. Many smaller credit unions come together, work together, for their risk officers and management.

20. What is the System's response to offside credit unions? If there is anything unusual enough they can go in and be the administrator/supervise (to get it to where they want it to be):

    a) DICO –they can go in and administer and be the supervisor
    b) CUMIS – cancels insurance program

21. Credit union board members must be elected from the credit union membership, their role is to serve and answer to the members. There are rules around the length of term for board members and training requirements and only for a few exceptions (e.g. New Brunswick) will there be a review of the quality of the board member. Across the country, credit unions send board members to training; this is the System working together. CUDA training 'Credit Union Director Achievement', this is a national program, run out of Credit Union Central of Canada group called CUSource and this is run independently of the provincial Centrals.

22. The larger credit unions are generally performing background checks on new board members.

23. They are aware that OSFI has new rules around Board of Director changes and that OSFI must be advised and presumably has some say and/or oversight to this. The credit union system is not there yet; will this come from the provincial regulators? It is not known.

24. DICO has a memorandum of understanding with FINTRAC to conduct examinations, as part of the on-going work that they do. DICO has a questionnaire/survey for the AML regime, the results of this survey are sent to FINTRAC. This then helps them in planning their work

25. DICO has working relationship with FICOM. FICOM is DICO and FSCO all in one. Ontario is the only major province that has two separate groups (DICO and FSCO); FICOM is the only financial services regulator in British Columbia. Also, DICO meets regularly with OSFI to stay abreast of the issues.

26. Many years ago, 15 – 20, there were 1,200 credit unions in Ontario, today there are 126 credit unions in Ontario. Much consolidation and this has resulted in larger, more sophisticated credit unions in the province.

27. DICO has published an 'Advisory' to the Ontario System regarding money services businesses (MSB); they regularly provide these types of guidelines.

28. DICO has no authority regarding the directors of credit unions, but to note:

    a) DICO Bylaw #5 – sound practices, this is all about governance
    b) DICO has also published guidelines for directors for training, competencies etc.

29. There are programs for monitoring the escalation of risk in a credit union:

    a) Financial metrics are reported monthly and DICO has a system to flag and follow up;
    b) Depending on the risk level, the approach to respond to the risk is executed;
    c) Report is issued after examination, action plan is requested and DICO works with the Board; and

d) They do have a watch list process.

30. When DICO does an examination, they take a sample of files and this includes commercial accounts.

31. If a new credit union was going to start, they would have to deal with FSCO; FSCO is the only authority to issue a charter number in Ontario.

32. Up to 2009, DICO was only the deposit guarantor, then in October 2009 the Act was renewed and a number of FSCO responsibilities went to DICO and so DICO became the regulator. FSCO still has market conduct issues (e.g. advertising, member complaints) for the whole financial services sector broadly. Also, concerns about credit union board members would be addressed with FSCO.

33. If two credit unions wanted to amalgamate, it is FSCO that issues the new charter. FSCO will consult with DICO on this. FSCO has a number of other legacy powers, Superintendent of FSCO is the only one that can deal with bond of association issues for credit unions for example (not involved very often). For credit union amalgamations this is FSCO, for any purchase and sale activity this is DICO.

34. DICO provides the deposit insurance to credit unions and caisse populaires in Ontario; ensures that regulations are followed and the sector is sustainable.

35. In Ontario, membership is required in order to use credit union services. Up to 3% of an Ontario credit union's membership can be outside of their bond of association – mostly Ontario credit unions are community bond. During examinations there is some spot verification done on this.

36. Credit Unions could have voluntary disclosure re: bad individuals/accounts – nothing formal

10.2 AML Compliance

37. Credit Unions look at AML as a burden; few have the money to pay for and resource what is perhaps needed. The compliance regime is not centralized in any way. This has resulted in a spectrum of AML regime response from weak to strong.

38. There is at least one 'National Risk Management Group' in the System (it is believed there are others) and this group:

    a) Is coordinated by CUMIS, approx. quarterly meetings
    b) Has involvement of persons from some regulators, some centrals, some larger credit unions
    c) Is focused on claims experience/claims trending – thefts, wire transfer losses, dishonesty losses
    d) Is not focused on AML, the focus is on the losses/potential losses to the credit union

39. Who determines the effectiveness of AML regimes within credit unions? Interviewees reflected that this was FINTRAC's role. Also that the provincial regulators and deposit guarantees do conduct some review of AML compliance programs. How effective is this? Not known, not a focus. Most provinces regulators and deposit guarantors are not focused on effectiveness.

40. Some groups within the System make the AML training mandatory and make it part of their conferences.

41. Recent experiences e.g. the MSBs have raised awareness within the System regarding AML issues.

10.3 Trends

42. Credit unions may be permitted under their province's legislation to have up to a percentage of non-members as customers (would be small, like say up to 5%). This means that there is potentially a growing market for credit union customers who are non-members. However, it is not thought that credit unions will broadly pursue this.

43. More credit unions are going after corporate business. These could be customers that would be non-members (as per above).

44. 'Exchange Network' as an example of how credit unions are coming together in groups, sometimes including with smaller banks, e.g. a Tier 2 bank, to honour each other's deposits and other forms of transactions.

45. Wealth management services, most credit unions now participate through the Credential Asset Management group ("CAM").

46. The larger credit unions are applying for Federal status so that they can operate in multiple provinces.

47. Credit unions are starting to have the resources to access outside expertise more and more (than they have been able to afford in the past).

10.4 Risk areas

48. All credit unions should be worried about reputational risk.

49. British Columbia credit unions have the most international transactions, Ontario might be next.

50. Most credit unions provide access to international banking services; only the smaller credit unions would not have this access.

51. Credit unions have had some exposure with getting involved with organized crime unwittingly and this is concerning.

52. Seems unlikely that smaller credit unions are targeted by money launderers because of the minimal opportunity for anonymity. 'If I were a money launderer, I would target the larger financial institutions for anonymity, they don't really know their customer.'

53. Credit Unions that don't have the proper internal controls, the smaller ones are weak, e.g. most banks are not working with MSBs, or at least the risky ones, so now they are approaching the credit unions. There have been losses to a credit union in the system related to banking MSB's. There is a recognition that this needs to be tightened up.

54. Risk is different depending on the size of the credit union: small – medium – large.

11. Risk factors

11.1 General market

11.1.1 Comparative level of system risk management and monitoring sophistication

The level of risk management and monitoring systems within the credit unions is significantly less than the sophisticated levels within the larger banks. While there is no data with which to quantify this, it is believed to apply broadly to all operational process of the credit unions, including specifically transaction monitoring systems. This is primarily caused by the make-up of the credit union system itself, reflecting that each credit union while being part of a larger system, is an independent, autonomous organization.

An important factor that mitigates some of the risks for most, smaller credit unions is that nature and size provide a better opportunity to know their clients and have a more personal relationship. As well, many credit unions are now using or beginning to use more sophisticated transaction monitoring software (e.g. the Verafin product), which, while sufficient to meet regulatory requirements, and provide a certain level of monitoring, are significantly less sophisticated than that complex data analysis (e.g. monitoring of customer network relationships as opposed to more focused transaction/profile monitoring) used in some of the larger banks.

11.1.2 Governance structure: Requirements for board members

Credit union board members must be members of the credit union, and this generally means, that to the extent the credit union board has a need for specific expertise and experience, there is a smaller pool of persons from which to draw from.

Interviewees shared that while there are rules regarding the length of term for board members and training requirements (e.g. around 'financial literacy'), only in a few provinces (e.g. New Brunswick) is a review performed on the quality (of the experience, expertise) that a board member brings to the make-up of the board.

Interviewees stated that the larger credit unions are generally performing background checks on new board members.

It is not known to what extent credit unions may be exploring the concept of independent directors (e.g. no membership requirement).

11.1.3 Fragmented regulation and oversight

The regulatory structure is fragmented and organized provincially. This does not easily allow for these organizations to deliver robust monitoring, oversight and to support national best practices risk management systems at the credit unions.

11.2 Products and services

11.2.1 International wire services

Many credit unions provide access to international wire transfer services, both incoming and outgoing. Interviewees stated that it would only be the very smaller credit unions that could not provide or could not provide access to these services.

11.2.2 Wealth management services

Research indicates that wealth management services are areas that credit unions are further pursuing for growth and expanded levels of service. Financial sector experienced experts report that this area of the business is basically built and sold based on privacy and that there are real struggles to effectively monitor activity and sources of funds.

Nothing else specifically identified different from rest of financial entity sector.

11.3 Delivery/access channels

11.3.1 Smaller sized and/or resourced challenged credit unions

Interviewees stated that credit unions that lacked the proper internal controls were typically smaller; meaning that risk management would not be as robust and the credit union would be more vulnerable to abuse. News article examples are provided in Appendix A.

An example was shared relating to the larger banks exiting MSB relationships and the credit unions being approached for services. Appendix A provides several examples of this occurring within Canada, as well as examples from the US.

Research indicates that the credit union regulators themselves have identified that 'some credit unions [in order] to improve profitability by seeking non-traditional sources of revenue' … '…have entered into arrangements to provide banking and wire transfer services to member-owned Money Service Businesses (MSBs) which are generating fee income from related cash handling, wire transfer and foreign exchange services.' 'This level of revenues may unduly influence the credit union's rationale for entering into the MSB business by placing an inappropriately high weighting on potential return versus the associated risk.' See the DICO Operational Risk Advisory provided at Appendix A.

"Credit unions need to be able to cope with slower lending growth by increasing non-interest income. Credit unions may need to make an aggressive push on non-traditional products by providing other financial services."[11]

11.3.2 Use of 'Agent' referral sources

Some credit unions have relationships with businesses as 'agents' to sign on new business, new members. This could include for example, local car dealership and mortgage brokers. This is not necessarily different from other

[11] IBIS World Industry Report 52213CA Credit Unions in Canada March 2013

types of financial entities; however, this potentially becomes an access channel to the services of the credit union which the credit union has limited resources to manage from a risk perspective.

11.4 Geography

11.4.1 Credit union system provides access to International Banking Network:

See above, e.g. international wire services. No other risks were specifically identified and different from rest of financial entity sector.

11.4.2 Access to International Banking Network, international wire services

11.5 Business relationships/linkages with other sectors

11.5.1 Reliance and interconnectivity with other financial service providers

Example: In order to provide US dollar transaction clearing, credit unions rely on provincial centrals who have agreements with Canadian banks and in turn rely on US banks. With greater scrutiny by US banks regarding AML/TFD compliance, this is impacting credit unions. See above re: risk management and monitoring sophistication level.

11.6 Transaction methods/types

Nothing specifically identified different from rest of financial entity sector.

Grant Thornton

Reporting Entity Sector Profile: Casinos

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

The Canadian gaming industry is an important economic driver in the economy and a valuable source of revenue for the provincial and territorial governments in Canada. The gaming industry includes land-based casino gaming, lottery, horseracing and sports betting. While video lottery terminals ("VLTs") are generally considered as gaming, for the purposes of this report, this is not considered as part of the casino sector.

The funds generated from gaming revenue are directed to, among other applications, government consolidated revenue accounts, health funding, charitable organizations and education. The sector is highly regulated.

Over the past 15 years, the Canadian gaming industry has more than doubled in size from approximately $6.4 billion in gross revenue[1] in 1995 to approximately $15.1 billion in 2010. In 2010, the industry generated approximately $900 million in non-gaming revenue, such as food and beverage, accommodations, entertainment and retail.[2] In 2017, the Canadian casinos & gaming sector is forecast to have a value of $20.8 billion.[3]

Revenue from casinos continues to be the largest segment of the sector. The most recently available data, 2011, indicates that the 72 casinos across Canada had total revenue in excess of $5.626 billion.[4]

[1] Revenue is measured as wagers less prize payouts, before operating expenses.
[2] Gateway Casinos Prospectus – 2012
[3] MarketLine Industry Profile Casinos & Gaming in Canada June 2013
[4] Canadian Gambling Digest 2011-2012, June 2013

2. Structure, size and segmentation, reporting entity population

Canada accounts for 13.3% of the Americas casinos & gaming sector value. The United States accounts for 73.7% of the Americas sector.[5]

Country	$Bn 2012	%
United States	98.4	73.7
Canada	17.8	13.3
Mexico	3.4	2.6
Rest of the Americas	13.9	10.4
Total	133.5	100%

The market breaks up the sector into different segments, shown below, and the casinos segment generally covers all gambling activities carried out within casino establishments, such as card games, roulette, and slot machines located in casinos.

Casinos is the largest segment of the casinos & gaming sector in Canada, accounting for 52.1% of the sector's total value. The Lotteries segment accounts for 24.4% of the sector.[6]

Category	$Bn 2012	%
Casinos	9.3	52.1%
Lotteries	4.3	24.4%
Sports betting and related	0.5	2.9%
Other	3.7	20.6%
Total	17.8	100%

Research indicates that the size of the casino operator is a key success factor which benefits a handful of operators by providing scale and barriers to entry for potential new entrants.

There are 72 casino locations across the country with over half of them (41) being located in BC and Alberta.

[5] MarketLine Industry Profile Casinos & Gaming in Canada June 2013
[6] MarketLine Industry Profile Casinos & Gaming in Canada June 2013

3. Economic and financial statistics

The top three revenue reporting provinces are Ontario, BC and Alberta which make up $4.115 billion or 73% of the total. While Ontario has the highest reported revenues, with 10 casino locations it has fewer than Alberta (24), and BC (17).[7]

The tables at Appendix A provide further details and data.

[7] Canadian Gambling Digest 2011-2012, June 2013

4. Regulation of the casino sector

Gambling in Canada is an illegal activity except where it is made legal through provisions set out in the Criminal Code of Canada and sanctioned under the authority of each province. The Government of Canada has minimal involvement in gambling beyond Criminal Code prohibitions and permissions. In 1985, an agreement between federal and provincial governments established annual provincial payments to the federal government to assure that only provinces can authorize gambling.

No two provincial regulatory or operational regimes are the same. Different games and lottery schemes are permitted or prohibited, depending on the province. For example, casinos may be commercial, charitable, owned/operated by government, and/or operated by private companies under contract to provincial gaming authorities (or a combination of these).[8]

Provincial regulators relevant to casinos are as follows:

British Columbia Lottery Corporation (BCLC)
Alberta Gaming and Liquor commission (AGLC)
Saskatchewan Liquor and Gaming Authority (SLGA), Saskatchewan Indian Gaming Authority (SIGA), Indigenous Gaming Regulators (IGR), SaskGaming
Manitoba Gaming Control Commission (MGCC), Manitoba Lotteries
Ontario Lottery and Gaming corporation (OLG), Alcohol and Gaming Commission of Ontario (AGCO)
Loto-Quebec
New Brunswick Lotteries and Gaming Corporation (NBLGC), Gaming Control Branch (GCB)
Nova Scotia Provincial Lotteries and Casino Corporation (NSPLCC), Alcohol and Gaming Division (AGD) of Service Nova Scotia
PEI Lotteries Commission

[8] Organization and Management of Gambling in Canada

5. Constraints

Highly regulated markets which favour incumbent operators are a significant barrier to entry. Operators need to have suitable premises and considerable experience in order to obtain casino operating agreements or licenses. A new company attempting to enter this sector would require large amounts of capital to establish a casino, employ staff and acquire gaming equipment.

Gambling activities in Canada operate exclusively under the control of the provincial and territorial governments. The laws differ from province to province and entry to the Canadian market is reportedly not as straightforward as other countries. Charities, Aboriginals and private operators can enter the sector in Canada only by obtaining provincially-authorized agreements and licenses.

6. Description of sector associations

Our research has identified the following Canadian sector related associations:

Canadian Gaming Association – is a not-for-profit organization whose mandate is to create a better understanding of the gaming industry by bringing facts to the general public, elected officials, key decision makers and the media through education and advocacy.

American Gaming Association – similar to above and also representing the commercial casino entertainment industry by addressing federal legislative and regulatory issues affecting its members and their employees and customers, such as federal taxation, Internet gambling, and travel and tourism matters.

North American Gambling Regulators Association – NAGRA is a non-profit professional association of gaming regulators throughout North America. The organization brings together agencies that regulate gaming activities and provides them a forum for the mutual exchange of regulatory information and techniques. Collecting and disseminating regulatory and enforcement information, procedures, and experiences from all jurisdictions provides on-going gaming education and training for all members. (www.nagra.org)

International Association of Gaming Regulators (IAGR) - The International Association of Gaming Regulators (IAGR) consists of representatives from gaming regulatory organizations throughout the world. The mission of IAGR is to advance the effectiveness and efficiency of gaming regulation.

Commercial Gaming Association of Ontario - The Commercial Gaming Association of Ontario Board (CGAO) looks to serve as a resource centre for all those who are involved, engaged in, or have an interest in the Ontario Charitable Gaming Centre. www.cgao.ca

7. Emerging business trends

Canada is expected to be ahead of the US in working towards a more coherent national regime; with growth resulting from these trends attracting new onshore and offshore providers into the Canadian market. Possibly these new entrants will be seen to some extent as a 'test bed for offerings and models that may later be applied in the US when regulations allow'.

With governments now facing severe fiscal constraints and eager to replenish their coffers, their attention has been caught by the potential of legalized and licensed on line gaming services as a valuable source of tax revenues. There is also a strong argument that, since consumers will engage in illegal online gaming anyway, it is better to license and tax it than to allow the revenues to go to unlicensed operators.

Land based casinos are growing in international locations such as Macau, a former Portuguese colony in China, and Singapore. In 2013, Macau saw gambling revenues of US$45.2 billion, which was several times ahead of revenues in Las Vegas ($6.5 billion) and Singapore ($6.07 billion). In comparison, total gambling revenues for the whole of Canada totalled $17.8 billion in 2012, with approximately half of this from casinos.

There are some views in the market that the regulatory trends will increasingly shift toward the licensing of inter-country and interstate online gaming services, where liquidity is pooled and tax shared on an agreed basis between the different tax authorities.

8. Products and services offered

Gaming in Canada includes a number of different activities such as lotteries, gaming machines, poker, blackjack, sports betting, horse racing, etc. which are delivered through several methods of distribution (online/outlets/casinos etc.), and different payoff margins.

Casino locations, aside from the gambling activities provide non-gambling forms of entertainment and social activities.

Junket reps provide "one-stop shopping" to their players and work on behalf of different casinos for the benefit of the casino and gambler. These services consist of identifying and marketing to promote the host casino, provide the prospecting aspect of player development (searching for new qualified players) for various casinos, and also potentially provide credit to the gambler. Junket operators also provide information and can offer exclusive access to about upcoming casino special events, gaming or golf tournaments, headliner entertainment or shows, etc.

While junket operators typically operate in Asia, targeting high rollers for Asian casinos, operators in Canada include those serving local casinos such as bus/coach services or travel agencies offering gambling vacations overseas. The provision of gaming related services within the province, such as junket operating, requires the operator to register/be licensed with the provincial regulator.

9. Type of customer(s)

Customers are individuals who attend on site at the physical location of the casino. Visitors from other countries and provinces attend regularly. The popularity of different gambling activities within Canada means the number of buyers is large.

Loyalty by a customer to a particular market player / casino is reported as unlikely to be high; although compulsory membership in many casinos is helping them retain customers. Switching costs for consumers vary according to the type of gambling. For example, many casinos require annual membership fees; thus constituting a switching cost should a consumer change to a different casino before the annual membership expires. Generally switching costs remain minimal, particularly in the case of high-street bookmakers.

10. Key points from interviews

10.1 Discussion re on-line gaming with processing service provider

1. Certain countries are known to have online gambling licenses that are similar to land-based casinos. These countries include: Isle of Man, UK, Netherlands as well as certain native reserves in Canada. In Canada, outside of Indian reserves, online gambling licenses are not issued. As such, online casinos are not permitted to operate in Canada (i.e. head office may not be registered in Canada) although gamblers could be located in Canada.

2. Where gambling licenses are issued, the government has strict regulation and licensing requirements including meeting certain annual audit requirements by public accounting firms – capital requirements, number of gambling wins versus losses, ensuring same players aren't consistently winning from or losing to same players.

3. There is currently no online gambling licensing program in the US. However, interviewee has seen companies in past that are registered in the US and permit US gamblers—these casinos operate illegally and interviewee refuses to become involved with them.

4. There are certain countries where a gambling license would not be trusted—FATF-identified high risk countries, sanctioned or where there is no licensing regime.

5. The people behind the online casinos are typically European, Eastern European, Canadian, Australian and Asian – companies are setup and registered in above offshore countries. The operators include well known poker players, IT people that can "build a better website" as well as mom & pop operators that have bingo sites. Has not seen involvement by organized crime in past. There are also a few large conglomerate operations with significant holdings by private equity and foreign (UK) based bank.

6. How does money come out of system – there are payment processors and some are associated with local casinos and banks that will pay out winnings – however, this is a very saturated market and little commission fees.

7. Online gambling is actually decreasing due to generational shift. Typical players are aged 36 to 50 and they are professional gamblers that are online to make money and not only for entertainment purposes. Younger generation prefer online, non-gambling games and other users prefer MLM (multi-level-marketing) for making money such as selling banner ads on websites.

8. Certain US states are looking into offering online gambling licenses (Nevada, New Jersey). These states are looking into how casinos will operate and how they will prevent players that are physically outside of state from gambling.

10.2 Discussion with AML Expert with casino industry experience

9. In many cases, government regulators' motives are aligned with the casino as pure money laundering operations are generally not profitable for the casino (money flows in and then back out). Exceptions to this include Ye Gon, who had brought in $60 million from Mexico to gamble; however, this was an instance of a prolific gambler and therefore was a lack of incentive to report (as there were winnings for casinos)

10. Areas of monitoring for casinos are the gambler's source of funds and reviewing for large losses – where does the money come from?

11. Debt collection should also be a key area that casinos look at – what is the source of money that the client uses to pay off the debt?

12. Junket operators are not a high risk area in the US – this is more prominent in Asia.

11. Risk factors

11.1 General Market

11.1.1 New entrants to the sector

First Nations groups are continuing to lobby for shares of gambling revenue; the industry has been dominated by larger, more experienced players. New entrants mean that possibly any new casino sites are not run and risk managed the way others are. There are some articles indicating this at Appendix B. More research would have to be done to properly assess the risk.

11.2 Delivery channel

11.2.1 Junket operators or marketing agents

This is an intermediary role; possible receipt of funds from overseas or illegal sources. While no information was identified specifically involving Canada, this is a continued concern at other international locations. This is thought to be less of a risk for Canada as comparatively, Canada's casinos are seen as less desirable gaming destinations. More research would have to be done to properly assess the risk.

11.2.2 On-line gambling and gaming

An interviewee reported that there is a shift away from on-line gambling to online gaming (entertainment) and other forms of on-line potentially profitable ventures (e.g. banner ads and multi-level marketing.) It is unknown what the impact of this is on physical casino operations, although as an example, casinos are financially suffering in Atlantic City despite the bankruptcy of two competing casinos. However, all of these on-line areas are not directly subjected to the PCMLTFA (generally, the companies processing payments for many of these on-line sites are subject to regulations) and as volumes grow, these on-line areas are likely more vulnerable to abuse by money launderers.

11.3 Transaction methods and types

11.3.1 Transactions structured to avoid thresholds

11.3.2 High volume of cash based transactions

11.3.3 Source of funds to repay gambling debts

Interviewee stated that funds used to repay gambling debts by gamblers was a risk factor and that, in their experience, the US casinos were not monitoring this to the extent it could be.

11.3.4 Use of casino chips as currency outside of the casino

While there are articles citing examples of this occurring at Appendix B, this is understood be less of a factor for many of the larger casinos within Canada who have been understood to have acknowledged this risk and worked to monitor the use of their casinos chips as currency outside of the grounds of the facility.

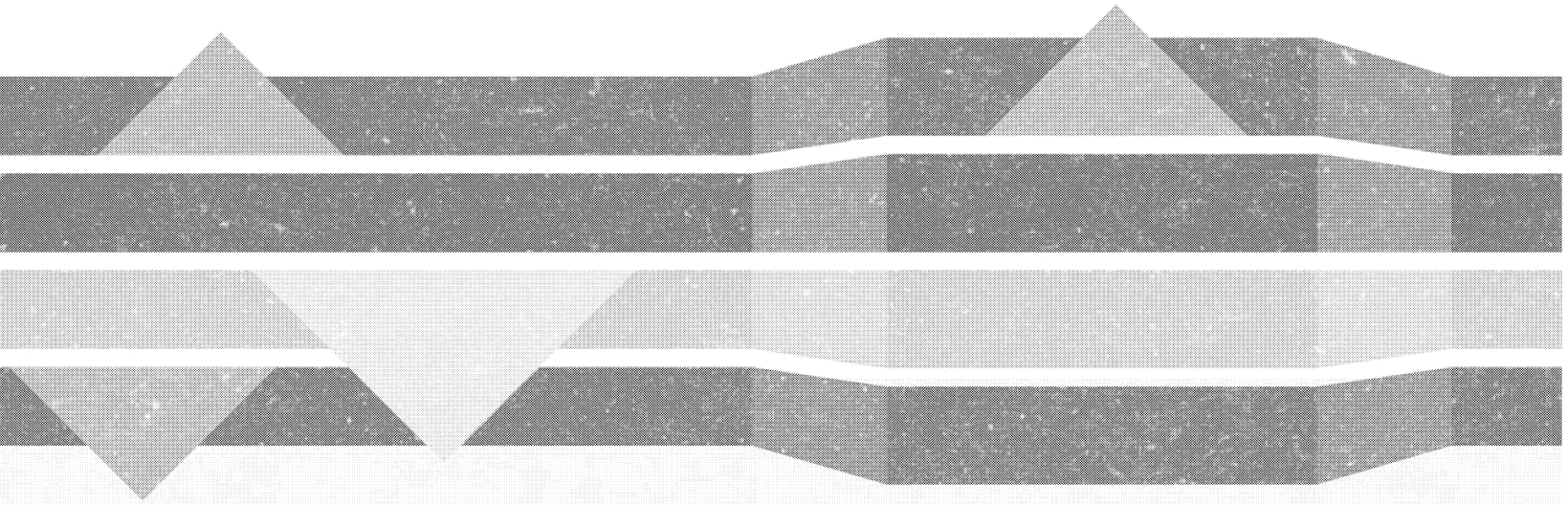
Article examples are provided at Appendix B.

Grant Thornton

Reporting Entity Sector Profile: Financial entities

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014



Appendix 9

Contents

1. General Sector Profile

The financial entities sector in Canada is dominated by the "big six" domestic banks and complemented with other domestic and foreign subsidiary banks (Schedule I and Schedule II). This sector also includes trust companies and loan companies, which operate under federal or provincial legislation. Credit unions, caisses populaires, financial cooperatives and the credit union centrals, which are also considered financial entities, are addressed separately.

There are a total of 80 banks regulated by the Office of the Superintendent of Financial Institutions (OSFI)[1]. The banking sector ranges from retail branch operations to commercial banking and lending to representative offices of foreign banks.

With low interest rates in a highly competitive and saturated market, resulting in low rates of return on lending products, the banking sector is consolidating. For example the big six acquiring the operations of smaller players, including Scotiabank's acquisition of ING Direct and Royal Bank of Canada purchasing Ally Canada.

Other financial sector organizations that are not considered as financial entities for the purpose of this report include Schedule III banks, private lenders, payday lenders and virtual currency providers.

A significant number of risk factors have been identified and these are detailed later in this document, some of the key factors are listed below:

- Exiting high risk client relationships
- Wealth management and private banking
- Trade finance and trade-based money laundering
- Foreign operations, including those that are headquartered in a foreign jurisdiction and banks that are Canadian with foreign branches
- New technologies
- Omnibus accounts

[1] OSFI - http://www.osfi-bsif.gc.ca/

2. Structure, size and segmentation, reporting entity population

The Canadian financial entities industry is dominated by the big six banks. In addition to competition, the barriers to entry are high, given the large capital and expense outlay and the resources required to meet the licensing requirements of OSFI. Competition is high as services converge and all financial entities compete for the same customer amongst the banks, credit unions, securities dealers and insurance companies.

2.1 Domestic banks (Schedule I)

Schedule I banks are domestic banks that are authorized under the Bank Act to accept deposits and may be eligible for deposit insurance from the Canadian Deposit Insurance Corporation (CDIC). There are a total of 29 domestic banks – the big six banks – Royal Bank of Canada, Toronto Dominion Bank, Bank of Nova Scotia, Bank of Montreal, CIBC and National Bank of Canada, account for 90% of the total assets in deposit taking institutions[2]

Banks contribute approximately 3% to Canada's GDP and employ over 275,000 Canadians[3].

The big six banks have significant retail branches across Canada – in total there are more than 6,000 branches[4] – and several of these banks have large international operations, serving clients globally with investing, account services and wealth management.

During the first fiscal quarter of 2014, stress tests indicated that four of the big banks had common equity capital ratios higher than what was required, exceeding capital targets. For the sixth year in the row, Canada's banks have been ranked the world's soundest by the World Economic Forum.[5]

Within Canada, the big six banks offer diversified services including deposit accounts, lending, investment banking and wealth management. Smaller domestic banks provide services to niche markets such as online banking, foreign exchange services, or catering to certain market segments and generally have less, if any bricks-and-mortar retail operations.

[2] Ibid
[3] Canadian Bankers Association – "Banks and the Economy"
[4] Ibid
[5] National Post – "Canadian Banks win top marks from World Economic Forum", September 4, 2013

2.2 Foreign subsidiary branches (Schedule II)

A total of 24 foreign banks are authorized under the Bank Act to accept deposits. The largest of these banks, for example HSBC, have global operations and head offices in a foreign jurisdiction. Foreign banks generally provide similar services as those of the domestic banks.

Foreign subsidiary branches operating in Canada generally follow customer identification (CID) requirements of the head office or Canada, whichever has the more strict requirements. However, in the past, some banks have been known to utilize foreign branch operations to make introductions and avoid the domestic countries' CID.

2.3 Foreign bank branches (Schedule III)

Schedule III foreign bank branches, which are not considered to be financial entities under the PCMLTFA, are authorized under the Bank Act to operate, but with restrictions. These restrictions vary, depending on the bank's Canadian activities and service offerings and may include one of the following:

- Restriction on accepting deposits (of any dollar amount) and only allow borrowing from other financial institutions;
- Restrict deposits to a minimum of $150,000 per deposit; or
- To establish representative offices where no banking is permitted.

2.4 Trust companies

Trust companies are regulated under the federal Trust and Loan Companies Act and provide services similar to those of a bank. However, where banks are not permitted to administer estates, trusts, pension plans and agency contracts, trust companies are.

OSFI regulates 44 trust companies in Canada, most of which are associated with banks.

2.5 Loan companies

There are 19 loan companies that operate under federal or provincial legislation and provide services similar to those of banks. Loan companies are also regulated under the federal Trust and Loan Companies Act.

2.6 Products and services

Banks offer a range of services including retail banking, wealth management, credit card services and lending. Besides their traditional offerings, banks are beginning to grow outside of their non-core banking services, for example, advisory services in capital markets, financial planning.

The variety of products and services is dependent on the size of the organization and the client segment it services. In general, products and services in the banking sector are divided by personal banking, business banking, consumer and real estate lending. Banks offer:

2.6.1 Personal banking

Personal banking products and services are expected to account for a quarter of the industry's revenue[6] consisting of savings and chequing accounts and term deposits which provide banks with liquidity and interest revenue. Bank accounts also provide the opportunity for banks to earn account and transaction related revenue from consumers.

2.6.2 Commercial banking sector

Similar to personal banking, commercial banking includes providing account and transaction services to Canadian companies as well as commercial lending.

2.6.3 Consumer loans and real estate lending

Consumer loans and real estate lending include personal lines of credit, auto loans, home equity loans and home mortgages.

While the industry faces low interest rates that have reduced the income from lending, demand for personal loans is high and increased 3.9% from 2012 to 2013[7].

2.6.4 Revenue from other services

Other revenues earned in the banking sector include commissions from sale of mutual funds, insurance products and credit card revenue.

2.6.5 Access channels

While not new, customers are increasingly using online banking services, with 67% using online banking to pay bills[8]. In order to remain competitive, banks continue to develop new methods for customers to access banking. Recent examples include electronic cheque deposit, cloud and electronic wallet payment services.

---

[6] IBISWorld Industry Report – Commercial Banking in Canada, March 2014
[7] IBISWorld Industry Report – Commercial Banking in Canada, March 2014
[8] Canadian Bankers Association

3. Regulation of banks

OSFI, an independent agency of the government of Canada, supervises and regulates banks to instill public confidence by ensuring that the risk of losses by depositors is kept minimal. These risks are monitored by reviewing and providing guidance, interpreting legislation and monitoring the financial and economic environment that may affect financial entities.

Trust and loan companies operate under federal and provincial legislation but are also regulated by OSFI.

In 2012, OSFI adopted the Basel III capital rules that help banks improve financial stability by raising quality and quantity of capital to shield the banks from economic shocks. As a result of these changes, there will be increased compliance costs. While Canadian banks have exceeded the ratios currently required and in some instances met the capital ratio requirements ahead of schedule, this further builds the reputation of Canadian banks and allows them the flexibility to make strategic acquisitions. However, this also constrains their profitability, compared with their global peers.

4. Constraints

High barriers to entry with well-established, heavily capitalized and marketed banks; barriers to entry include large capital outlay, costs to seek banking license and time to market.

5. Description of sector associations

- *Canadian Bankers Association* – a voluntary organization that works with Canadian domestic bank, foreign bank subsidiaries and foreign bank branches to lobby the government and promote financial literacy amongst Canadians.
- *Canadian Bankers Association's Bank Crime Prevention and Investigation Office (BCPIO)* – coordinates the banking industry's crime investigation and prevention activities and protects banks customers against financial crime.
- *Institute of Canadian Bankers* – is a private membership community for the Canadian banking industry.
- *Canadian Coalition for Good Governance* – represents Canadian institutional shareholders in the promotion of corporate governance practices that best align the interests of boards and management with those of the shareholder.
- *Canadian Bank Machine Association* – With operations in more than 1,500 rural and urban areas across Canada, the CBMA and its member organizations provide Canadians with convenient and alternative access to currency.
- *ATM Industry Association (ATMIA)* – is an independent, non-profit trade association, which works to promote ATM convenience, growth and usage worldwide, to protect the ATM industry's assets, interests, good name and public trust, and to provide education, best practices, political voice and networking opportunities for member organizations.
- *Interac Association* – Interac Association is responsible for the development and operations of the Interac network, a national payment network that allows Canadians to access their money through Interac Cash at 60,000 Automated Banking Machines and Interac Debit at 766,000 point-of-sale terminals across Canada.

6. Emerging business trends

Canada hopes to become North America's first primary centre for trading the Chinese yuan (RMB). While trading centres have been established in other cities internationally, North America does not currently have a trading centre. Establishing the centre will allow Canada and China to buy and sell each other's currency quickly.

- Due to the difficulty and/or expense of transaction monitoring, financial institutions are refusing to provide banking to certain client groups. In other cases, banks have also identified potential reputational risk and higher risk of fraud in certain sectors. As a result, certain industries have difficulty establishing or maintaining bank accounts (i.e. being debanked) including those related to/associated with diplomats/embassies, MSB's, legal marijuana merchants, payday loan companies, cheque cashing companies, virtual currency merchants.

- Banks are increasingly adopting new technologies to service customers, for example electronic cheque deposits and mobile payment services. These technologies can expose the bank to greater fraud risk, e.g. cyber-crime is currently one of the leading headlines in the world of frauds, investigations and IT security issues.

- *Banking Bitcoin* - there has been much in the news over the last year and a half regarding Bitcoin and also Bitcoin exchangers. Typically Bitcoin exchangers need a bank account as they provide a service which converts money into Bitcoin and vice versa. Banks have had real challenges with having to understand the technology, the business and what the risks are to banking a Bitcoin exchange business, how to provide services and monitor appropriately.

7. Type of customer(s)

Canadian financial entities serve a diversity of customers, both individuals and entity customers. There are no exact numbers on the number and types of clients, however, it is expected that almost 80% of revenue is anticipated to be from personal clients[9].

Clients at some of the big six banks are serviced according to the client's complexity of needs as well as asset level. For instance, clients that require more sophisticated financial planning and/or have significant investible assets will be provided greater personalized service.

As the big six banks are geographically located throughout Canada with concentration in the major metropolitan areas, customers are generally from the same geographical area. Canadian banks that are internet-based generally do not permit non-Canadians to open accounts in order to meet customer identification requirements.

In order to identify new opportunities, some banks have their representatives attend industry conferences around the world to attract new clients and maintain the accounts of existing clients. As a result, there is more and/or continued focus on servicing clients beyond Canadian borders with their global banking needs.

[9] IBISWorld Industry Report – Commercial Banking in Canada, March 2014

8. Key points from interviews

8.1 Discussion with senior compliance officers of banks

The Basel January 2014 paper on AML management lays out priorities and there are at least a couple of good points in here.

These are the three pillars for large financial services organization to manage AML risk and they need to do each of the following:

- Develop consolidated KYC systems across all business lines and geographies. Some banks are doing this already for specific lines of business, e.g. capital markets but very few today are there across all operations and some are only just starting.
- Develop consolidated group wide monitoring for all products / services / geographies / groups, etc. All the larger banks around the world are at different stages of doing this.
- Develop consolidated high risk management, global for AML compliance.

There are many challenges for a financial institution to overcome before being able to accomplish above – these are money, time, privacy, data systems and legacy systems. Buy in is needed from the governance of the organization. Big Data and data integrity are issues. Close to 90% of the data privacy issues can be overcome for the most part through client consent agreements.

Data protection is important and involves issues around the movement of data that the large banks are exploring… "I can share data but I can't move data". Organizations need to look at options to bring data together to monitor or analyze virtually, so that the bank can look, see and then put the data back.

- These projects are multi-year projects, two plus years and project management is key. There is value to doing this, however:
- The consolidation of the data and analysis is identifying new risks, risks that the local units were not aware of, and don't even know to look for.
- Rules can be applied consistently over many units and globally and data integrity can be checked.
- Always need to include local risks / operations to integrate with what is being done at the global level. Must appreciate local knowledge so that you don't become generic.
- Opportunity for the development of more complex rules to query and analyze the data.

Transaction monitoring used to be transaction-centric, then client-centric (profile the client) and now the focus is on client networks.

In the large bank environment, the business unit (profit centre) always owns the risk. AML compliance must challenge the business – must be part of an effective program. Who calls the shots at end of the day: in our bank

there is a reputational risk committee, made up of persons internal to the bank. The reputational risk committee can make decisions to not bank and exit relationships.

The primary focus of regulation in investments securities is investor protection – market manipulation etc. From an AML perspective the organization doesn't really need to do anything different, than what is already being done elsewhere – Need to apply the context and look for flows of funds. However, this is different from investor protection.

Need to know the client's clients. This day will come for securities sector but it is currently not here yet.

The big challenge seems to be the ever increasing regulatory pressure and expectation. There is a lot of infrastructure and investment being made and lots of resources spent. There are good intentions but the reality is that effective monitoring of transactions and client activity cannot be done in a rules-based, super-proceduralized, perfectly auditable. The interviewee thinks a lot of time is spent pointlessly – running rules and investigating alerts and coming up with nothing. Investigations are and should be more complex. Also, by putting pressure on the banks, the banks are declining clients such as MSBs which is simply sending them to other avenues and sending tricky clients underground.

The main issue with AML in Canada is lack of prosecution/investigation/ enforcement. So, the Banks can spend millions upon millions and send millions of reports to FINTRAC but if down the line the RCMP has 10 officers in the whole country to work them, what's the point? It would be better to give the RCMP more money difference is to be actually made.

8.2 Risk areas

- The wealth management side of the business is built and sold based on privacy. There are real struggles to overcome these hurdles internally as there are still issues with people on the ground in all the various locations.

- Smaller institutions are always inherently conflicted – would need an independent board to counterbalance the inherent risk – "How do you say no to business when you need to deliver results?"

- Trade Finance has been an issue for years - How does a large bank find trade-based money laundering? The bank asks and sees bills of lading but so what? Money moves to China, good move to Canada, does the bank need to monitor the price of sparkplugs? What is the bank's role in all this? Is all the data easily available to the bank? Not necessarily and not sure how to resolve.

- The unintended consequences of these (AML compliance) regimes: the big banks end up saying no to certain line of business, certain customers and these groups become unbanked… could be specific customers, specific products e.g. the wealth management business in Latin America, the banks are out of this sector in certain countries. So, new business is now going to the MSB's and the credit unions. Money laundering going undercover.

- What does this lead to (major countries being sanctioned)? We are (current regimes) moving the problem – we are not solving it; because it comes down to reputational risk for larger banks. What's wrong with Big Canadian bank "laundering" – we want to work with law enforcement. We (the big bank) can find it, can trust us, if the money laundering moves to smaller corner stores, to other countries, we won't be able to find it, won't be able to trust the parties when you start to go after it.

- *Other risks – increasing extra-territoriality.* Experiencing some challenges now with being a Canadian "branch" of a US institution and having to comply with OFAC requirements. But, I don't think that is limited to my bank. I think the world is shrinking and requirements are more far reaching and complex.

- Who is responsible within a Canadian-regulated FI conglomerate for an offshore account? It depends and there is no clear answer. When a customer wants to access from a services perspective, all of banks doors are open; when there is litigation or regulatory oversight, all the doors close.

8.3 Discussion regarding Bank of Canada

The Bank of Canada is not subject to the PCMLTFA. It is responsible for the production and issuance of 'cash' across the country, it has the wholesaler role to distribute the cash, banknotes. The RCM does the coins. The Bank has no role or supervision for how the money is used by the banks it distributes to. Money laundering is important, but it is a secondary concern to them.

They did have cause to consider how their work was/could be used by a potential money launderer. Back in 2000, they withdrew the $1,000 note as parties were identifying it as a support to criminal activity. They reviewed and could see no economic reason to maintain the note. In the past, notes of larger amounts were used for bank settlements. No longer required so they withdrew it. The $100 note is a useful note and it is often used as a savings method. They conduct surveys to determine this.

They track the aggregate growth of banknote circulation and it has been steadily increasing. They monitor the flows, the rates and the flows of banknotes around major centres.

- Not just any bank can buy cash from there, there are specific rules before bank can have direct access to cash:
- Need to be a member of the CBA
- Must be able to settle balances in the electronic system

There are only 10 actual banks accessing, 12 are eligible; it is not closed, but criteria must be met. The 100's of smaller banks become customers of the 10 that are accessing.

They do connect with their counterparts overseas. Generally the model we follow here in Canada is the model that most around the world use. The European banks tend to be more granular, in some cases they have retail transactions.

From an operational perspective, the bank has to manage inventory. When there is unexpected activity or bank note volume, they talk to the bank, what is going on? Usually a specific situations etc. Demand spike at one bank may be because they have won a customer from another bank – cash services are a key profitable service for a bank.

Has been steady growth of bank notes. Some moderation over last few years, but over the longer term, use of cash money is up. Why? Volume of transactions is increasing. It was 48% 5 – 6 years ago, today the proportion of cash transactions is 45%. Use of cheques has dropped off considerably as there has been an increase of on-line activity.

Bitcoin is interesting – but it is not a real thing yet.

The UK central bank is required to have an AML officer – their role is somewhat different than Bank of Canada. Bank of Canada does not have an AML officer.

8.4 Discussion with compliance manager at large financial institution

Asking for AML resources is a concern – there does not seem to be enough resources – first AML, now FATCA and still to find the right skill set as well as getting approval from bank.

Banks are identifying risky areas and dealing with it. However, bankers need to be trained to identify high risk – sometimes, this is accomplished and they see that the account opening/activity should and will be stopped so it is better to ask questions up front. However, in some cases, there will be sales people that try, in futility, to override determination and ask the bank to take on a client as there is a need to make sales targets. Bankers are also more focussed on credit risk as opposed to money laundering risk.

High risk areas continue to be customer fraud on bank, for example, cheque kiting, use of complex ownership structures, mortgage fraud.

High risk areas that banks are concerned/aware of are virtual currency merchants. Also use of private lenders/financial companies, leasing companies, and the real estate sector to flow funds through. These industries are unregulated/not strongly regulated and few controls.

9. Risk factors

9.1 General market

9.1.1 Overlapping regulations

While the banking sector is heavily regulated, banks that perform multiple regulated activities and/or have worldwide operations are challenged with monitoring the global AML risks as well as the reputational and operational risks.

9.1.2 Exit of high risk relationships

Banks are making decisions to exit high risk relationships with no real resolution to money laundering – the activity is simply being shifted to other organizations where there may be little to no monitoring performed and/or the risk tolerance is higher. This view was shared by a number of the persons interviewed and there is a real concern that illegal funds in the system, if not 'banked' where it can be monitored and followed, will evade the detection and monitoring systems we have in place and be allowed to flourish. These decisions appear to be being made as Canadian banks see very real need to manage any reputational risk.

9.1.3 Transaction monitoring

Working with a number of legacy systems and across multiple jurisdictions it is a challenge to monitor all transaction data. While there is value in combining data for monitoring and analysis, this is difficult, time and resource consuming. Smaller or other organizations that do not have resources may not be undertaking this analysis. Interviewees shared that there is a wide spectrum as to how evolved some of these systems are, with apparently more on the less evolved end than the higher.

9.1.4 Competitive environment for sales to meet their targets

Sales people are inherently conflicted as they see these accounts as adding to their sales targets, of which we were told by one interviewee there continues to be significant pressure to make their numbers. For larger banks, they have resources, can make client acceptance and exit decisions through independent compliance and governance functions; smaller banks have less opportunity for this oversight

9.2 Products and services

9.2.1 Wealth management and private banking

Transactions for high net worth, private clients are highly sought after in the banking world from a sales perspective. With these types of clients it can be hard to distinguish between what is a "normal" transaction versus "atypical/suspicious transaction". Bankers may, knowingly or unknowingly, be involved with clients that are money laundering. Similar to the risk factor identified above regarding meeting sales targets, there is inherent risk with the provision of wealth management and private banking services, where often higher degrees of privacy and confidentiality are sought.

9.2.2 Trade finance/trade-based money laundering

Despite the efforts to identify, trade based money laundering is difficult to identify because the value of some goods is not easily attainable or it is difficult to establish whether dollar amounts are reasonable. There are questions as to whether the bank should be held responsible for monitoring to this level of detail. Interviewees shared that while in principal the monitoring tools and techniques available are nice, in practice this continues to be a significant risk area.

9.3 Delivery channels

9.3.1 New technologies

As banks compete to attract new and maintain existing customers, new technologies will be introduced that allow for greater anonymity of the person completing the transaction and potential for fraud.

9.4 Geography

9.4.1 Foreign operations of Canadian banks

At least some of the larger Canadian banks have a process to, or are building a process, to identify and monitor transactions globally and make sure consistency of rules. However, there has been difficulty with privacy legislation and building these systems requires significant resources.

9.4.2 Customer focus versus regulation and investigation barriers

There appears to be a real difference between first, when a customer who would like to access banking services in a number of different countries is received by the 'sales' side of a bank and introductions are made to banking contacts (within the bank's network) in a number of different countries versus second, when the regulators or authorities come knocking and have to access the bank's records and people through the walls of individual country regulations and local law enforcement. Several interviewees agreed that this is a reality- that the customer side of the bank is very service oriented, introductions are easily and quickly made, and that there are real regulatory and law enforcement challenges, including privacy laws. During interviews, we queried a number of times regarding whose responsibility it was (within a bank and from a regulator perspective) to have oversight of transactions occurring in offshore locations of Canadian banks. We did not receive a clear answer, in fact we did not receive any definitive answer, other than simply it depends.

The risk factor for money laundering and terrorist financing here is that the sales/market side of our institutions are very focused on customer service and have pressures to meet sales targets. And while there may be global monitoring and detection systems within a bank operating globally, access to these resources by regulators and law enforcement is still not clear.

9.4.3 Canadian branches of Foreign Financial Institutions

With larger global financial institutions that have minimal Canadian operations (or are considered immaterial to a global total), little and insufficient resources are being spent locally to understand AML risks both for the purposes of meeting Canadian regulations and to ensure that there are controls to mitigate/monitor the risks for the Canadian market. Organizations often utilize internal audit teams that are not trained to identify and understand AML risks and regulations.

9.5 Business relationships / linkages with other sectors

9.5.1 Use of lawyer trust accounts

Notwithstanding the challenges identified above regarding trade-based money laundering, our interviews with a lawyer identified that import/export companies use lawyers trust accounts to facilitate legitimate trade. However, the lawyer may not have sufficient knowledge of the parties and parties may use the trust account to shield the monitoring and identification of money laundering activity.

As well, interviewees shared that often they encounter challenges regarding trust accounts, in some cases that the responses to certain due diligence questions asked were subject to solicitor client privilege and therefore no specific answer was provided.

9.5.2 Omnibus accounts

Accounts for companies in other regulated sectors can pose a potential risk – while organizations would be screened to mitigate risk for the bank, how much review is performed on a regular basis, especially when there have been cases of large, international FI's involved with sanctioned activity. Examples provided at Appendix A.

9.6 Transaction methods/types

Nothing specifically identified other than what is available in much AML authoritative literature. The focus of our efforts was spent on risks seen as more structural to this sector.

Grant Thornton

Reporting Entity Sector Profile: Lawyers

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General sector profile

The legal industry in Canada is a mature and active sector with broad divisions between the criminal and the civil segments and significant division of the civil segment into specific areas of practice. Over the past decade, law firms have experienced steady and continuous growth due to expansion in international trade and the emergence of new areas of practice, particularly in business law. Demand for legal services has been facilitated by corporate restructuring, privatization, mergers and acquisitions, intellectual property rights and new financial instruments that require legal advice.

Revenue growth is expected to rise as the economy continues to recover but there is no doubt that the recession has created stress on large firms with the drop in work on M&A, IPO and other practice areas that had been significant revenue drivers. Slowing corporate profits also led to cost cutting and the impact on law firms is still being felt. Statistics Canada lists 26,997 employers and others in the sector which tallies with a recent private sector estimate of 27,215.

We have identified the following primary risk factors:

- Receipt of funds into trust account using methods and from sources unexpected;
- Nature of legal services and use of trust accounts; and
- Solicitor client privilege.

2. Structure, size and segmentation, reporting entity population

According to The Canadian Law List (A Thomson Reuters Company), there are 27,191 law firms in Canada. This number includes multiple offices in various provinces of the larger firms. The legal landscape is diverse with large national and international firms and varying sizes in-between to a significant number of sole practitioners. The last ten years has also seen a significant rise in the number of specialist boutique firms which focus on only niche practice areas such as litigation or intellectual property.

Canada's 30 largest law firms by size range from the largest with 769 lawyers to a regional firm with 118 lawyers; however, these represent a minority as the majority of lawyers work outside of these firms.[1] Law firms are heavily focussed in four provinces in particular, mirroring business and economic activity in the country with Ontario at 10,652, British Columbia at 5,126, Quebec at 4,226 and Alberta at 3,870 firms.[2]

Commercial law services make up 38% of the Canadian market and business and corporate clients over 65% of the total.[3]

[1] Lexpert
[2] Statistics Canada
[3] IBISWorld Industry Report – Law Firms in Canada, February 2013

3. Economic and financial statistics

A 2013 report identified law firm revenues in 2013 of $26.7 billion, with $5.2 billion in profits and $6.1 billion in wages. Growth is expected to improve from 2.1% in the period 2008 – 2013 to 3.6% expected growth 2013 – 2018.[4] Canadian law firms came out of the recession stronger, without significant damage to their bottom line. There has been some contraction, especially in the mid-tier firms but not as significant as that experienced in the US.

During the next five years, economic improvement, investment activity and corporate profit are expected to drive demand for legal services and revenue forecasts indicate that that revenue will increase an average 3.6% per year to $31.8 billion in the five years to 2018.[5]

[4] Ibid
[5] IBIS World Industry Report – Law Firms in Canada, February 2013

4. Regulation of the legal sector

Every lawyer in Canada and notary in Quebec is required by law to be a member of a law society and to be governed by its rules. Canada's 14 provincial and territorial law societies govern over 100,000 lawyers and 4,000 Quebec notaries in the public interest.

The Federation of Law Societies of Canada is their national coordinating body and provincial bodies are as follows:

- The Law Society of Upper Canada (Ontario)
- Law Society of British Columbia
- Law Society of Alberta
- Law Society of Saskatchewan
- Law Society of Manitoba
- Law Society of Upper Canada
- Barreau du Québec
- Chambre des notaires du Québec
- Nova Scotia Barristers' Society
- Law Society of New Brunswick
- Law Society of Prince Edward Island
- Law Society of Newfoundland and Labrador
- Law Society of Yukon
- Law Society of the Northwest Territories
- Law Society of Nunavut

Lawyers must be called to the Bar in the province that they practice in. Each province has a Legal Profession Act. In Ontario for example lawyers are governed by the Law Society of Upper Canada (legislation and rules). On top of this there are many other act and regulations that govern lawyer's professional activities.

- Law Society Act
- Barristers Act
- Solicitors Act
- Class Proceedings O. Reg. 771/92
- County and District Law Associations R.R.O. 1990, Reg. 708
- Complaints Resolution Commissioner O. Reg. 31/99
- Hearings Before the Hearing and Appeal Panels O. Reg. 167/07
- Law Foundation R.R.O. 1990, Reg. 709
- e-Laws-Gov. of Ont.
- Statutes and Regs. – Dept of Justice

5. Constraints

The Canadian Bar Association code of conduct prohibits lawyers from knowingly assisting, enabling or permitting any person to act fraudulently, dishonestly or illegally.[6]

[6] https://www.cba.org/CBA/activities/pdf/codeofconduct06.pdf

6. Description of sector associations

Our research has identified the following Canadian lawyer sector associations:

- *Canadian Bar Association (CBA)* - is a professional, voluntary organization which was formed in 1896, and incorporated by a Special Act of Parliament in 1921. Today, the Association represents some 37,000 lawyers, judges, notaries, law teachers, and law students from across Canada. 'The CBA is the essential ally and advocate of all members of the legal profession; it is the voice for all members of the profession and its primary purpose is to serve its members.' The CBA has branches in each of the provinces and territories (e.g. Ontario Bar Association).

- *Criminal Lawyers Association* - is one of the largest specialty legal organizations in Canada, with more than 1,000 members. 'We are a voice for criminal justice and civil liberties in Canada.'

- *Canadian Defence Lawyers* - Canadian Defence Lawyers is the only national organization representing the interests of civil defence lawyers.

- *Canadian Maritime Law Association (CMLA)* - Members of the CMLA include practicing maritime lawyers and other persons, companies and groups interested in the shipping and maritime industry. The mandate of the CMLA is to advance the development of effective, modern commercial maritime law within Canada and internationally.

- *Ad IDEM - Canadian Media Lawyers Association* - Ad IDEM stands for Advocates in Defence of Expression in Media. Members are leading media lawyers across Canada.

- *Indigenous Bar Association* - One of the primary goals and objectives of the Indigenous Bar Association is the promotion and reform of policies and laws affecting Indigenous Peoples in Canada.

- *National Association of Women and the Law*- is an incorporated not-for-profit organization that promotes the equality rights of Canadian women through legal education, research, and law reform advocacy.

- *International Law Association (ILA) – Canadian Branch* - The ILA was founded in Brussels in 1873. The ILA now has some 3,500 members in 45 national and regional branches around the world. The ILA has consultative status as an international non-government organization with a number of the United Nations specialized agencies.

- *Canadian Association of Refugees Lawyers* - Founded in 2011, the Canadian Association of Refugee Lawyers serves as an informed national voice on refugee law and human rights, and promotes just and consistent practices in the treatment of refugees in Canada.

- *The Refugee Lawyers' Association* - of Ontario is an association of approximately 200 lawyers in the Province of Ontario in Canada advocating on behalf of refugees.

- *Canadian Association of Labour Lawyers* - was created in the late 1980's. Its approximately 250 members are all lawyers who represent the labour movement across Canada. They practice in law firms or as employees of labour organizations.

- *Canadian Association of Provincial Court Judges* – is a federation of provincial and territorial judges' associations. Founded in 1973, its membership now includes most of the over 1,000 provincial and territorial judges in Canada.

- *Canadian Civil Liberties Association (CCLA)* – Since 1964, CCLA has defended the fundamental human rights and civil liberties of all Canadians through public education, litigation, citizen's engagement and monitoring and research

- *Canadian Superior Court Judges Association* - represents approximately 1,000 judges who serve on the superior courts and courts of appeal of each province and territory, as well as on the Federal Court of Canada, the Federal Court of Appeal and the Tax Court of Canada.

- *Association of Corporate Counsel* - is a global bar association that promotes the common professional and business interests of in-house counsel who work for corporations, associations and other private-sector organizations through information, education, networking opportunities and advocacy initiatives.

- *Canadian Muslim Lawyers Association* - The CMLA represents Muslim individuals of all backgrounds who are in the legal profession in Canada. 'We exist to interact with and assist Muslim lawyers, law students, the Muslim community, the legal profession and the public at large in various capacities, offering, professional advocacy, education, networking and peer support.'

- *Canadian Lawyers for International Human Rights (CLAIHR)* – is an organization that has been raising awareness and promoting human rights within Canada and abroad for over 18 years.

- *Hellenic Canadian Lawyers Association* - is a national non-profit organization founded in 1982. Its primary purpose is to maintain a reliable network of lawyers, judges and law students of Hellenic origin.

- *Iranian Canadian Lawyers Association (ICLA)* - is a legal advocacy group that was formed in November 2002 by a group of like-minded lawyers and law students of Iranian heritage. The establishment of ICLA was in part a necessary corollary of the burgeoning community of lawyers of Iranian heritage throughout Canada.

- *Canadian Association of Black Lawyers (CABL)* - formed in March 1996, is a national network of law professionals and individuals committed to reinvesting in the community. CABL's continuing goal is to bring together law professionals and other interested members of the community from across Canada to cultivate and maintain the Association of Black professionals in Canada.

- *Canadian German Lawyers Association* - The Canadian German Lawyers Association was set up in 1992 in Germany as a non-profit organization to bring together Canadian lawyers who act on behalf of German speaking clients, German Rechtsanwälte who represent Canadian clients, as well as members of the German Canadian business and professional community.

- *Korean Canadian Lawyers Association (KCLA)* - The objectives of the KCLA include the promotion of professional and social interaction between its members; the promotion and advancement of the well-being of the Korean Canadian community; the promotion of legal education to members of the Korean Canadian community; and promotion of understanding and awareness of the nature of the legal profession.

- *Legal Aid Ontario* - In 1998, the Ontario government enacted the Legal Aid Services Act in which the province renewed and strengthened its commitment to legal aid. The Act established Legal Aid Ontario, an independent but publicly funded and publicly accountable non-profit corporation, to administer the province's legal aid program.

- *Law Help Ontario* - Law Help Ontario is a project of Pro Bono Law Ontario that provides pro bono legal services to people who cannot afford to hire a lawyer and are unrepresented in a legal matter. The project is currently piloting two self-help centres in courthouses in the Toronto area. In the future, centres may be launched in other locations across Ontario.

7. Emerging business trends

Law firms in Canada are showing clear sign that the industry is in a state of flux. There have been a number of mergers e.g. that of Ogilvie Renault and McLeod Dixon, both of which joined a UK based law firm, Norton Rose. The firm subsequently merged with U.S. based Fulbright & Jaworski to become Norton Rose Fulbright and Fraser Milner Casgrain joined with SNR Dentons. In both cases, one of the factors at play appears to have been size in the global marketplace. As well as this, other law firms, particularly the mid-tier firms are believed to be under considerable financial pressure and the recent failure of Heenan Blaikie, a prestigious law firm is the most recent example. Canadian law firms are of interest to UK and US firms because of the mining, energy and natural resources markets.

Another recent trend that appears to be gathering momentum is proposed changes to legal billing practices. Clients want to pay less and don't want to pay by the hour; they want to pay for results. The hourly system is viewed as inefficient and law firms are looking at ways in which it can be improved on. One new example is Cognition LLP which is shaking up the market with new ways of providing legal services, such as fixed-fee services as alternative fee arrangements. For example, a law firm could charge a client a flat fee for a particular service, such as a corporate acquisition, no matter how many hours it ends up taking essentially spreading more risk from the client to the law firm.

Bay Street law firms are also increasingly looking to outsource, either to lower-cost legal-service providers in Canada or new overseas providers in India, for rote legal tasks that before would have been done in-house. The savings, in many cases, are being passed onto clients.

McCarthy Tétrault LLP partner Matthew Peters, who is the firm's national leader for markets, says there is a transformation under way. The traditional law firm, with its pyramid of associates and partners all charging clients hundreds of dollars an hour, is headed for history's dustbin. High-end law firms, such as McCarthys, will specialize in complex legal work and farm out the rest to the equivalent of legal factory production lines.[7]

Companies are more likely to engage in high-cost litigation when corporate profit is high. Furthermore, strong corporate profit stimulates initial public offerings, merger and acquisition activity and capital raisings, which all require the services of law firms. Corporate profit is expected to increase representing a potential opportunity for the industry.

[7] The Globe and Mail – "The end of the billable hour? Firms and clients look beyond traditional billing to new cost-saving arrangements, such as outsourcing", November 28, 2013.

Solicitor client privilege issues and challenges: A discussion paper prepared by the CBA outlines and discusses a number of issues regarding solicitor client privilege in Canada and reviews how privilege is used around the world and different from the Canadian context. The CBA outlined the challenge as follows: "…to consider how this ancient concept which is a fundamental part of the administration of justice should apply and adapt to the changes of the 21st century." And observed, "We live in an increasingly globalized legal world and Canadian law on the Privilege differs in significant respects from other jurisdictions which are important both in terms of their influence on Canadian law and our clients' interactions. Moreover, the law and practice in these jurisdictions, especially the United States, shows that in Canada there are many Privilege issues that remain unresolved."[8]

[8] Solicitor Client Privilege in Canada, Challenges for the 21st Century, Discussion Paper for the Canadian Bar Association, February 2011

8. Products and services offered

Lawyers and law firms in Canada provide a very wide range of services, with the larger firms providing much of the full ranges of services. Some smaller boutique firms specialize in only one practice area as a speciality, for example, litigation.

The range of services encompasses the following[9]:

- Aboriginal Law
- Advertising, Marketing and Regulatory Affairs
- Asia
- Asset-based Lending
- Automotive
- Banking and Financial Services
- Business and Corporate Commercial
- C2D
- Capital Markets
- Charities & Not-For-Profit Organizations
- Chemicals Group
- China and Southeast Asia
- Civil Fraud
- Class Actions
- Cleantech
- Climate Change and Emissions Trading
- Commercial Insurance
- Commercial Leasing
- Commercial Litigation
- Commercial Real Estate
- Competition Law / Antitrust
- Construction and Engineering
- Copyright Law
- Corporate Commercial Litigation and Arbitration
- Corporate Finance and Securities
- Corporate Governance
- Corporate Lending and Project Finance
- Crisis Management
- Defamation & Media
- Defence, Security and Aerospace
- Insurance and Tort Liability
- Intellectual Property
- International Trade and Investment Law
- Labour and Employment
- Latin America
- Legal Translation Services
- Life Sciences
- Litigation and Arbitration
- Manufacturing, Sales and Distribution
- Marketing and Distribution
- Medical Defence Group
- Mergers and Acquisitions
- Mining
- Mortgage Recovery Services
- Municipal Law and Other Government
- Nuclear
- Occupational Health & Safety
- Oil & Gas
- Outsourcing
- Patents
- Pension Fund Investment
- Pensions and Benefits
- Plan Nord
- Privacy and Access to Information
- Private Equity & Venture Capital
- Procurement
- Product Liability
- Project Finance
- Public- Private Partnerships/Alternative Financing
- Public Policy and Government Relations

[9] Services identified from websites of Canadian larger law firms.

- Discovery Management
- Distressed M&A
- Doing Business in Canada
- Drug Pricing & Reimbursement Group
- Educational Institutions/Universities & Colleges
- Electricity
- Employment & Labour Law
- Energy
- Entertainment Law
- Environmental
- Executive Compensation
- Family Law
- Financial Services Regulatory
- Food & Natural Health Products Law
- Foreign Investment/Investment Canada
- Franchise and Distribution Law
- Gaming Law
- Government and public policy
- Hardware, Software and Semiconductor Manufacturers
- Health Law
- Immigration Law
- Income Funds and REITs
- Infrastructure
- Insolvency and Restructuring
- Insurance - Corporate and Regulatory
- Real Estate
- Urban Development
- Regulatory Investigations
- Renewable Energy
- Research
- Restructuring, Bankruptcy & Insolvency
- Retail Services
- Risk Management and Crisis Response
- Russia and the CIS
- Securities, Capital Markets and Public Companies
- Securitization and Structured Finance
- Shareholder Activism
- Succession Planning & Estates
- Supreme Court of Canada Services
- Tax Dispute Resolution
- Technology
- Trade-marks
- Transfer Pricing
- Translation
- Transportation and Logistics
- Trusts and Estates
- U.S./Cross-Border
- Wealth Management
- Wireless Communications
- XClaimTM - Portfolio Claims Management

9. Type of customer(s)

Business clients are believed to make up over 65% of law firm clients and it is clear that business and commercial activity requires the most legal services. Individuals are also significant users of legal services for personal issues such as wills, trusts, divorce, tax and financial related advice being top issues. The Canadian legal market is focussed primarily on residents but there is no doubt that local law firms, especially those with foreign offices also provide advice to companies and individuals outside the country. The increase in global economic activity and Canada's primacy in mining, resources and energy are all significant drivers of such legal activity.

10. Geographic considerations

Lawyers are only allowed to practice at the bar in the geographic area where they are called. In practice this means court work and legal advice, more often does not include litigation. So in practice, lawyers operate locally and regionally based on the needs of their clients but can also advise on issues nationally. When court work is required, lawyers engage local expertise. On a global basis, a similar pattern is used, giving the larger international firms an advantage in countries where they have operations.

11. Key points from interviews

Interviews with our global Grant Thornton contacts identified a number of cases involving both notaries and lawyers. These sources indicate that trust accounts and cash payments were a factor in each case, although, as in Canada, the use of cash is gradually being reduced. Lawyers acting as agents for individuals in a range of transactions is also a common situation which has also been identified as a money laundering risk.

- CBA is the governing body, the umbrella organization; lawyers are regulated provincially across the country.
- What kind of services do accounting firms provide to law firms/lawyers? Accounting firms provide audit work, assurance, tax compliance work including partnership tax filings, personal tax work, tax planning structures for the partnerships and partners, provide assistance with any merger & acquisition activity. Accounting firms generally have client referral relationships with law firms.
- Has seen a number of cases in smaller law firms and also sole proprietorships involving lawyers stealing money from clients. Often the law society gets involved and if they need an accountant to assist, they hire one. The larger firms have more controls in place over trust accounts, more monitoring and procedures in place.
- Lawyers are required to have an independent review of their trust accounts every year. The example below is from the province of Nova Scotia, but we understand it is similar across the country. The required review is in three parts:

    1. Law firm completes the review form, and this is submitted to the Law Society;
    2. Accounting firm completes a review form; and
    3. The third part is completed if parts one and two do not agree

- The review form is then provided direct to the law society, this is usually done by the assurance provider, e.g. the accounting firm.
- Complaints from lawyers regarding other lawyers or complaints received from clients are made to the Barristers Society, or the provincial equivalent. It is dealt with through their process and an investigator is hired to assist if required. Sometimes this investigator is an accountant.
- Lawyers must be called to the bar in the province they are practicing in. However, lawyers are permitted to practice outside of their province up to a certain number of days (not that many). This will depend on the province, and you would want to call the law society of the province that you are interested in.

- Anyone can file court documents anywhere. In fact, most filing is done by paralegals and legal assistants, as well as by hired agents. A lawyer can file something out of province and then hire a local agent to appear on the matter. The registries are generally quite helpful.

- There are significant fee pressures coming from clients, we can no longer bill as we have done in the past, need to figure out value billing and how do we apply that to the work of legal services? The answers are not clear. Clients are no longer loyal to a firm; they shop around for the best fees. The market is very competitive.

Discussion notes with sole practitioner:

AML area is focussed on cash – accordingly, there are limits to acceptable amounts of cash. The Law Society provides guidance to amount of cash accepted. Lawyers are aware of these rules and therefore are watching out.

Areas of higher risk are where private lenders are involved – lawyers have no idea where source of money is coming from or necessarily the people behind the organization.

There are also instances where straw purchasers are involved – the straw purchaser will buy property and get mortgage. Mortgage is paid off quickly and home is sold for profit and money launderers are not only able to clean the money but also make money in a rising property market. Lawyer does not see source of funds as money can come from bank draft.

Lawyer's privilege will shield transactions – a lawyer, in his professional capacity as a legal professional, may not disclose/report crimes unless someone's life is in imminent danger. Privilege would apply to clients and 'non-clients' (i.e. do not have to have an engagement letter.)

Another opportunity is the involvement of the lawyer in an import/export transaction:

- Interviewee was once approached by a domestic company to hold funds in trust for an import/export transaction as per an agreement. Under the agreement, the interviewee would hold the funds until the seller shipped goods and buyer confirmed receipt of goods.

- While this can be a typical transaction, the interviewee was approached with the details of the transaction already setup – typically, lawyer is involved to structure and advise on transactions but in this case, all details had already been negotiated.

- The transaction dollar amount was also abnormally large to approach a sole practitioner to handle – these are usually handled by larger firms. In the end, interviewee declined transaction as there were a number of issues, including an increase in insurance premiums for the transaction.

- Interviewee also stated that the problem with this transaction was that a lawyer would not know whether goods were actually shipped – he is taking the word of the receiver that goods had been delivered.

12. Risk factors

12.1 General market factors

12.1.1 Market competitiveness and pressure on fees

While the CBA code of conduct prohibits lawyers from 'knowingly assisting, enabling or permitting any person to act fraudulently, dishonestly or illegally' there are clearly situations where it is not 'known' this is the case and there is market competitiveness and fee pressure, especially on the mid-tier firms.

12.1.2 Knowledge of client

Lawyers may not have or want full knowledge of all parties that they work with and the source of funds that are involved. A lawyer faces reputational risk however, there have been instances where lawyers are involved in transactions without sufficient knowledge of the client or, even after becoming aware of a client's questionable background, continued to provide services.

12.1.3 Lawyer as a gatekeeper

Legal professionals are approached and, knowingly or unknowingly, may be involved with setting up entities for the purposes of money laundering. Examples provided at Appendix B.

12.2 Product and service factors

12.2.1 Nature of services and use of trust accounts

Lawyers, through the various services they provide and their legal and business expertise, are sought after by those desiring to launder funds. Because money laundering is a process which seeks confidentiality/anonymity, legal services can be involved in the process both wittingly and unwittingly. International sector experts and investigators shared that they were aware of a number of cases wherein legal services had been used, including the use of a trust account, to assist money laundering operations.

12.2.2 Solicitor client privilege

Solicitor client privilege provides the client with confidentiality where legal advice of any kind is sought from a professional legal adviser unless that privilege is waived. To the extent that privilege is used to hide the true nature of sources and/or uses of funds and/or persons involved in companies and transactions, this provides real risk for money laundering and terrorist financing.

12.2.3 Work involving lawyer acting as agent

Lawyers that act as agents, especially for financial transactions, property purchases and other areas as identified for the other sectors. As an example, there is a case involving a lawyer setting up companies for fake mortgages and buying multiple real estate properties for a drug dealer. See Appendix B.

12.3 Delivery channel factors

12.3.1 Size of firm/independent lawyers

Smaller firms and independents are seen as more vulnerable, more likely to provide services to groups undertaking illegal/unethical activity as there is less firm infrastructure in place to monitor quality and provide oversight.

12.3.2 Lawyers who provide services outside of their areas of expertise

This is potentially an indicator that the lawyer, client relationship is not service driven.

12.4 Geography factors

12.4.1 Referrals to offshore affiliates located in higher risk jurisdictions

Clients located in high risk international locations

12.5 Business relationships/linkages with other sectors

12.5.1 Provision of legal privilege over other services e.g. Accounting

12.5.2 Privilege cited in response to banker due diligence questions

12.5.3 Higher risk real estate transactions

Lawyers who provide financial services to clients around higher risk real estate transactions have opportunity to understand the client and the source and use of the funds.

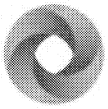
12.6 Transaction methods and types

12.6.1 Receipt of funds into trust account using methods and from sources unexpected

12.7 Client type and characteristics

12.7.1 Client characteristics

Given the nature of legal services, it is believed that many of the client type and characteristic factors, as were listed for the accounting sector, are relevant to this sector as well.



Grant Thornton

Reporting Entity Sector Profile: Money services businesses

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014

Contents

1. General Sector Profile

Canada's Money Services Businesses ("MSB") sector is an integral financial sector that provides foreign exchange, money remittance services, money orders and traveller's cheques, often to communities across the country which are not well served by banks and other financial service providers. Notwithstanding this, there are segments of the sector which are emerging rapidly, using tools like technology and online presence to provide payment processing solutions and platforms that are competing with the banking sector in niche markets.

In Canada, there are over 800 MSBs registered with FINTRAC consisting of small, owner-managed businesses to large international MSBs with significant operations in Canada. The structure of an MSB varies depending on the customers served, how customers are served (e.g. physical location and/or on-line platforms) and the reach of the business. Smaller MSBs tend to operate from one location, serving customers in the local vicinity. Larger MSBs usually have a head office, that may or may not directly serve customers, and operations include one of or a variation of wholly owned branches, agents or franchisees.

Agents are used in many ethnic-based MSBs due to their reach in the local community. Depending on the agreement, agents may or may not be exclusive to an individual MSB, meaning that they may act as agents for multiple MSBs. In many instances, the agent provides other services in addition to the MSB services, for example convenience store, grocery store, restaurant or hair salon. Franchisees, which operate as a separate business, would typically be registered as an MSB or as an agent of an MSB.

Global MSBs, whose operations are headquartered in Canada or a foreign country, traditionally have centralized compliance functions that consider both the AML requirements in the headquarters' country of domicile and Canadian regulations.

A number of risk factors have been identified and these are detailed later in this report. Factors include:

- A number of general market conditions;
- The size of the MSB and the corresponding resources particularly for larger volumes of transactions; and
- Geographic factors including transactions with overseas counterparties.

2. Structure, size, segmentation and reporting entity population

There are a total of 837 MSBs registered with FINTRAC, 36 of which have head office addresses registered outside of Canada. The highest number of registered MSBs are in Ontario, British Columbia and Quebec, which in total, account for 86% of all the MSBs across the country.

Registration of MSB	Number
Alberta	56
British Columbia	167
Manitoba	11
New Brunswick	7
Nova Scotia	2
Ontario	451
Quebec	102
Saskatchewan	5
Outside of Canada	36
Total	837

3. Economic and financial statistics

"Remittances to the developing world are expected to grow by 6.3 percent this year to $414 billion and are projected to cross the half-trillion mark by 2016".[1]

The number of Canadian sourced foreign currency and money transfer transactions is difficult to estimate given the large number of known MSBs as well as unregistered MSBs. In addition, many MSBs are privately owned and/or do not report these amounts in total or by country. Activity in the sector includes both individual consumer activity as well as business/corporate commercial activity.

The World Bank indicated that in 2013, the countries that received the highest amount of officially recorded remittances included India (estimated $71 billion), China ($60 billion), the Philippines ($26 billion), Mexico ($22 billion), Nigeria ($21 billion), and Egypt ($20 billion).[2]

We identified a number of larger known MSBs or related companies that operate in Canada and have compiled the following information:

- Paypal, a subsidiary of eBay Inc. - In fiscal 2013, Paypal performed three billion transactions generating $180 billion in net total payment volume.[3]
- Western Union - In fiscal year 2012, Western Union reported global consumer-to-consumer transfers of $79 billion, of which $71 billion related to cross border transfers.[4]
- Cambridge Mercantile Group - The Company performs $15 to $20 billion in foreign currency annually.[5]
- Moneygram - In fiscal 2013, the company reported that money transfer volume increased 18% in US outbound and 13% increase in foreign outbound sends and that revenue increased from the previous fiscal year to $1.3 billion.[6]

[1] http://www.worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank
[2] Ibid
[3] http://www.ebayinc.com/in_the_news/story/ebay-inc-reports-fourth-quarter-and-full-year-2013-results
[4] http://ir.westernunion.com/files/doc_financials/WU2012ARFinalWeb.pdf
[5] http://www.camagazine.com/archives/print-edition/2013/april/upfront/news-and-trends/camagazine73250.aspx
[6] http://files.shareholder.com/downloads/AMDA-1TA9OX/3049203675x0x658987/C9F32416-D506-4AAC-A3D2-54D8D1907E24/2012_10-K.pdf

4. Regulation of the MSB sector

MSBs in Canada are primarily regulated by FINTRAC with the exception of those operating in Quebec, which also require licensing from the Autorité des marchés financiers.

This sector has been scrutinized closely by FINTRAC and, in some cases to a larger extent, by the bankers that service the MSBs. A number of financial service providers (banks and credit unions), but not all of them, have put in place significant risk management and monitoring procedures over the accounts provided to their MSB clients. The risk management and monitoring procedures typically include ensuring that the MSB is meeting the regulations of the PCMLTFA, reviews of specific transactions and flows of funds through the accounts and due diligence regarding the ownership of the MSB business and its clients. The banking service provider as regulator has in some cases been very effective. In essence, the banks have taken significant steps to ensure that their customer chain (e.g. supply chain of customer transactions) has a level of transparency in regards to monitoring and oversight. This has become a significant constraint to the activities of the MSBs, who must now adhere to these requirements. For example, in the past, MSBs may have undertaken transactions on behalf of other MSBs who were acting on behalf of customers or groups of customers. Banking oversight has primarily disallowed this activity and demanded that MSBs only deal with customers they have direct relationships with.

MSBs which operate globally, deal with regulators specific to each local. Many MSBs operating here in Canada have operations (either through a parent, or through subsidiaries) in the United States and thus are dealing with state regulators and licensing requirements.

To the extent an MSB also provides cheque cashing and payday loan services, the following apply:

- Bill C-26, Criminal Interest Rate[7]
- Ontario – Payday Loans Act, 2008
- Saskatchewan - The Payday Loans Act 2012
- Alberta – Fair Trading Act - Payday Loans Regulation 157/2009
- British Columbia - Business Practices and Consumer Protection Act – Payday Loans Regulation 57/2009
- New Brunswick – Bill 4 - An Act Respecting Payday loans - Cost of Credit Disclosure and Payday Loans Act, 2008-4-30
- Manitoba – The Consumer Protection Act – Payday Loans Regulation 50/2010
- Nova Scotia – Consumer Protection Act - Payday Lenders Regulations (Section 18U), R.S.N.S. 1989, c. 92
- Prince Edward Island – Bill 69 - Payday Loans Act – May 2009

[7] http://www.cpla-acps.ca/english/reports/C-26%20Eng.pdf

5. Constraints

In addition to the regulations, as described above, we noted the following:

- Vital to the operations of many MSBs, banking facilities provides the company with account, wire transfer, foreign exchange services as well as the ability to accept payment other than cash. Accordingly, without banking, many MSBs are crippled and/or can no longer operate.

- The current regulatory customer identification requirements assume that the MSB's customer is Canadian or physically located within Canada. As operations become increasingly international in nature and the use of online platforms for the provision of these services becomes more popular, the MSB sector needs to effectively address this requirement. The regulatory requirements do not make exceptions or currently provide guidance on how to this.

6. Description of sector associations

Our research has identified the following Canadian and International MSB related associations:

- *Canadian MSB Association* - "The Canadian MSB Association's mission is to provide a channel for organizations who are governed by payments compliance regulations within Canada." - http://canadamsb.org/aboutus/
- *Canadian Payday Loan Association* - The Canadian Payday Loan Association (CPLA) represents the majority of licensed payday lenders in Canada. CPLA works to ensure payday loan companies hold themselves to a higher standard of responsible service and to help customers make informed financial decisions. CPLA is the national trade association for companies that provide Canadians with short-term loans or payday advances in small amounts to help cover unanticipated expenses. - http://www.cpla-acps.ca
- *Community Financial Services Association of America* - CFSA is the only national membership trade association that provides services exclusively to the payday advance industry. Members represent nearly two-thirds of this market segment with more than 8,000 stores nationwide. CFSA is actively involved with policy makers to promote legislation and regulation that balances the interests of members with substantive consumer protections that ensure responsible and informed use of the product. - www.cfsa.net
- *Money Service Business Association of Canada* - the Money Service Business Association of Canada was established in 2011 by a group of MSBs who shared a common interest in compliance and a desire to maintain harmonious relationships with Canadian banks. The association is intended to unify MSBs in order to bring mutual benefit to MSBs, their banks, the regulators by whom they are both regulated, and the communities they serve. - http://www.msbac.ca
- *National Money Transmitters Association (North America)* - "The National Money Transmitters Association is the only broad-based group representing the state-licensed money transmitters of the United States. Our mission is to promote rational regulatory policy, industry compliance with all applicable laws, consumer protection and fair conditions for competition." - http://www.nmta.us/site/page.php?240

7. Emerging business trends

Our research and discussions have identified the following emerging trends:

- *Online Technologies and Virtual Payment Networks* – Companies are increasingly providing their services over the internet and through mobile applications. This permits companies to serve a greater number of customers without the setup of agents and branches.

- *Virtual Currencies and Virtual Payment Networks* – Virtual currencies are becoming mainstream with high profile investors and media exposure on a daily basis. The ease of use and relatively unregulated area of virtual currencies and virtual payment networks, such as Paypal, can compete with typical money transmitters.

- *AMF Licensing* - Quebec's licensing requirements became mandatory in the fall of 2013, and as a result, MSBs that operate in Quebec have different information collection requirements than that of other provinces.

- *Foreign Currency Forward Contracts* - Some MSBs provide the option of hedging their corporate customer's exposure to foreign currency swings and offered hedging. Certain provincial securities exchanges are reviewing this area to determine whether securities regulations and registration is applicable.

- *Access to Banking* - As previously identified, banking services are vital to many MSBs. With a limited number of financial institutions banking these entities, MSBs are either closing up operations or pursuing other avenues in order to continue their operations.

- *Impact of regulations on other sectors* - For example, as the banking sector responds to scrutiny from their regulators, this impacts the MSBs who use the services of the banks. This includes Canadian banks receiving detailed questions from their US bank clearing providers and then passing the question along to obtain responses from the MSBs. As a result, some MSBs have been recently told that deposits of certain US sourced funds will no longer be permitted due to regulatory requirements, like FATCA (Foreign Account Tax Compliance Act).

Appendix 9

8. Products and services offered

MSB organizations are generally divided into those that provide foreign currency exchange and those businesses that conduct money remittances or a combination of the two. Money orders and traveller's cheques, which operate in a niche market are usually a subservice of these MSB types.

Often MSBs provide their services in specific currencies and to certain regions of the world, often related to the network of individuals serviced.

Foreign currencies, especially cash, are acquired through different sources, generally from customers, banks and other MSBs. In the most optimal operations, an MSB would be able to acquire and sell the same foreign currency, which would reduce the acquisition cost of the foreign currency; otherwise, the MSB would need to purchase additional funds at market rates from banks and other MSBs. Foreign exchange rates are generally monitored closely by the MSBs and the acquisition cost would include a spread above the official foreign exchange rates.

Currency exchange risk is also a factor for many of the MSBs and some will employ hedging, typically by offloading or selling the currency to a financial institution or another MSB. Some of the larger foreign currency companies will also offer forward currency contracts as a means for customers to hedge their currency exchange exposure.

Many MSBs, either as part of their currency exchange or as their sole business, will provide international money remittance transactions. Overall, the purpose of the money remittance transaction is to transfer funds between Canada and another country, however, in some instances, the Canadian MSB acts as an intermediary for the transaction, as funds flow in from one country to Canada and out to a third country.

The method of how the funds are transferred can differ according to the size of the transaction, location of the funds, the beneficiary, and the availability/access to banking, as follows:

- Directly through a financial institution - The MSB sends the funds as a wire transfer through the financial institution, directly to the beneficiary's bank account;
- Consolidate amounts through a financial institution - The MSB combines the funds of several senders and sent as a single wire transfer to a recipient that will divide the funds amongst the designated beneficiaries. The recipient will be either a related individual, a related business, an unrelated business with which there is an agreement to work together. The unrelated business could include a large bank in the foreign country or an MSB-type business in the foreign country which would use the local bank to receive the funds and direct the payments to beneficiaries.
- Trade-based remittance - Also known as hawala, the MSB will receive or pay out funds in Canada based on trust or an agreement with a foreign MSB. No funds are physically transferred between the foreign MSB and the Canadian MSB; in order to settle the transfer of funds from Canada to the other country,

the MSB will eventually deliver funds to a beneficiary in Canada on behalf of the foreign MSB. Variations to this method include transactions where payments are made to foreign import/export companies on behalf of the foreign MSB.

9. Type of Customer(s)

The types of customers served by MSBs vary as much as the different types of MSBs that exist. While traditional MSBs serve the "unbanked" with money transfers to foreign countries, an increasing number serve a niche market that competes with financial institutions, providing faster and better service at a lower cost.

While there are niche services that target certain ethnic markets, others position their market advantage by offering management advice and expertise, for example, hedging a corporate client's currency risk.

While transaction amounts vary depending on the customer and reason for the transaction, some attributes that have been noted are:

- Individuals sending amounts to individuals in other countries are typically smaller and sent to support family;
- Individuals receiving amounts from foreign countries will include individuals immigrating to Canada or investing/purchasing assets in Canada; and
- Corporate customer foreign exchange and remittance transactions vary in dollar amount and frequency depending on the suppliers and customers involved.

10. Geographic considerations

MSBs are predominantly located in the larger urban centres across the country, Toronto, Vancouver and Montreal, reflecting in part larger ethnic populations and/or larger numbers of business enterprises.

In addition to areas that see an increase in the number of new immigrants, another factor to consider is that Canada has a large number of foreign temporary workers that perform seasonal or temporary work including agriculture, personal care and skilled or unskilled labour. These workers, in many cases send funds frequently to support families in their native countries.

MSBs that are involved in foreign currency exchange, often due to the proximity to the US border, conduct a significant portion of their transactions between Canadian and US funds. .

With an increase in the demand for online services, an increasing number of MSBs have also begun offering their remittance services online. Geographically, these types of MSBs can operate out of a single location instead of being physically close to the customer.

Considering broadly the MSBs across the country which provide remittance services, funds are sent to all corners and countries of the globe.

11. Key points from interviews

11.1 Sector Background

1. There are few barriers to enter into the MSB market place - all that is required is FINTRAC registration - not certain of how robust the system is and how much reliance to place. Perhaps a better system is the AMF, which conduct criminal background checks and has a licensing regime. In the UK too, there is a "fit and proper" test of ensuring operators have a good track record.
2. One barrier to entry is getting banking - some banks outright refuse to serve MSBs and in some cases, the owners' personal banking. In other cases, banking is provided but at a substantially higher fees for the MSB; however, the MSB is forced to pay as there are not many options in the market place. As a result, some MSBs will operate in a "grey" area - registered with FINTRAC but operating another company, typically an import/export company.

11.2 AML Compliance

3. KYC requirements is increasing but uncertain as to how information is being used or whether it is useful. Appears that a lot of information is collected.
4. Competition is a factor - there are unregistered MSBs that operate and require few, if any customer details and no ID requirements. They operate without the regulatory cost burden of compliance. There is not enough policing to stop this activity, even when it is reported to FINTRAC.

11.3 Risk areas

5. With higher operating costs and relatively low rates of policing, MSBs can go underground. Even if the MSB remains FINTRAC-registered, money may go towards a network of weak or non-existent banking controls.
6. With the availability of conducting transactions online, businesses can move offshore to an online platform and have fewer KYC requirements.
7. Overseas counterparties can be a riskier area as uncertain how much due diligence or KYC information is collected for each transaction.
8. Some MSBs provide other services that are not regulated, such as cheque cashing and payday loan - while there are regulations in those respective areas, who is looking at whether money laundering is considered in those areas? For instance, bill payment is also a risky area but an MSB would only report if they are registered to perform FX or money transfer activity, otherwise no obligation to report. Interviewee reported instances where they have seen payments made in small bills used to pay expensive utility bills ($10k +) where there is high probability this was a grow-op.
9. Prepaid cards is a potentially risky area - many of these are not closed loop (available for use at multiple retailers) such as Mastercard or Visa prepaid - there is no KYC check at the places you can buy these cards.

12. Risk Factors

12.1 General Market

12.1.1 Ease of entry to the market

Entry into the MSB market is relatively easy, with sector participants required to register with FINTRAC (and the AMF in Quebec). In some cases there continue to be organizations which are not registered. Accordingly, sector participants can knowingly or unknowingly expose the market to money laundering and terrorist financing risks. A mitigating factor is that many financial institutions restrict the availability of banking facilities for new entrants including requiring ownership due diligence and monitoring over transactions and the MSB's compliance regime.

12.1.2 'Unbanked' MSB Activity - Unintended Consequences

As indicated, there has been significant risk management programs put in place in some of the larger banks and this has resulted in some of the MSBs becoming unbanked. To the extent that the activity is still occurring - that is, the funds still flow between parties - this unbanked activity moves underground and becomes in essence unseen and not monitored.

12.1.3 Trade Based Money Laundering (TBML)

Whether the MSB is unable to obtain a bank account or there are few if any methods of formally transferring funds, MSBs may use trade based methods to transfer funds. There is a higher risk that these methods, if unchecked, leave the system exposed to money laundering. As an example, one interviewee identified an MSB which operated by remitting funds to non-sanctioned individuals in an OFAC-sanctioned country. As there was no formal method to transfer funds, payments were made from Canada to a foreign company that potentially supplied sanctioned products to the same country.

12.1.4 Use of Services by Fraudsters and Scam Artists

The sector has been used by fraudsters and scam artists who have taken advantage of targeted individuals, for example by soliciting advanced fees with the promise to pay winnings. The use of MSB services to facilitate these crimes means that it becomes more difficult for law enforcement and victim parties to trace the flow of funds. The use of the sector for fraud generates illegal funds which are then subsequently moved and these movements become attempts at money laundering.

12.2 Products and Services

12.2.1 Virtual Currencies

The use and popularity of virtual currencies, such as bitcoin, has increased in the last several years, exposing the sector to unknown vulnerabilities, including legalities and fraud-related issues. While not currently competing with mainstream MSBs, opportunities are provided for people to launder funds as this activity is basically unregulated except through the denial of banking services. Recent cases include Liberty Reserve that had its own currency and

facilitated over $6 billion in illicit money transfers, and Mt. Gox, the bitcoin exchange that recently went into bankruptcy protection over stolen bitcoins. See Appendix A.

12.2.2 Other Services

MSBs that offer other services that are not FINTRAC-regulated, for instance cheque-cashing or payday loans, can leave the system exposed to gaps as there are few requirements regarding these activities and none of them really consider AML compliance. Businesses that offer similar, but non-FINTRAC regulated services only (e.g. cheque cashing) aren't required to be registered and therefore would have no obligation to identify and report suspicious activity. This is a significant concern and results, for example, in a specific MSB business having the currency exchange and remittance transactions it conducts subject to close scrutiny while the cheque cashing activities basically occur unmonitored. Some banks are currently discussing how to effectively address this in regards to money laundering concerns, but in the absence of regulatory requirements, are challenged to have the activity effectively monitored.

12.3 Delivery Channels

12.3.1 Size of the MSB

MSBs that are larger have more resources to devote to compliance. Smaller MSB businesses and individuals are subject to inherent risk and operate with structures which are challenged to provide effective oversight once transaction and customer volumes become too large for manual monitoring and oversight. There are a smaller number of larger businesses in this sector and a higher number of smaller organizations. It is noted that the banking sector oversight has caused a significant tightening up of the compliance regime procedures for a number of the MSB organizations, small and larger, in some respects resulting in regimes that are highly effective on a comparative basis across all of the regulated sectors.

12.3.2 Use of Agents

The use of agents is an important factor for many MSBs growing their business, especially those that target certain ethnic communities. The level of due diligence conducted on agents as well as the ability of agents to perform at a sufficient level and the ability of the MSB using the agent to monitor activity, all vary among different organizations.

In addition, individuals or entities that act as agents on behalf of more than one MSB may be at risk for knowingly or unknowingly structuring transactions. If the agent does not report this activity to the MSBs, identification and reporting of these transactions is difficult, if not impossible.

12.4 Geography

12.4.1 Overseas Counterparties

MSB remittance businesses provide services to their clients through the use of counterparties in the overseas locations that funds are sent to. To the extent that flow of funds between these parties is not monitored, subject to oversight and review, there are significant opportunities for illegal funds to be moved. Currently the regulatory regime in Canada focuses on the transactions these organizations have with their customers, e.g. the source of the money to the MSB. The regulatory regime does not provide for mandated oversight of the flow of funds at the

accumulated level. Generally, reviews of the compliance regimes of MSB businesses will highlight that funds between the counterparties were not subject to review. There is currently no incentive for the MSB business to pay for the cost to have a review of these transactions performed and reported on.

12.4.2 Movement Offshore of Online Platforms and Networks

The services of moving and exchanging money, to the extent there is access through the banking sector, can be provided through online platforms that are made accessible to customers all over the world. The movement of these platforms to offshore centres may indicate that regulatory requirements are being avoided and thus the services more accessible to those with illegally sourced funds.

12.5 Business relationships/linkages with other sectors

12.5.1 Banking "Gatekeeper role"

Without an understanding of the MSB's customers and how funds are transmitted, money transmitters can expose a financial institution to money laundering risk.

12.5.2 Overseas counterparties- see above

12.6 Transaction methods/types

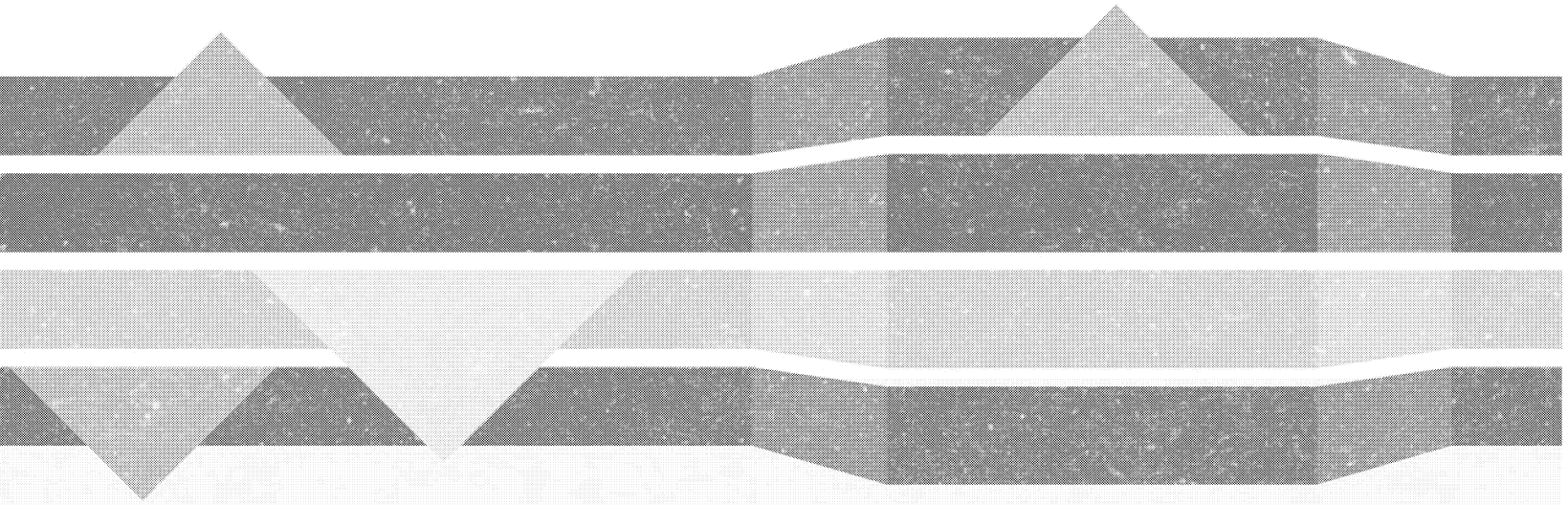
Nothing specifically noted beyond the characteristics of transactions applicable to banking sector, including structuring, third parties, method of payment etc.

Grant Thornton

Comparative Analysis Table

Money laundering and terrorist financing vulnerability assessments

Prepared for FINTRAC | March 31, 2014



Appendix 9

Reporting Entity Sector Profiles
Money laundering and terrorist financing vulnerability assessments
Comparative Analysis Table

Risk Factors	Real Estate	DPMS	Securities	Accountants	Life Insurance	BC Notaries	Credit Unions	Financial Entities	Casinos	MSBs	Lawyers
General Market	Very High	Very High	Very High	Low	Medium	Not Rated	Medium	Very High	Low	Very High	Medium
Comparative level of stability of Cdn market	✓		*								
Market competitiveness at agent/individual level; quality and ethics of firms/sales individuals	✓✓		✓	*	✓✓	*	*	✓		*	✓✓
Minimum level of regulation and/or oversight OR volume of regulation challenges	✓	✓						✓			
Regulatory fragmentation			✓		✓		✓				
Ease of entry to market OR new entrants	*	✓	✓						✓	✓	
No cross border controls	*	✓									
Trade based money laundering		✓						✓		✓	
Level of law enforcement/authority awareness		✓									
Inability to share information amongst sector participants			✓	*							
High level of fraud within sector	*		✓							✓	
Management of multiple reporting lines					✓						
Governance structure: Board member requirements							✓				
Comparative risk management/transaction monitoring							✓	✓			
Exit of high risk relationships								✓		✓	
Products and Services	Medium	Medium	High	High	Low	High	Very High	Very High	Low	Very High	High
Characteristics of sector products/services/assets	✓	✓	✓	✓	✓	✓	✓	*		*	✓
Specific service e.g. iron butterfly, exempt market in securities, tax planning in accounting, international wires, wealth management)			✓	✓			✓	✓			*
Off-book products/uncertified; unregistered		✓	✓								
Purchase of life insurance policies by terrorist fighters					✓						
Expanding scope of services and/or breadth of services				✓		✓				✓	*
Delivery Channels	Medium	High	High	High	Low	Medium	High	Very High	Low	Very High	Very High
Use of agents: property purchases; agent referrals; junket operators and marketing agents	✓				✓	✓	✓		✓		✓

This table should only be considered in conjunction with the report entitled: Reporting Entity Sector Profiles- Money Laundering and Terrorist Financing Vulnerability Assessments, March 31, 2014.

Reporting Entity Sector Profiles
Money laundering and terrorist financing vulnerability assessments
Comparative Analysis Table

	Real Estate	DPMS	Securities	Accountants	Life Insurance	BC Notaries	Credit Unions	Financial Entities	Casinos	MSBs	Lawyers
Risk Factors											
Size of sector party	*	✓	✓	✓			✓			✓	✓
On-line sales / new technologies	*	✓						✓	✓	✓	
Pawnshops		✓									
Exempt market / unregistered activity / off book			✓	*							
Provision of services outside of area of expertise				✓							✓
Use of legal privilege	*			✓							✓
Geography	Very High	High	High	Medium	Low	Low	Medium	Very High	Low	High	Medium
Use of foreign money (to purchase real estate asset, offshore companies in securities sector)	✓	*	✓								
Investments in emerging markets, offshore centres	✓		*								
Global market for sector product / access to international financial network		✓				✓	✓	✓		✓	
Clients from foreign jurisdictions/high risk			✓	✓		*					*
Referrals to offshore affiliates located in higher risk jurisdictions				✓	✓			✓			*
Canadian branches of foreign financial institutions								✓			
Business Relationships/ Linkages with Other Sectors	High	Medium	Medium	High	Low	Medium	High	High	Low	Medium	Very High
Use of lawyers and their trust accounts	✓			✓				✓			✓✓✓
Supplier/counterparty risk / impacts		✓✓					✓			✓	
Reliance on regimes of other jurisdictions, other financial institutions		*	✓				✓	✓			
Lack of clarity as to who is monitoring within sector			✓		*		*				
Use of nominees	*		✓								
Providing services under guise of other sector (DPMS re wealth management)		✓									
Gatekeeper role			*	*	✓					✓	*
Conflict of interest issues				✓							
Higher risk real estate transactions (accountants and lawyers)	*			✓		✓					✓

This table should only be considered in conjunction with the report entitled: Reporting Entity Sector Profiles- Money Laundering and Terrorist Financing Vulnerability Assessments, March 31, 2014.

Reporting Entity Sector Profiles
Money laundering and terrorist financing vulnerability assessments
Comparative Analysis Table

	Real Estate	DPMS	Securities	Accountants	Life Insurance	BC Notaries	Credit Unions	Financial Entities	Casinos	MSBs	Lawyers
Risk Factors											
Clients who opinion shop				✓							
Engaged to perform work through third parties				✓							
Transaction Methods and Types	Very High	Medium	High	Low	High	Very High	Very High	Very High	Very High	Very High	Very High
Use of cash	✓	✓							✓		
Structuring									✓	*	
Incomplete deals (real estate and insurance)	✓				✓						
Corporate vehicles: including shell companies and property management companies, institutional accounts	✓✓		✓	*		*	*	*		*	*
Private mortgages and lending / source of funds for debt repayment	✓								✓		
Transactions conducted using physical/bearer securities/chips as currency			✓						✓		
Third party payments					✓						
Surrendering of large value policies early					✓						
Receipt of funds, method and sources unexpected						*					✓
Customer Types and Characteristics				High							High
Customer Types and Characteristics				✓							✓
Overall Comparative Risk Rating	Higher	Higher	Higher	Higher	Lower	Higher, (but limited)	Medium	Lower	Lower	Medium	Higher

✓ - Risk factor identified specifically and listed in report

* - Upon review, this is noted as a risk for the sector, not specifically listed as such in the report

A four point scale was used to rate each risk factor group by sector: Low, medium, high, and very high.

This table should only be considered in conjunction with the report entitled: Reporting Entity Sector Profiles- Money Laundering and Terrorist Financing Vulnerability Assessments, March 31, 2014.

Grant Thornton

Reporting Entity Sector Profiles: Appendices by Sector

Appendix A – Industry Statistics and Reporting Entity Data

Appendix B – Case Examples and Typologies

Prepared for FINTRAC | March 31, 2014

Grant Thornton

Reporting Entity Sector Profiles: Real Estate Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

Real estate industry SIC codes

Code	Description
6500	Real Estate
6510	Real Estate Operators (No Developers) & Lessors
6512	Operators of non-residential buildings
6513	Operators of apartment buildings
6531	Real estate agents & managers (for others)
6532	Real estate dealers (for their own account)
6552	Land sub-dividers & developers (no cemeteries)
6798	Real estate investment trusts
1531	Operative builders
6553	Cemetery sub-dividers and developers
1521	General contractors – single family house
1522	General contractors – res-buildings, other than single family
1541	General contractors – industrial buildings and warehouses
1542	General contractors – non res buildings, other than ind buildings and warehouses

Real estate industry NAICS codes

Code	Description
531	Real estate
5311	Lessors of real estate
531111	Lessors of residential buildings and dwellings (except social housing projects)
531112	Lessors of social housing projects
5312	Offices of real estate agents and brokers
53121	Offices of real estate agents and brokers
531211	Real estate agents
531212	Offices of real estate brokers
5313	Activities related to real estate
531310	Real estate property managers CAN

Code	Description
23	Construction
236	Construction of Buildings
2361	Residential Building Construction
23611	Residential Building Construction
236110	Residential Building Construction
2362	Non-residential Building Construction
23621	Industrial Building and Structure Construction
236210	Industrial Building and Structure Construction
23622	Commercial and Institutional Building Construction

Using NAICs codes, searches for statistical data on the Real Estate Industry sectors were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Real estate (NAICS 531)

Number of establishments in Canada by type and region: December 2012
Real Estate (NAICS 531)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	5,848	23,448	29,296	11.3%
British Columbia	9,156	35,861	45,017	17.3%
Manitoba	1,247	5,314	6,561	2.5%
New Brunswick	780	2,441	3,221	1.2%
Newfoundland and Labrador	607	1,518	2,125	0.8%
Northwest Territories	69	129	198	0.1%
Nova Scotia	1,044	3,681	4,725	1.8%
Nunavut	44	33	77	0.0%
Ontario	17,253	83,054	100,307	38.6%
Prince Edward Island	198	630	828	0.3%
Quebec	9,110	51,865	60,975	23.5%
Saskatchewan	1,357	5,087	6,444	2.5%
Yukon Territory	60	176	236	0.1%
CANADA	46,773	213,237	260,010	100%
Percent Distribution	18.0%	82.0%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments
by employment size category and region: December 2012
Real Estate (NAICS 531)

Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	4,650	1,144	47	7
British Columbia	7,270	1,848	33	5
Manitoba	876	358	11	2
New Brunswick	594	183	2	1
Newfoundland and Labrador	466	139	2	0
Northwest Territories	30	39	0	0
Nova Scotia	745	290	8	1
Nunavut	9	35	0	0
Ontario	13,136	3,980	115	22
Prince Edward Island	144	52	1	1
Quebec	6,280	2,785	43	2
Saskatchewan	1,043	309	4	1
Yukon Territory	42	18	0	0
CANADA	35,285	11,180	266	42
Percent Distribution	75.4%	23.9%	0.6%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of establishments in Canada by type and region: December 2012 Offices of Real Estates Agents and Brokers (NAICS 5312)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	1,212	4,266	5,478	10.5%
British Columbia	1,457	8,066	9,523	18.2%
Manitoba	166	1,034	1,200	2.3%
New Brunswick	129	366	495	0.9%
Newfoundland and Labrador	77	328	405	0.8%
Northwest Territories	1	3	4	0.0%
Nova Scotia	156	705	861	1.6%
Nunavut	0	0	0	0.0%
Ontario	2,795	20,958	23,753	45.4%
Prince Edward Island	18	94	112	0.2%
Quebec	1,065	8,467	9,532	18.2%
Saskatchewan	147	793	940	1.8%
Yukon Territory	3	4	7	0.0%
CANADA	7,226	45,084	52,310	100%
Percent Distribution	13.8%	86.2%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of establishments in Canada by type and region: December 2012 Real Estate Property Managers (NAICS 53131)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	591	1,719	2,310	10.6%
British Columbia	908	2,179	3,087	14.1%
Manitoba	118	341	459	2.1%
New Brunswick	47	128	175	0.8%
Newfoundland and Labrador	36	74	110	0.5%
Northwest Territories	2	11	13	0.1%
Nova Scotia	80	265	345	1.6%
Nunavut	2	2	4	0.0%
Ontario	2,183	6,434	8,617	39.5%
Prince Edward Island	11	26	37	0.2%
Quebec	1,175	5,162	6,337	29.0%
Saskatchewan	79	232	311	1.4%
Yukon Territory	3	9	12	0.1%
CANADA	5,235	16,582	21,817	100%
Percent Distribution	24.0%	76.0%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Real Estate Property Managers (NAICS53131)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	351	223	14	3
British Columbia	593	308	6	1
Manitoba	63	51	4	0
New Brunswick	35	12	0	0
Newfoundland and Labrador	30	6	0	0
Northwest Territories	1	1	0	0
Nova Scotia	55	24	1	0
Nunavut	0	2	0	0
Ontario	1,418	729	28	8
Prince Edward Island	7	4	0	0
Quebec	729	437	9	0
Saskatchewan	47	32	0	0
Yukon Territory	3	0	0	0
CANADA	3,332	1,829	62	12
Percent Distribution	63.6%	34.9%	1.2%	0.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Construction (NAICS 23)

Number of establishments in Canada by type and region: December 2012 Construction (NAICS 23)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	20,388	25,822	46,210	16.4%
British Columbia	21,245	30,509	51,754	18.3%
Manitoba	4,136	4,603	8,739	3.1%
New Brunswick	3,053	1,859	4,912	1.7%
Newfoundland and Labrador	2,294	1,093	3,387	1.2%
Northwest Territories	172	137	309	0.1%
Nova Scotia	3,716	2,631	6,347	2.2%
Nunavut	57	23	80	0.0%
Ontario	41,205	60,700	101,905	36.1%
Prince Edward Island	664	459	1,123	0.4%
Quebec	27,100	20,455	47,555	16.8%
Saskatchewan	4,379	5,212	9,591	3.4%
Yukon Territory	241	248	489	0.2%
CANADA	128,650	153,751	282,401	100%
Percent Distribution	45.6%	54.4%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Construction (NAICS23)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	13,125	6,918	301	44
British Columbia	13,565	7,499	174	7
Manitoba	2,282	1,823	31	0
New Brunswick	1,738	1,290	24	1
Newfoundland and Labrador	1,270	1,008	13	3
Northwest Territories	68	99	5	0
Nova Scotia	2,222	1,471	22	1
Nunavut	11	44	2	0
Ontario	24,590	16,199	384	32
Prince Edward Island	388	273	3	0
Quebec	15,826	11,053	209	12
Saskatchewan	2,544	1,796	37	2
Yukon Territory	143	97	1	0
CANADA	77,772	49,570	1,206	102
Percent Distribution	60.5%	38.5%	0.9%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Using SIC codes, searches were carried out on Lexis to extract statistical data on the Real Estate Industry sectors from Duns Market Identifiers.

Real estate companies

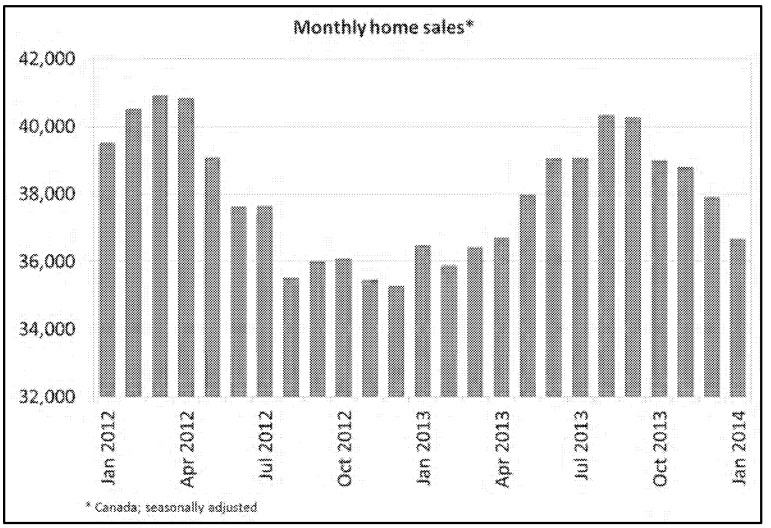
SIC Code		Ontario	BC	Alberta	Quebec	Manitoba	NWT	Nova Scotia	Nfld	Sask	NB	PEI	Yukon	Nunavut	Total
6500	Real Estate														
6510	Real estate operators (no developers) & lessors														
6512	Operators of non residential buildings	972	501	453	1222	96	11	219	97	89	105	24	4	0	3793
6513	Operators of apartment buildings	613	239	177	704	70	7	183	41	62	97	22	3	1	2219
6531	Real estate agents & managers (for others)	869	398	420	489	127	9	86	22	125	48	12	2	1	2608
6532	Real estate dealers (for their own account)														0
6552	Land subdividers & developers (no cemetries)	125	64	56	25	3	0	8	2	17	6	0	0	0	306
6798	Real estate investment trusts	35	12	19	23	3				3					95
1531	Operative builders	199	142	70	199	4		40	6	9	12				681
6553	Cemetery subdivders and developers	705	456	242	234	52	5	67	17	48	32	10	1	1	1870
1521	General contractors - single family houses	3155	1531	1517	2982	407	46	442	209	342	279	42	13	26	10991
1522	General contractors - res builders, other than single family	1059	613	432	1329	86	14	129	48	50	73	17	5	4	3859
1541	General contractors - ind buildings and warehouses	1370	439	520	1208	84	17	125	99	76	100	11	5	8	4062
1542	General contractors - non res buildings, other than ind buildings and warehouses	2614	1206	1175	2654	286	28	263	151	250	210	33	18	19	8907
6519	Lessors of real property														0
7011	Hotels & Motels	1789	1198												2987

Source: Lexis (Duns Market Identifiers)

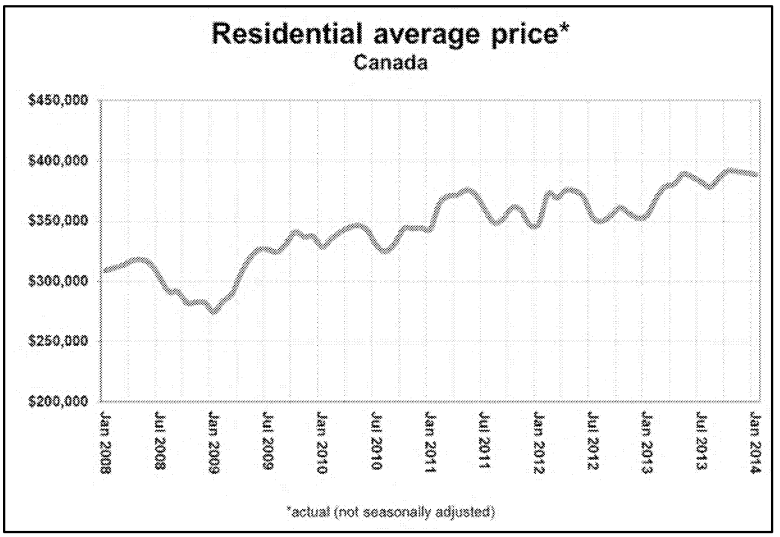
Canadian home sales by city, dollar volume (in millions)

Area	Nov. 2012	Nov. 2013	Percent change
Calgary	757.9	967.2	27.6%
Edmonton	369.7	438.6	18.6%
Fraser Valley	371.3	478.4	28.8%
Gatineau CMA	60.1	55.7	-7.2%
Halifax-Dartmouth	96.6	91.8	-4.9%
Hamilton-Burlington	333.8	377.1	13%
Kitchener-Waterloo	157.1	151.6	-3.5%
London and St Thomas	125.6	141	12.2%
Montreal CMA	867.1	847.5	-2.3%
Newfoundland & Labrador	107.9	110	2%
Ottawa	328.5	323.9	-1.4%
Quebec CMA	134.6	119.3	-11.3%
Regina	70.5	79.4	12.6%
Saguenay CMA	16.9	12.5	-26.4%
Saksatoon	114.6	130.1	13.6%
Saint John	20.2	20.9	3.4%
Sherbrooke CMA	27.3	21.7	-20.5%
St. Catharaines	40.7	37.7	-7.3%
Sudbury	41.7	35.2	-15.6%
Thunder Bay	23.9	31.6	32.3%
Toronto	2,811.5	3,444	22.5%
Trois Rivières CMA	9.3	7.5	-19%
Vancouver	1,182.3	1,852.1	56.7%
Victoria	168.5	173.2	2.8%
Windsor-Essed	61.4	64.2	4.6%
Winnipeg	209.2	212.1	1.4%

Source: Canadian Real Estate Association



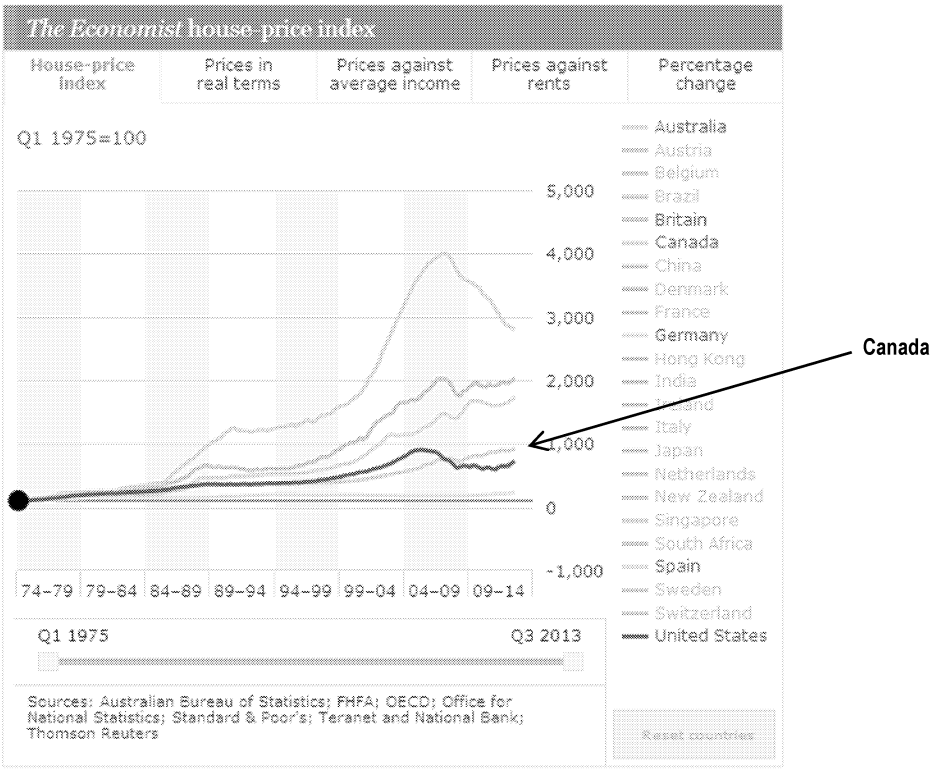
Canadian home sales as at January 2014



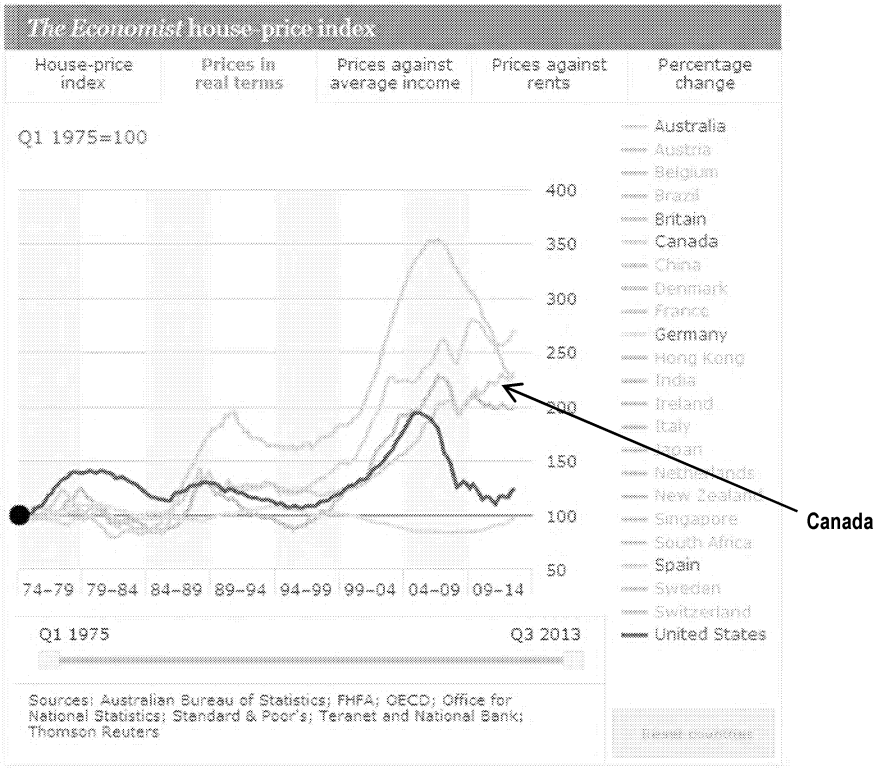
Source: Canadian Real Estate Association

The Economist House Price Index

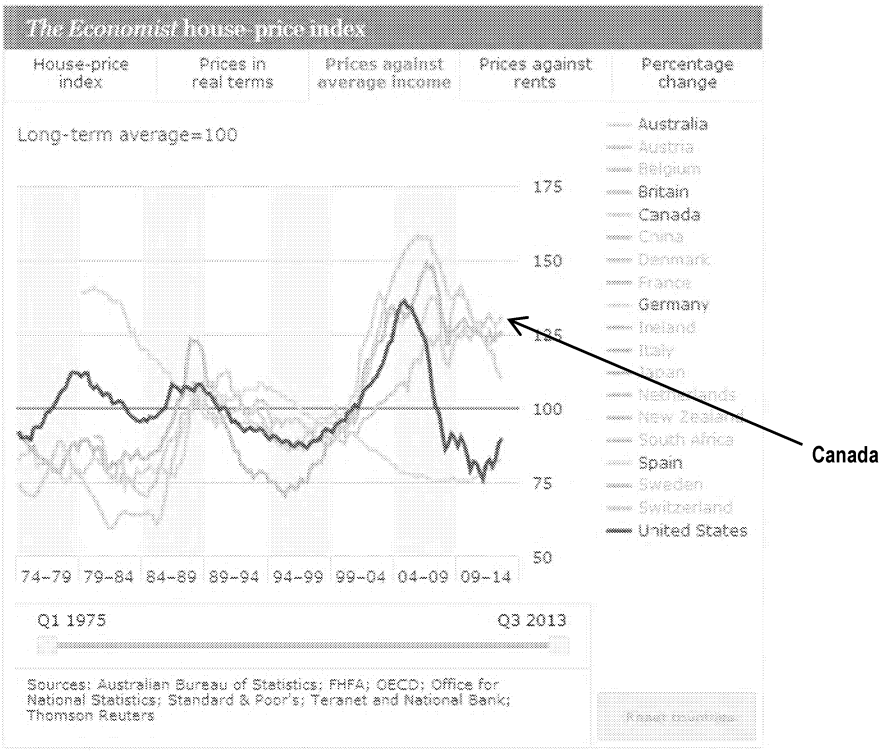
This interactive tool uses five different measures to illustrate relative house pricing on a global basis.



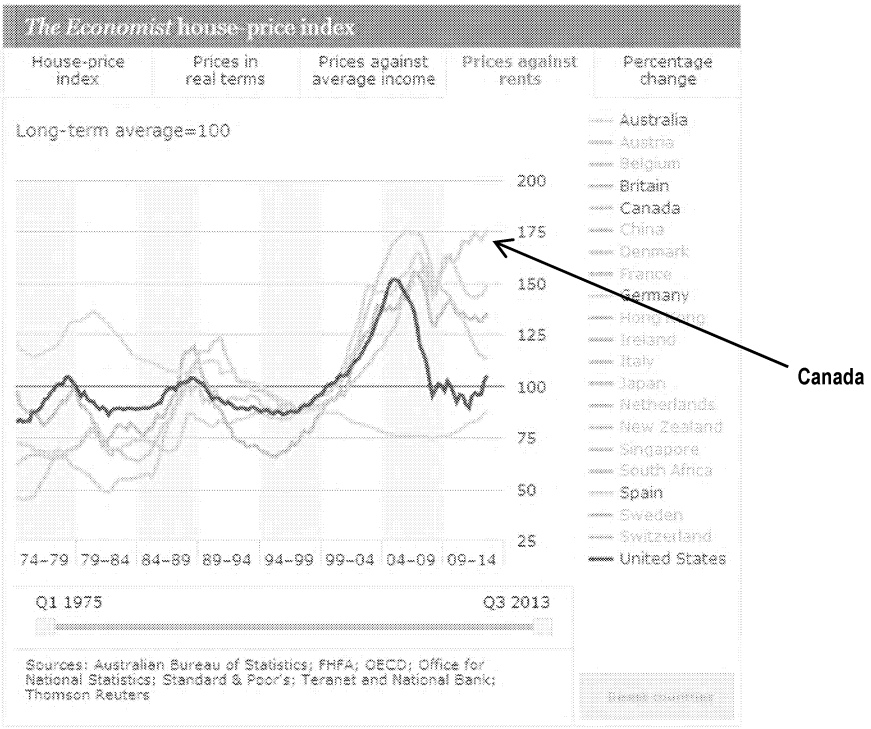
House-price index—rebased to 100 at a selected date and in nominal terms only



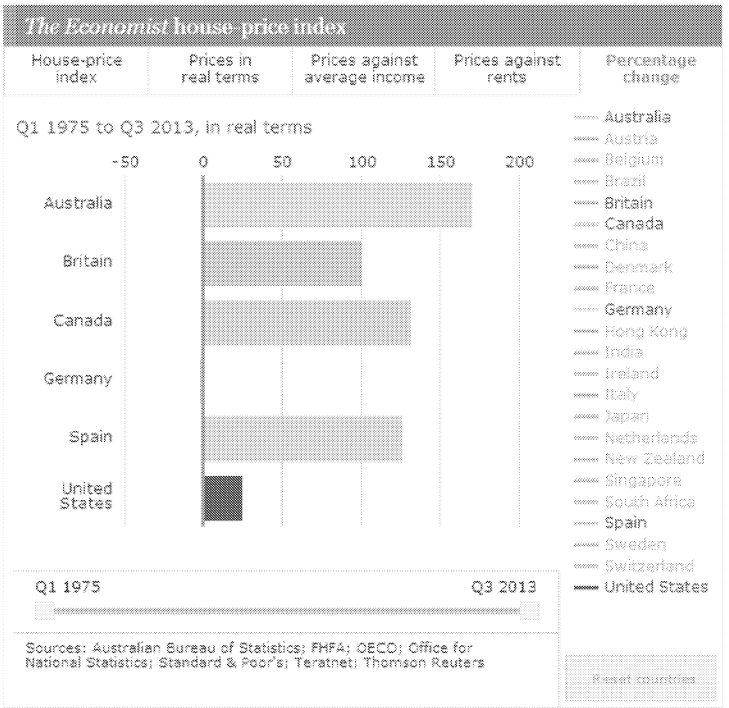
Prices in real terms—rebased to 100 for the selected date, but the index is deflated by consumer prices to take account of the effects of inflation on purchasing power.



Prices against average income—compares house prices against average incomes in each country, rebased to 100 at the selected date.



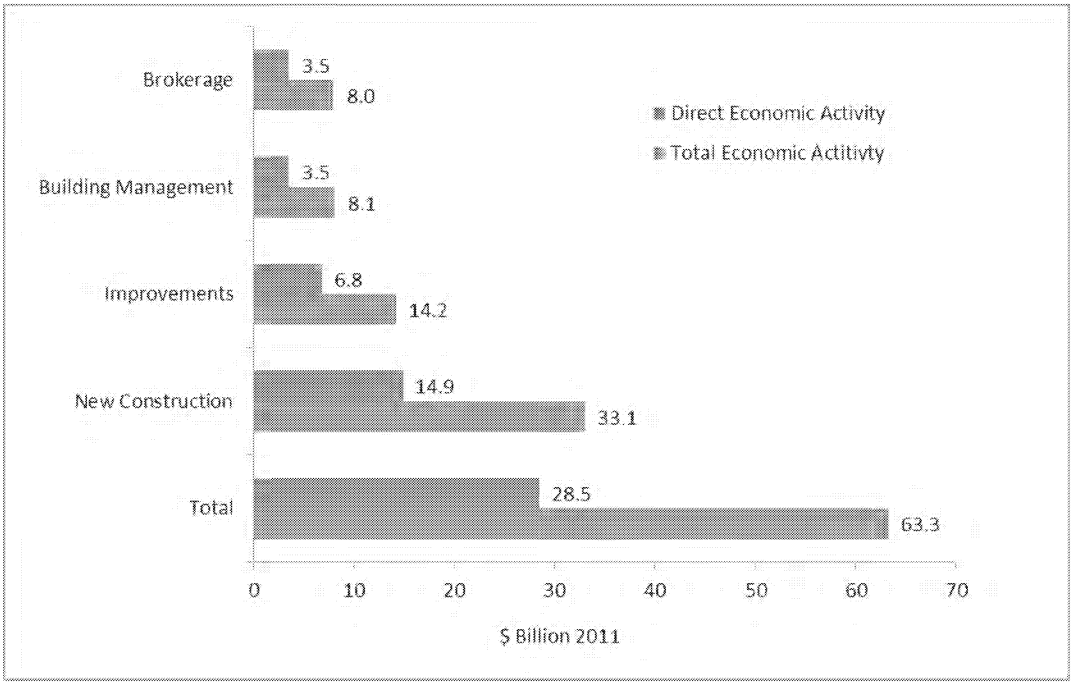
Prices against rents—compares the relationship between the costs of buying and renting, rebased to 100 at the selected date.



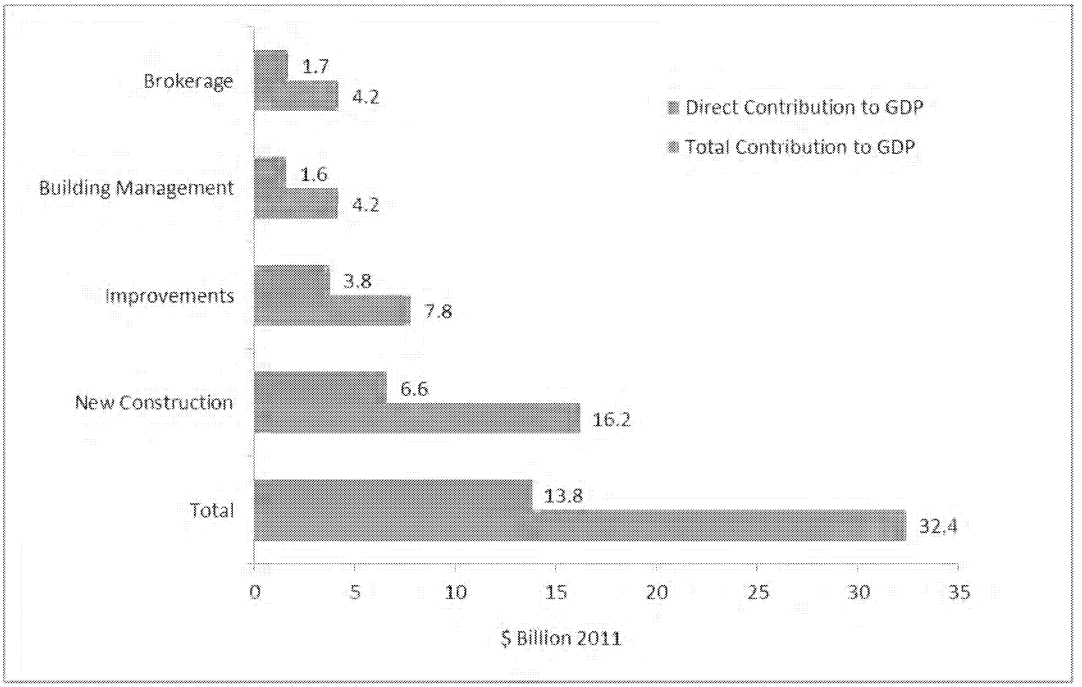
Percentage change (in real terms)—shows the increase or decrease in real prices between two selected dates.

The Contribution of the Commercial Real Estate Sector to the Canadian Economy

Economic activity generated



Contribution to National GDP



Source: The Contribution of the Commercial Real Estate Sector to the Canadian Economy – Altus Group Economic Consulting (Prepared for REALpac and NAIOP) – September 2012

Foreign investment in luxury single family homes in Canada

City	Domestic Investment	Foreign Investment	Strongest Foreign Influences
Vancouver	60%	40%	China, Iran, USA
Calgary	85%	15%	
Toronto	75%	25%	USA, China, Russian, Middle East, India
Montreal	51%	49%	China, Syria, Mexico, USA, Russia
Victoria	90%	10%	USA, England, China
Salt Spring	85%	15%	Asian, USA, European
Oakville	Increased foreign buyers in last two years		Mainland China
Niagara-on-the-Lake	Increased foreign buyers in last two years		China
Sun Peaks	75%	25%	Australia, UK, USA
Whistler	75%	25%	Australia, UK. USA
Mont Tremblant	85%	15%	

Source: Sotheby's International Realty – 2013 Top Tier Trends Report

Real estate rental and leasing and property management (Canada)

	2010	2011p
	$ millions	
Canada		
Lessors of residential buildings and dwellings (except social housing projects)		
Operating revenue	39,164.3	40,889.1
Operating expenses	33,293.6	34,614.2
Salaries, wages and benefits	1,598.6	1,626.4
	%	
Operating profit margin	15.0	15.3
	$ millions	
Non-residential leasing		
Operating revenue	35,353.2	36,427.4
Operating expenses	26,606.5	27,325.6
Salaries, wages and benefits	2,504.4	2,543.1
	%	
Operating profit margin	24.7	25.0
	$ millions	
Real estate property managers		
Operating revenue	5,052.9	5,263.0
Operating expenses	4,141.2	4,300.9
Salaries, wages and benefits	1,169.1	1,191.7
	%	
Operating profit margin	18.0	18.3

P : preliminary.
Notes:
- North American Industry Classification System (NAICS), 2007 - 53112, 53113, 53119, 53131 and 531111.
- Figures may not add to totals because of rounding.
Source: Statistics Canada, CANSIM, table 357-0017 and Catalogue no. 63-248-X.
Last modified: 2013-03-26.

Appendix B: Case examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report. In particular, they illustrate how organized crime figures from other countries and politically exposed foreign persons, were able to bring presumably illicit funds into the Canadian financial system, using the real estate sector.

1. A foreign attraction to Montreal's real estate market, Montreal Gazette, November 23, 2013
2. Foreign Ownership of Canadian Property: More calls for the mystery numbers, The Vancouver Sun, November 7, 2013
3. Vancouver real estate: The fog of foreign ownership, The Vancouver Sun, March 23, 2013
4. How Asian buyers are boosting Vancouver's luxury housing market, The Globe and Mail, July 26, 2013
5. Is the money-laundering driven real estate "boom" ending, Zerohedge.com, September 30, 2012
6. Lawyers and Real Estate Transactions, Money Laundering in Canada: Chasing Dirty and Dangerous Dollars, Margaret E. Beare and Stephen Schneider, 2007
7. Saxena guilty in massive fraud, jailed for 10 years, The Vancouver Sun, June 8, 2012
8. Chinese suspect in smuggling case released into Canadian house arrest, BBC, March 10, 2001
9. Lai Changxing leads a very lavish lifestyle in Vancouver, Chinese in Vancouver, May 4, 2007
10. Court documents say alleged dragon head laundered triad cash in Canada, The Canadian Press, March 3, 2013
11. Lai Tong Sang's luxury house in Vancouver's Fraserview neighbourhood was the target of a drive-by shooting in July 1997, Montreal Gazette, February 3, 2013
12. Family brawl enthralls Asia; Gambling tycoon sues Canadian children over alleged coup as offspring, wives fight over empire, The Toronto Star, January 28, 2011
13. Fugitive's flight ends; Man accused of embezzling millions in Kazakhstan lived in luxury in King City until arrest this month, Toronto Star, February 20, 2012

14. Toronto's Trump Hotel; An exclusive first look at the tallest residential tower in Canada, built by the country's youngest self-made billionaire, Toronto Star, March 24, 2011

15. Alex Shnaider- The steel magnate, Canadian Business, December 5, 2005

16. Former oil executive says he signed controversial deal 'under duress', Globe and Mail, April 4, 2013

17. Court freezes sale of home once owned by drug smuggler; Custom-built residence 160km east of Kamloops is valued at $1.75 million, Vancouver Sun, January 27, 2011

18. Canada gets reputation as haven for fugitives, The Boston Globe, December 21, 2000

19. Beijing goes hunting for overseas real estate bought with dirty money – Qz.com – November 5, 2013

20. Canada froze billions in assets to support Arab Spring: RCMP. The Globe and Mail, July 15, 2012

21. Tunisians in Montreal protest Ben Ali family, CBC News, January 27, 2011

22. Ottawa asked to speed up seizure of ex-dictator's assets, National Post, March 15, 2012

23. Libya claims stake in Saadi Gaddafi's $1.6M Toronto condo, National Post, October 31, 2012

24. Brokers gone bad, Canwest News Service, April 20, 2010

25. Mortgage Fraud hits $1.5b a year: Easy to do, often lucrative, real estate agents say it is growing quickly across Canada, The Vancouver Sun, March 20, 2006

26. Lawyer faces fraud charges; RCMP also lay charges of money laundering after raids on Etobicoke home, Concord law office, The Toronto Star, June 9, 2012

27. Mortgage scam probed in Toronto house flips; Seven homes in the Junction were taken on a wild real estate ride that ended in a lawyer's suspension, The Toronto Star, January 7, 2012

28. Global fraudster faces new charges, The Toronto Star, April 11, 2007

29. Ice Queen pledged to sell fast food, South China Morning Post, February 28, 1996

A foreign attraction to Montreal's real estate market

BY ALLISON LAMPERT, GAZETTE REAL ESTATE REPORTER NOVEMBER 23, 2013

People are seen w aiting outside the offices for the Seville condos on St-Catherine St. W. in 2010.
Photograph by: Dario Ayala, The Gazette

MONTREAL — Down the street from Montreal's old Forum, in a bustling neighbourhood now dotted with Chinese noodle shops, ethnic grocers and new construction, the sign on the door of the Le Seville condo building asks residents in French, English and Chinese: "Do you know the person you let in?"

Since last year's annual meeting — when some condo owners from China had difficulty following the discussion — the board of directors has been translating important material — such as the sign on the door and the building's annual budget — into Chinese.

"It was clear that the Chinese buyers needed to have access to a language they'd understand, like everyone else in the building," said condo board president Colin Danby, who learned Mandarin during seven years spent in Taiwan.

"Not everything is translated. But as a board, we take that step when it is something important like building security."

Residents estimate that between 20 to 40 per cent of the Seville's co-owners are either Chinese

Canadian, recent immigrants who own neighbouring shops in the area known as Shaughnessy Village, or are foreign investors from China.

They bought into the sold-out first phase of the 477-unit Seville in 2010 — when low interest rates and an economy that had emerged relatively well from the 2008 financial crisis drove demand for Montreal condos to near-record highs.

While the vast majority of foreign real estate buyers in Canada have focused on Toronto and Vancouver, investors from China, Middle East and Europe also helped fuel Montreal's condo boom, which peaked in 2012.

In 2011, Montreal had the second highest number of permits and starts for new condos of any city in North America. Toronto was in first place.

"More inventory, more investors," said Alexandre Sieber, senior managing director of Quebec operations for real-estate services firm CBRE Ltd. "As you build inventory, you are diversifying the investor base."

Some firms estimate that up to 20 per cent of Montreal condos bought as rental properties — or to be flipped for a profit — were purchased by foreign buyers searching for inexpensive prices in a comparatively stable market.

Foreign investors have also bought small multi-unit buildings for use as student rentals and are showing interest in large properties, including vast tracts of land in the Laurentians, brokers say.

Just like Vancouver, or Toronto, there is no hard data for the number of foreign real-estate investors in Montreal.

But two foreign buyers, along with half-a-dozen commercial and residential real estate brokers, told The Gazette that sales to foreigners and landed-immigrants in areas like Westmount and LaSalle are on the upswing.

And Asian and Middle Eastern money is behind at least two new large sites downtown that are being promoted for residential development.

"We're certainly seeing an increase in foreign buyers, especially from China," said Robert MacDougall, senior vice-president for investment sales and special projects at the commercial real estate services firm Jones Lang LaSalle.

MacDougall said about 10 to 20 per cent of his offers on properties now come from foreign investors, mostly Asians.

In addition to the foreigners who've long been purchasing condos for their adult children attending McGill and Concordia universities, people who have recently arrived from Asia are also buying homes in Westmount to be close to their kids' private schools, brokers say.

Sotheby's International Realty Canada estimated recently that half of the luxury properties sold in Montreal this year were purchased by foreigners.

"Two or three years ago, I had the odd buyer show up from China. That was kind of a novelty," recalled Brian Dutch, a broker with Re/Max DuCartier, who specializes in the Westmount market. "Then all of a sudden, there was another Chinese broker calling for an appointment. And then there's another.

"From it being the odd one, there are now at least two inquiries on a weekly basis."

While foreign buyers are appreciated by the real estate industry because they purchase properties in a relatively soft housing market, investors from Asia and the Middle East have been blamed for driving up home prices in Vancouver. Economists have warned that foreign buyers also create a more volatile market driven by yields, rather than by fundamentals like having a place to live.

In Montreal, there have been a few instances of buyers from other countries failing to show up at the notary's office, after signing contracts — and leaving hefty deposits — to purchase homes.

But Montreal brokers have yet to see widespread bidding wars with Asian or Middle Eastern buyers willing to pay above-market prices.

"I have seen those kinds of news stories from Toronto and Vancouver (about inflated prices), but my clients are more cautious," said Jason Yu, a broker with the Brossard-based agency Esta Agence, whose commercial and residential buyers are mostly recent immigrants from China.

Yu, who's worked with Dutch on multiple sales to Chinese buyers in Westmount, said several of his clients are wealthy Asian families moving to Montreal as part of the Quebec Immigrant Investor Program.

A decade ago, Yu and his family came to Canada from China as immigrant investors under a program that requires applicants with a net worth of at least $1.6 million to make an $800,000 interest-free loan to the government for five years.

The Quebec program — which mirrors a federal one that's now frozen and does not accept new applicants — remains hotly debated, amid criticism that 90 per cent of the mostly Asian arrivals promptly move elsewhere in Canada, while their $800,000 stays in la Belle Province.

Quebec's quota for 2013-2014 is 1,750 immigrant investors.

Despite the large number who leave, Yu says that he also sees immigrants who choose to stay in Montreal.

In the last few months, three of his Chinese clients purchased homes in Westmount, while a fourth is looking to buy downtown condos as an investment. She said the family moved to Montreal largely for her daughter's education.

One immigrant from Shanghai described how her family moved to Westmount a few years ago through the Quebec investor program. Her husband is working in China right now while she raises their daughter and takes French classes in Quebec.

“We made the decision very quickly, based largely on what a friend from China who lived in Montreal told us,” said the woman, who spoke to The Gazette on condition that her name wouldn’t be published.

“We didn’t even know about Bill 101.”

The language law hasn’t affected the family, since her daughter is enrolled at a non-subsidized English girls’ school, where she is learning both official languages.

She said she’s constantly meeting new recent immigrants from China. Last week, the woman received a call from Dutch, who had been her real estate broker when she bought her home. Dutch invited her to meet a newcomer from Shanghai who had an accepted offer on a house in the area.

Dutch also invited the newcomer’s neighbour, a recent arrival from Beijing.

“I called my client to come over because I wanted as much for her and for them to get to know each other,” Dutch said. “Everyone was busy on their iPhones, sharing contact information and yacking away in Mandarin. It was fun.

“It’s something we haven’t seen before.”

Also new is the tendency of immigrant investors — even ones who leave Quebec — to purchase properties in Montreal.

“Will they stay? History says they won’t, but they are making investments here,” said Eric Goodman, owner of Century 21 Vision in Notre-Dame-de-Grâce.

He described one new condo project in LaSalle, where 80 per cent of the units were sold to Chinese buyers, including recent immigrants, or investors who are still in China.

“They are buying them as investments and they are buying them for family members who may come in the future,” said Goodman.

“They are always looking for places to put their money. They feel it is safe to build here, even if they’re not going to make as much of a return as in Toronto.”

Goodman’s agency also sold the land to the developers behind the YUL mixed condo and townhouse project on René Lévesque Blvd. near Lucien L’Allier Rd. The YUL project, backed by Chinese investors, is being marketed to foreign as well as local buyers.

Adjacent to YUL, land on René Lévesque Blvd. next to Guy St. has been purchased by investors from Qatar who intend to launch their Babylon residential development this spring.

The downtown area has proven attractive to investors because of the large pool of student tenants, and the limited construction of new rental buildings to replace the city's aging stock.

Indeed, investors — who make up an estimated 40 per cent of owners at Seville — generated such demand for the project that people were lining up at 10 a.m., a day before the sales office opened in 2010.

Colin Danby, now condo board president for the Seville's phase 1, arrived at 3 p.m. He was No. 58 in line, he recalled. The crowd was so large that by 8 p.m., developer Groupe Prével decided to give out tickets to buyers.

And just like the hockey scalpers outside the old Forum in the 1970s, "authorized" Seville buyers were said to be hawking condo tickets on the street for $5,000 each.

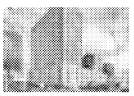
alampert@montrealgazette.com

Twitter: RealDealMtl

Previous Next

People are seen w aiting outside the offices for the Seville condos on St-Catherine St. W. in 2010.

Photograph by: Dario Ayala, The Gazette



Foreign ownership of Canadian property: More calls for the mystery numbers

November 7, 2013. 6:02 pm • Section: Real Estate, The Search

Vancouver is ranked the world's second most unaffordable city for housing. But people seem more upset about how investors are driving up property prices in London, England, which is only rated thirteenth.

Why does Canada not keep public data on investment ownership in real estate, whether by foreigners or homegrown residents? The question is starting to gain more attention than when some of us in B.C. raised it earlier this year.

With Canadian cities, especially Metro Vancouver, becoming infamous for their unaffordability in regards to real estate, another voice has been added to those urging the federal Conservative government to at least collect data on the influence of investors — foreign and otherwise — on the country's housing market.

The latest call for property ownership transparency comes on top of recent **media reports in Canada that the real estate market of London, England, has become badly distorted** by ultra-wealthy foreign owners, referred to as "non-domiciled residents." The influence of such buyers, including many Russian tycoons, is said to be causing London's housing prices to "lose touch with reality." A few excerpts from the piece by Leah McLaren:

> A British finance worker employed by a private Swiss bank recently told me at a London dinner party that he spends "at least half" his working life "buying up London real estate

> for Russian clients, simply as a place to park their money." Clients, he added, who don't pay taxes in the U.K.…
>
> So what does this mean for the people who actually live in this city? Well, for people with families and jobs and net worths well under seven figures (people, in other words, like this columnist), it's not good news.
>
> Local services like state schools and libraries are essentially ignored by non-domiciled residents, who have no real stake in their community, given that they don't actually live there. And independent businesses are suffering across London from the lack of local patronage…
>
> Increasingly, in London neighbourhoods like mine, the people who do actually live here feel resentful—and baffled—by the lives of our invisible super-rich neighbours.

If that's what Canadians and the British are saying about London, what would they say about **Vancouver, which Demographia judges the second most unaffordable city in the world,** after Hong Kong. By comparison, Demographia ranked London thirteenth most unaffordable (see chart below).

RELATED: **How much foreign ownership in Vancouver? Media has no clue.**

Vancouver planner Andy Yan fights to prevent a "zombie" city

How foreign buyers are influencing Vancouver's luxury housing market

Here is an excerpt from a new column on the need to collect foreign ownership data, by Toronto business writer David Parkinson. It's headlined: **"Canada's housing numbers don't measure up":**

> … a bigger concern are the numbers on investment activity in the housing market, particularly among foreigners. They don't exist. Last week, some of the country's top economists raised this issue with federal Finance Minister Jim Flaherty, who has acknowledged that he has no hard data on how much of Canada's housing boom has been fuelled by investors who are looking to make money as property owners rather than acquire personal residences.
>
> The distinction matters a great deal. A substantial downturn in the housing market – say, one triggered by government policy – would trigger a much bigger exodus of investors than permanent residents, and so the risks to the Canadian economy rise with the proportion of investor money pumping up the market. And yet Mr. Flaherty has been crafting policy aimed at cooling the market without that information. The Office of the Superindentent of Financial Institutions has been talking since mid-2011 about uncovering the amount of foreign investment in Canada's real estate market – and yet we still have no visibility.
>
> Cleaning up this muddle of inadequate housing data must be made top priority for Canada's financial and statistical institutions. We can't keep flying blind.

Demographia's **2013 list of world's most unaffordable cities** shows Vancouver in second place and London in thirteenth:

Appendix 9

A0000812_10-000547

Vancouver real estate: The fog of foreign ownership

March 23, 2013. 5:18 pm • Section: Immigration, Real Estate, The Search

Unlike in most jurisdictions around the world, neither Metro Vancouver, British Columbia nor Canadian government agencies keep public records on foreign ownership of real estate. They're unwilling to learn from what has been done for decades in diverse political places - such as Florida, Switzerland, Austria, Prince Edward Island, Manitoba, Alberta, Denmark, Japan, Indonesia, Bali, Thailand, Australia, Turkey, Singapore and Beijing.

Fear and resentment simmer just below the surface for most Metro Vancouverites. Yet the issue that worries so many has mostly come up against public silence. Until now.

A recent survey by the respected Vancouver Foundation found three out of four Metro Vancouver residents who had an opinion agreed with the statement: "There is too much foreign ownership of real estate here."

And Simon Fraser University explored this hot-button issue Wednesday evening in Vancouver through a panel discussion at the Djavad Mowafaghian Centre, which quickly sold out.

The speakers did what they could to respond to heated discussion of the growing housing dilemma in Vancouver, which Demographia has ranked the second most unaffordable city of 325 around the world.

The average cost of a single-family detached home has jumped in Vancouver to $1 million. Meanwhile, median incomes have barely budged for decades. Only Hong Kong is more expensive.

"Housing affordability in B.C. remains poor and worsening," says RBC senior economist Robert Hogue. Vancouver's unaffordable housing prices, he said, "depend on a constant flow of imported money."

Young wannabe homeowners are being frozen out of the city of Vancouver, as well as the North Shore, Vancouver, Richmond, Burnaby and elsewhere.

Local businesses, hospitals, organizations and universities can't recruit top candidates because even skilled professionals can't afford to live here. Like Hogue, many say the region's stratospheric prices are being heated up by real estate investors and speculators. Many are wealthy non-Canadians simply looking for a safe place to park their money.

What to do about this affordability crisis?

It's a complex question. But one of the strongest factors working against coming up with a working solution is there is no solid data on which to base a strategy.

Unlike most countries, cities and jurisdictions around the world, neither Metro Vancouver, British Columbia nor Canadian government agencies keep public records on foreign ownership of real estate.

For some unstated reason, B.C. public officials are unwilling to learn from what has been done for decades in diverse political places – such as Florida, Switzerland, Austria, Prince Edward Island, Manitoba, Alberta, Denmark, Japan, Indonesia, Bali, Thailand, Australia, Turkey, Singapore and Beijing.

Indeed, these jurisdictions do not only collect data on foreign ownership, they have brought in various taxation methods to restrict property speculation and foreign ownership, to reduce investor demand. That's what specialists say drives up prices and squeezes out locals.

UPDATE: Vancouver planner Andy Yan fights to prevent a 'zombie' city (April 20, 2013)

"Passports of convenience" stir strong Canadian disagreement (July 13, 2013)

RELATED: Chinese immigrants: Why they come, why one-third return

Mapping Metro Vancouver: The rise of ethnic enclaves

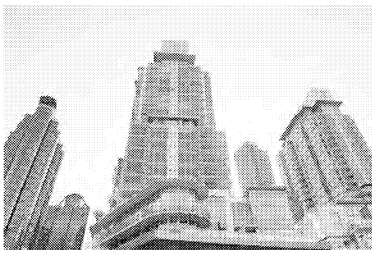
Sadly, when British Columbians are forced by politicians to operate in a vacuum about rates of foreign ownership, we are not able to fully back up our opinions in this debate – which often pits homeowners and the real estate industry against young people and renters.

One side in the dispute doesn't want to discourage foreign investment, admitting they like the out-of-country real estate profits. Some of them add that condos not filled by offshore owners can be rented out.

The other camp talks about how hard-working people deserve the chance to own a home.

And they lament that untold Metro Vancouver homes sit largely empty, without residents who would be contributing more strongly to the neighbourhood, the wider economy and the tax base.

If we are to have an authentic dialogue about these competing arguments, we need to press governments to start gathering the facts. Fast.



People have dramatically different figures on how many Vancouver condos are empty or foreign owned. Researcher Andy Yan admits it's not reliable to track the addresses to which B.C. property assessment reports are sent. Nor is it dependable to determine if condos are vacant by measuring how much electricity they use.

So far, B.C. politicians have shown no willingness to gather accurate data. As elected officials who are supposed to answer to voters, their inaction seems irresponsible.

Perhaps they fear being labelled racist. But that doesn't make sense, for many reasons.

The foreign investor debate is not about immigrants to Canada buying homes for themselves. And it should make no difference to government officials collecting property data whether non-Canadian investors come from Seattle or Dubai, Paris or Singapore.

In addition, concern about foreign ownership clearly cuts across Metro's ethnic spectrum. The Vancouver Foundation survey, for instance, found residents who speak Chinese in their homes, by a margin of almost three to one, also agree "there is too much foreign ownership of property here."

So far there has been only a handful of public figures willing to openly air this burning issue. They include Peter Ladner, former Non-Partisan Association councillor and a current fellow of SFU's Centre for Dialogue.

"Because our housing prices are around 10 times median income – with five times being 'severely unaffordable' – potential newcomers to the region stay away and the valuable workers move away," writes Ladner.

"If we are really serious about affordability in Vancouver, we would be looking at more homes for more people and fewer homes for investors and speculators."

Ladner is supported by Sandy Garossino, a prominent businesswoman and arts philanthropist. Andy Yan is another weighing in, trying to figure out the extent of foreign investment, and empty dwellings, in Metro Vancouver.

But Yan, who spoke at the forum sponsored by SFU's Vancity Office of Community Engagement and the SFU City Program, would be the first to admit he has had to use desperate measures to try to collect any sort of information on foreign ownership.

Random stories from neighbours or realtors are not enough, suggests Yan, who has been consulting for Bing Thom Architects and a committee of the city of Vancouver.

Yan uses humour to explain the research challenge: "The plural of anecdote is not 'data.'"

To determine the extent of foreign ownership, Yan also admits it's not entirely reliable to track the addresses to which B.C. property assessment reports are sent. Nor is it really dependable to determine if condos are vacant by measuring how much electricity they use. Which he has tried.

What's stopping politicians from collecting proper data?

If scores of jurisdictions around the world, including in struggling developing countries, are able to collect solid information about foreign ownership of real estate, why can't it be done in our rich, technologically sophisticated province?

Hong Kong is just one of many places getting serious about the problem of foreign ownership.

As Ladner has pointed out, Hong Kong officials have discovered that, since 2009, about "half of new luxury apartments purchased are never occupied. Is this where Vancouver is heading?"

Foreign ownership of residential property is a divisive issue, which cuts to the heart of the hopes and dreams of most Canadians. Politicians at the municipal, provincial and federal level need to respond to it in the way of scientists.

Faced with important questions, good scientists and academics don't just cast aspersions about someone else's character. They get serious about collecting evidence.

Then they move to solutions.

Only by checking the facts can our society creatively move forward for the benefit of as many Canadian residents as possible.

- 30 -

MORE: Here are some informative Peter Ladner columns on foreign ownership of Vancouver real estate:

'Fiscal reality continues to elude Vancouver real estate market' - Feb. 2013

"We need more homes for people, fewer for investors" - Jan. 2012

'Questions about affordable real estate need answers now" – October, 2011

'Foreign investors driving 'scary' real estate prices" – April, 2011

* * *

RELATED: **The Myth of Foreign Buyers?**

March 27: How much foreign ownership in Vancouver? Media shows it has no clue.

How does foreign ownership influence Vancouver property prices? Panel

Believers in God tend to be more forgiving: StudiesNext Immigration post Behind scenes, Pope advocated 'civil unions' in ArgentinaPrevious Immigration post
We encourage all readers to share their views on our articles and blog posts. We are committed to maintaining a lively but civil forum for discussion, so we ask you to avoid personal attacks, and please keep your comments relevant and respectful. If you encounter a comment that is abusive, click the "X" in the upper right corner of the comment box to report spam or abuse. We are using Facebook commenting. Visit our FAQ page for more information.

THE GLOBE AND MAIL

How Asian buyers are boosting Vancouver's luxury housing market

HADANI DITMARS
Special to The Globe and Mail
Published Friday, Jul. 26 2013, 5:27 PM EDT
Last updated Monday, Jul. 29 2013, 5:30 PM EDT

There is a buzz at the first Canadian conference of the Asian Real Estate Association of America happening here in Vancouver.

Chinese-American agents from Chicago, Kelowna-based realtors with Chinese buyers looking for vineyards and even a lone cowboy agent from Boise, Idaho, who have gathered here for a few days of seminars and contact-making are all talking about it: the much-touted "luxury-home tour."

More Related to this Story

- How about a new car with that condo?
- For Vancouver, housing and income don't add up
- New Vancouver projects target urban affordability

There is some last-minute drama from disappointed would-be tour-goers who could not secure a seat on either of the two buses taking realtors to four homes that range upwards from $9-million. And at the 11th hour, a Globe and Mail contributor is informed that "media have been banned" from entering the first house on the tour. That would be the $22.8-million, four-storey home in Upper Shaughnessy that, at a cursory glance, reveals at least 10 pages of Google entries showing every nook and cranny of the cyborg Tudor mansion that appears half pastiche-traditionalist/half state-of-the-art smart house – at least to judge from its glossy brochure.

But my seatmate, a charming Chinese-American agent from the United States, returns from the "media-free" tour of the would-be Vancouver Gatsby's abode underwhelmed. "This is not a house for the Chinese buyer," she says. "It's not contemporary enough. There's too much dark wood panelling and old-fashioned interiors."

While the 1980s wave of Hong Kong buyers, raised on British colonial tradition, might have gone for this kind of Tudor fantasia, not so for the current Asian investor. According to a recent article published in Vancouver's Chinese-language newspaper Ming Pao, the main group that is feeding this year's 70-per-cent jump in sales of homes over $4-million in Greater Vancouver

Is The Money-Laundering Driven Real Estate "Boom" Ending?

Submitted by Tyler Durden on 09/30/2012 11:42 -0400

One by one all the money-laundering loopholes in a broke world are coming to an end.

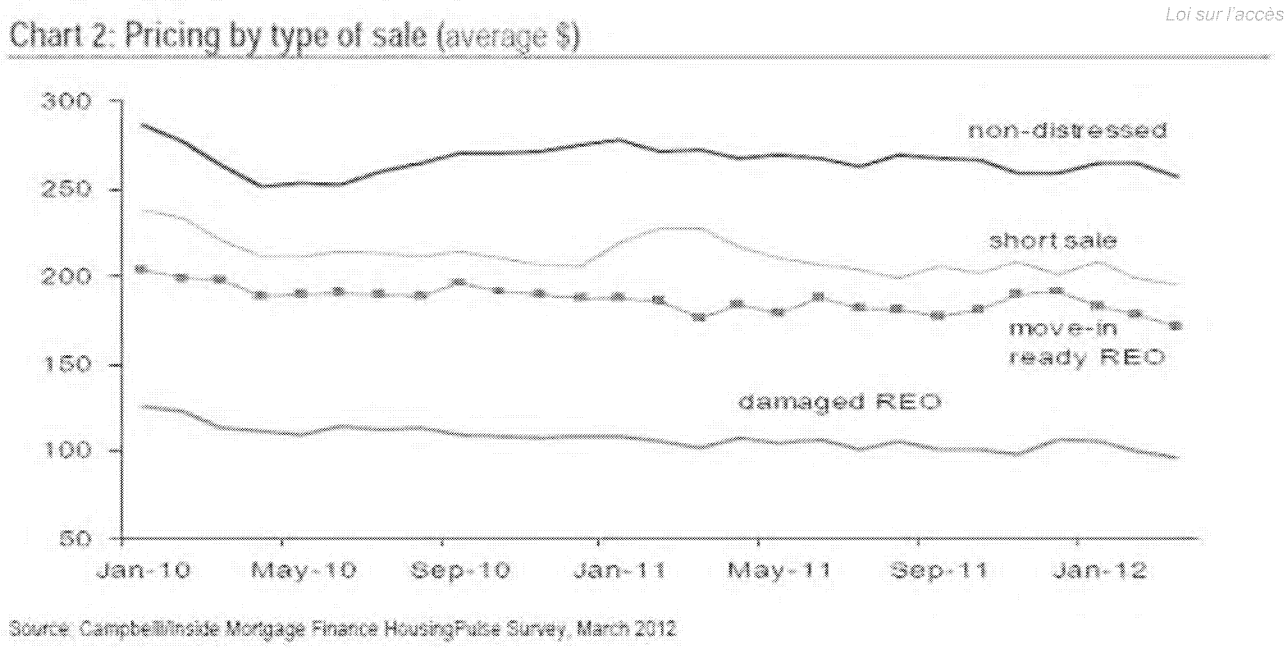
First it was Swiss bank accounts, which for centuries guaranteed the depositors absolute secrecy, and as a result saw money inflows from all the wealthiest savers in the world, who felt truly safe their wealth (obtained by legal means or otherwise) would not be redistributed forcefully. In the ecosystem of finance, Switzerland was***the*** depositor bank. Then 2008 happened, and starting with the US, shortly to be followed by every other insolvent country, demands were issued for a full list of people who had used Zurich and Geneva bank vaults to avoid the risk of asset taxation, capital controls and confiscation on their own native soil. The result was the end of the Swiss banking sector as the ultimate target of all global money laundering. In the ensuing power vacuum, others have sprung up to take its place, most notably Singapore, but its days as a tax-haven are numbered by how long it takes China to fall face first into a hard landing at which point no saving on the Pacific seaboard will be safe.

Now, it is the turn of real estate.

While hardly a secret, for decades the ultra-luxury housing segment in any country was the target not so much of local wealthy individuals and business, but**foreigners**, for whom the grass was always greener, and sought to put their money into "hard assets" abroad to save it from local confiscation. After all, it is far easier to be sued and prosecuted by your own government than a foreign one. Two very vivid examples are the most expensive house in Miami ever sold, which two months ago fetched a price of $47 million, which was purchased by "a Russian who bought the home in the name of a U.S.-based limited-liability company" and in the until recently a record $88 million paid for a 15 CPW penthouse for the daughter of Russian billionaire, Dmitry Rybolovlev (bought from Citi's Sandy "End TBTF" Weill). The record was topped at $90 million paidfor a One57 duplex apartment paid by an unknown individual, almost certainly a foreigner.

The common theme here of course is that foreigners come to the US (or London, or Geneva, or Hong Kong) or any other wealthy megapolis with their almost always ill-gotten, and untaxed gains, spend the money indiscriminately on local real estate even as the local authorities look the other way because by lifting any offer, these foreigners, while laundering illegal money, are also keeping the all important housing market afloat thus perpetuing the illusion that the domestic economic is rising. Instead all that is happening is it is attracting illegal foreign capital flows.

The biggest beneficiary so fas has been the US, which in the past 2 years has seen not one but four housing markets develop, as we have showed before.



And while the lower-end segment has continued to implode (see Foreclosure Stuffing), it is the ultra-luxury part of US housing that has bootstrapped the housing market.

For now. Because if London is any indication, global ultra-luxury real estate market is the next "Swiss bank account."

What happened in London? The NYT explains:

> ***At the request of the Athens government, the British financial authorities recently handed over a detailed list of about 400 Greek individuals who have bought and sold London properties since 2009.***
>
> *The list, closely guarded, has not been publicly disclosed. But Greek officials are examining it to determine whether the people named — who they say include prominent businessmen, bankers, shipping tycoons and professional athletes — have deceived the tax authorities by understating their wealth.*
>
> *"These people have money and they are known — but it is not clear yet if they have violated any laws," said Haris Theoharis, an official in the Greek Finance Ministry. Tax investigators have been examining the list to see whether there is any overlap between those who bought London properties and those already identified as being tax cheats.*

What a broke Greece will find without a doubt, is that of the 400 Greeks who spent millions on London real estate, virtually none paid any taxes in previous years. Also, they most certainly declared zero offshore real estate. After all why should they: until this moment foreign real estate was the default mode of funneling capital into safe destinations.

Alas, as the Swiss banking SNAFU showed, in the New Normal, nothing can be taken for granted any more. First it is Greek demands for London real estate transparency. Next it will be Putin asking Geneva and Vienna to point out which Russian oligarchs bought real estate there, then Mariano Rajoy, as broke as Greece, will ask for a list of all Spaniards buying real estate in London **and**Geneva. Until finally, someone returns the favor to Uncle Sam, who was the first to blow up the myth of Swiss bank secrecy, and requests a list of all broke European buying real estate anywhere between New York to Los Angeles.

What happens then? Well, as we have been writing for months, for now the NAR, best known for misrepresenting the real state of the existing US housing market for years, has an open waiver for anti-money laundering regulation from none other than Uncle Sam. Because while it is one thing to blow up the biggest breadwinning industry in Switzerland to pad the tax bill and to spread class warfare, it is something totally different to represent to the world that ultra-luxury segment aside, which is merely an artifact of global money laundering, the US real estate housing emperor is as naked as he was 4 years ago.

As a reminder, here is where the NAR stands on the issue of its most generous clients possibly being some of the worst criminals known to man, courtesy of Elanus Capital:

> *Many of you reading this will undoubtedly have spent time in an international bank and been forced to sit through countless hours of "know your client" and AML training. Fascinating to note that the National Association of Realtors lobbied for and received a waiver from such regulation. That's right, realtors actually went to the U.S. government and said: we want to be able to help foreign business oligarchs and other nefarious business people launder money through the real estate markets of the United States – and prevailed.*
>
> *Here's their official position:*
>
> *"NAR supports continued efforts to combat money laundering and the financing of terrorism through the regulation of entities using a risk-based analysis.* ***Any risk-based assessment would likely find very little risk of money laundering involving real estate agents or brokers****. Regulations that would require real estate agents and brokers to adopt anti-money laundering programs* ***may prove to be burdensome and unnecessary given the existing ML/TF regulations that already apply to United States financial institutions."***
>
> *Hat's off to the NAR – that is some serious doublespeak.****My translation: We'll support you as long as we don't have to support you.***

Indeed it is. What the NAR is saying is that for now go ahead and lift every offer on every duplex and triplex off Central Park. Your money is absolutely safe with us... this instant. But the second a broke Europe comes demanding reparations for endorsing 4 more years of Obama (something that wasalready documented), for destroying the Swiss banking industry, and for keeping the EUR much higher than it would have been had it not been the Chairman's 5 easing episodes, all bets are off.

This means all European, Asian, and even local oligarchs may be sweating just a little bit, now that the winds have shifted, and suddenly what was considered safe and untouchable, has become fair game in the great "fairness" redistribution scheme that is the only game left in a broke and insolvent global town.

bank accounts or between multiple trust account files established on behalf of the client or companies beneficially controlled by the client, for no apparent commercial reason or financial gain.

The services of a lawyer are especially essential in large-scale money-laundering conspiracies. Indeed, in the largest money-laundering operations uncovered by the RCMP to date, all have identified the persistent involvement of one or more lawyer in conducting suspicious transactions for clients. One such example is that of a Montreal lawyer named Giuseppe (Joseph) Lagana who was sentenced in 1995 to thirteen years in prison for masterminding a $47-million money-laundering operation.[34] Another is Basil Rolfe, a Vancouver-based lawyer who admitted to handling at least $8 million in drug proceeds between January 1993 and June 1994.[35] Lawyers are often required as part of large-scale money-laundering operations because the greater the quantity of cash generated by the criminal enterprise, the greater the need for increased sophistication in the laundering scheme. In turn, this increased sophistication requires the expertise of white-collar professionals working to construct and navigate the laundering operation through the complexities of the legitimate business and financial world.

In short, the nature of the involvement of lawyers in money laundering is dictated by the complexity and sophistication of the laundering operation itself. In rudimentary schemes such as those involving the simple purchase of a home, a lawyer is not sought out by the money launderer but becomes involved out of the necessity to involve legal professionals in real property transactions. In these cases only a limited range of services are offered by the lawyer, who is generally not in a position to detect a suspicious transaction or client (especially given the lack of due diligence conducted on clients). In larger, more complex laundering schemes, there appears to be a concerted effort by criminal offenders to seek out and involve lawyers. In these cases, lawyers are more actively involved in providing a wide range of services specifically tailored to money laundering and often appear to be in a position where there is a greater chance that they are cognizant of the criminal source of the funds.

Lawyers and Real Estate Transactions

The instances where lawyers came into contact with the proceeds of crime are mostly the result of the popularity of real estate as a money-laundering vehicle, combined with the necessary role of lawyers in real

estate transactions. Typical services provided by lawyers to clients purchasing real property include conducting lien searches, obtaining property tax information, calculating property tax payments for the buyer and seller, obtaining information on insurance requirements, preparing title transfer and mortgage documents, registering the transfer of title, and receiving and disbursing funds through the law firm's trust account as part of the real estate deal, including deposits, down payments, 'cash-to-close,' and mortgage financing.

In a case we have previously discussed, Frederick Tatum, a principal player in a New York-based Jamaican drug trafficking group, arranged to have large amounts of cash physically smuggled into Canada by family members who then laundered the money through financial institutions, law firms, and real estate transactions in Toronto. The drug cash was often taken directly to D. Charles English, a real estate lawyer who was frequently involved in facilitating real estate transactions by family members with tainted funds. A ledger seized from English's law office indicated that the amounts of cash provided to him on any single transaction ranged from U.S.$11,000 to $65,000, much of it in $100, $50, and $20 bills. Most of the real estate purchases made by Tatum family members were immediately preceded by large cash deposits into their lawyer's bank account. Between 1995 and 2000, the period in which Tatum was most active in the drug trade, family members purchased and sold more than forty homes in the Greater Toronto Area. Title to most of these properties was registered in the name of family members or companies controlled by them. In addition to facilitating the purchase and sale of these properties, English was also involved in drafting mortgage contracts, which in many of the property purchases were purportedly between members of the families, but which police ultimately traced to Frederick Tatum's drug revenues. In six real estate transactions, the total cost of the properties was CDN$1,382,696 and of this total, $940,396 was allegedly financed by various family members. English was also a registered owner of three properties, co-owned by two of Frederick Tatum's sisters.

The lawyer's role was significant. A vast number of real estate transactions conducted by family members involved the family's lawyer. On 15 August 2001, a search warrant was executed at English's law offices and in response, the lawyer asserted a claim of solicitor-client privilege on behalf of his clients. However, on 19 December 2001, a judicial order was issued that the documents seized from the law office be turned over to the RCMP. These documents became essential evidence in the

proceeds of crime investigation. Although homes registered in the names of family members were forfeited as the proceeds of crime, the lawyer was never charged.

Incorporating Companies

Lawyers are often used in a number of capacities to facilitate laundering schemes involving criminally controlled companies. First, they are used to incorporate companies, which includes completing all the necessary paperwork, filing the appropriate incorporation and tax documents with government regulatory bodies, setting up bank accounts, and establishing a board of directors. Second, a lawyer may act as a director, officer, trustee, and, in some cases, the owner or a shareholder of the company. Third, if the company operates a legitimate business, the lawyer may manage its ongoing legal, administrative, and financial affairs. Fourth, lawyers have been involved in fabricating accounting and legal documentation. Fifth, a law office may be used as the corporate address for a company controlled by a criminal entrepreneur. Sixth, lawyers have been used in some cases to deposit the cash proceeds of crime into bank accounts, including legal trust accounts, under the guise of legitimate revenue derived from a company.

During one proceeds of crime investigation into three Alberta-based cocaine and marijuana traffickers, named Jake Dowling, Mark Shields, and Sam Zimmerman, police identified three lawyers who helped the accused in setting up and operating companies which were eventually proven to be nothing more than money-laundering vehicles. Documents seized by the RCMP indicated that Sherry Howell acted as legal counsel on behalf of Dowling in the incorporation and preparation of annual returns for DowlShields Investments Inc., a public company in which Dowling and Shields each held 50 per cent voting shares. The corporate address listed for this company was Howell's law office. Documents seized by police from the law office of Howell also showed that she represented Dowling in the purchase of real estate, the title of which was registered in the name of DowlShields Investments Inc. Among the documents were letters from Howell addressed to the company, including certificates of incorporation, bank statements for commercial accounts, and documents showing that Dowling and Shields were directors and shareholders of the company. Another lawyer acted on behalf of Dowling in incorporating a numbered company, conducting real estate transactions on behalf of Dowling or numbered companies he controlled, purchasing a car wash, and preparing lease agreements between Dowling and the tenants of a home that was used for a marijuana grow operation. Finally, documents seized by police indicated that Gordon Hoffner, a partner in a local law firm, acted on behalf of Mark Shields and Sam Zimmerman in the incorporation of three other Alberta companies.

Legal Trust Accounts

Criminal revenue is often placed in a law firm's bank account in the name of the offender, a nominee, or a company associated with the offender. In the majority of the police cases, trust accounts were simply used as part of the normal course of a lawyer's duties in collecting and disbursing payments for real property on behalf of a client. Regardless, the significance of a legal trust account in the context of a money-laundering operation should not be underestimated: it can be used as part of the initial first step in converting the cash proceeds of crime into other less suspicious assets, it can serve to help hide criminal ownership of funds or other assets, and it is often used as an essential link between different money-laundering vehicles and techniques, such as real estate, criminally controlled companies, nominees, and the deposit and transfer of illegal revenues. In short, a legal trust account can be used in all four stages (placement, layering, integration, and repatriation) of the money-laundering process.

In one case, Peter Humber used the proceeds from the sale of cocaine, marijuana, and steroids to purchase several homes throughout British Columbia. He admitted to an undercover police officer that he regularly provided cash to his lawyer who would then deposit the funds into his law firm's bank account, $4,000 to $5,000 at a time. When the balance of the account reached a certain level, Humber would use the funds to purchase property. The same lawyer represented Humber in the purchase of most of these properties. Police were able to prove that many of the homes were purchased with the proceeds of crime and used as locations for marijuana grow operations. When asked about his money-laundering operations by an undercover police officer, Humber explained that he purposely used legal trust accounts to help block access to information about the true ownership of funds in the account. Humber boasted to the police officer that legal trust

accounts are 'safe havens' because the police, taxation officials, or the 'bar association' could not readily access them.

Lawyers Handling Cash

In some of the police cases, a lawyer or a delegate within a law firm physically handled cash directly generated from criminal activities. In most of these cases, the cash was provided to a lawyer in the context of a real estate transaction and these funds were deposited in trust for the client. However, in other cases, there was no real estate transaction involved and, in fact, no rational explanation why the client was providing large amounts of cash to his/her lawyer.

For example, on 2 October 2000, Rob Cheney was convicted in Edmonton for drug trafficking and received an eighteen-month sentence. The proceeds of crime investigation showed that Cheney had amassed considerable assets over the years, despite the fact that he had no legitimate source of income. Cheney laundered his drug profits through banks, companies he established, legal trust accounts, and real estate. Real estate purchases would often be financed in part through funds from legal trust accounts filled with deposits of cash directly generated from drug sales. Cheney used different lawyers and law firms to facilitate his laundering activity, including Ron Day of Day and Company, Barristers and Solicitors, and Lester Barry of Barry, Egbert, Krauss (and formerly of Day and Company).

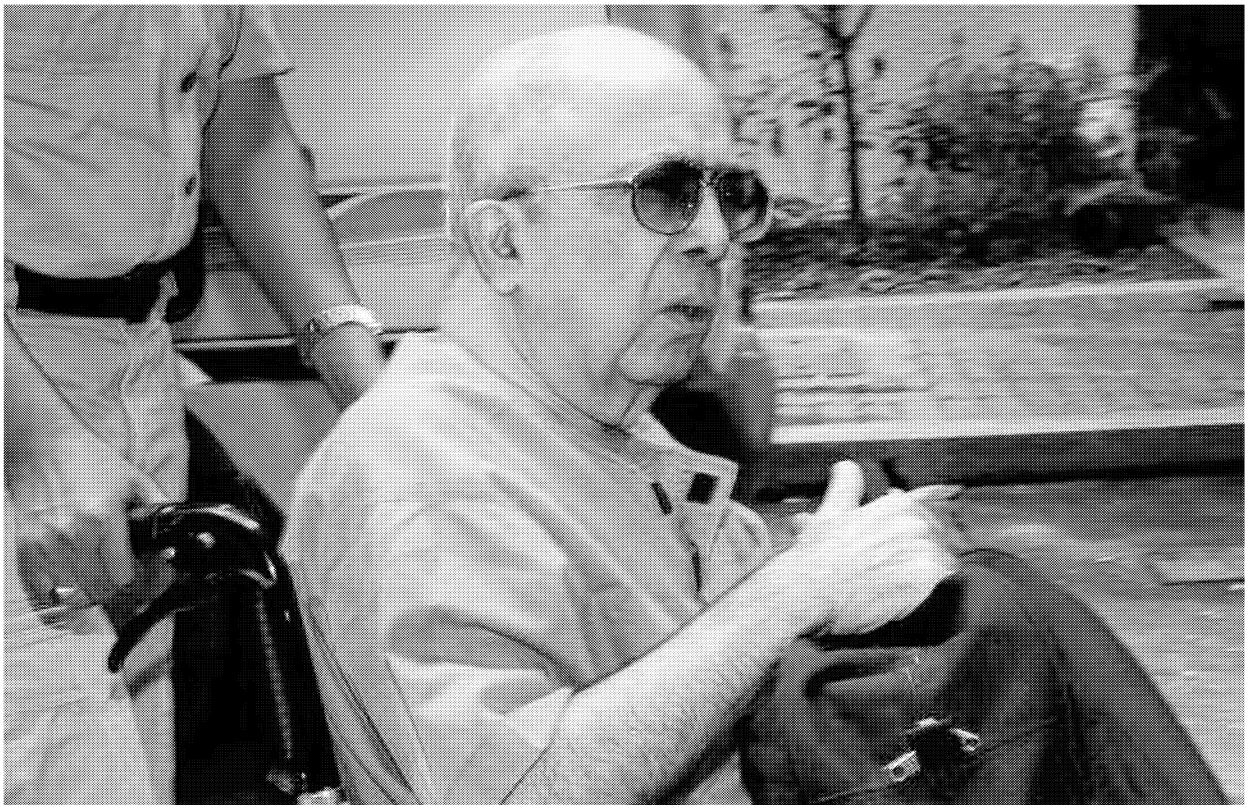
The services provided to Cheney by the law firms included facilitating the purchase of real estate, setting up and maintaining shell and active companies, and accepting large sums of cash from Cheney. Ron Day personally made many of the cash deposits in trust for Cheney. Police seized a number of deposit slips, dated between 17 July 1993 and 18 April 1998, indicating that Day had deposited $285,000 (ranging from $19,000 to $70,000, mostly in Canadian $100 bills) on behalf of Cheney. All of the deposit slips included the signature or initials of either Ron Day or Lester Barry. Police intercepted a phone conversation in which Cheney described how he once visited his lawyer with a suitcase containing $150,000 in cash, which was subsequently deposited for Cheney in trust. In another phone conversation, Cheney was heard to say that his lawyer accepted a suitcase with $60,000 in cash, which was also deposited into the trust account. These funds were then used to purchase a Porsche 911 for Cheney. In another phone conversation, Cheney directed an accomplice to deposit $35,000 in cash into Cheney's lawyer's trust account.

Accountants

Like a legitimate company, criminal entrepreneurs must keep track of their revenue and expenses, as well as assets and liabilities, and ideally this job is best carried out by someone possessing accounting or bookkeeping skills. Although criminal organizations parallel legitimate businesses in many ways, they are unique in that few businesses purchase millions of dollars in product using cash. The principal job of an accountant working for a successful criminal enterprise is to keep track of the volumes of cash generated by drug trafficking and other profitable crimes. In police cases where accountants were implicated in laundering money, they were used to provide accounting services for both the personal and company-related finances of criminal entrepreneurs.

The need by large-scale criminal operations for accountants was made vivid during a trial of Hells Angels' members and associates in Quebec. Stephane Sirois, a former member of the Rockers – a biker gang affiliated with the Nomads Chapter of the Hells Angels – testified in court that the Nomads purchased as much as 1,000 kilograms of cocaine at a time, which would then be distributed to members of the Nomads and other Hells Angels' chapters for wholesale distribution. The drug revenues were collected by couriers who carried bags of cash to nondescript apartments where they would be counted. By the end of their investigation, police had seized $5.5 million in cash from safes located at various apartments. Police also confiscated accounting spreadsheets which indicated that in one eight-month period in 2000, the Nomads made $92 million from the sale of cocaine. In one recording taped secretly by Sirois, he is heard asking another Rocker named Jean-Guy Bourgoin if he knows of a good accountant. Bourgoin replies with the name of Georges Therrien in Laval. 'He's one hell of a good guy,' Bourgoin responds. 'He worked twenty-five years for the government. And he was Rizutto's accountant – he's always worked for that Italian clique. You give him cold cash – 'Here, wash this for me' – and he will play with your money.' Bourgoin was most likely referring to Vito Rizzuto, described by police as the head of Montreal's leading Mafia family.[36]

Other than the necessity of tracking large amounts of cash in small denominations, police cases show that the tasks performed by accountants for criminal entrepreneurs are no different than that which they perform for legitimate clients. Large-scale criminal entrepreneurs require accountants to help not only with their own personal finances but also with the companies that have been set up to clean their illegal



Rakesh Saxena, a former adviser to the Bangkok Bank of Commerce, in a wheelchair is pushed by a prison official upon his arrival at criminal court in Bangkok, Thailand Friday, June 8, 2012. Saxena, 60, an Indian national, was sentenced to 10 years in prison and ordered to pay US$41 million in fines and compensation for embezzlement that helped spark the 1997 financial crisis.

Photograph by: Apichart Weerawong , AP Photo

Rakesh Saxena, the former Thai bank official who holed up in Vancouver for 13 years while fighting extradition on embezzlement charges, has been sentenced to 10 years in jail in Thailand.

Saxena, 59, was found guilty on five counts of securities fraud between 1992 and 1995, having siphoned off tens of millions of dollars from the now defunct Bangkok Bank of Commerce, where he was employed as an adviser.

The scandal caused a run on bank deposits and led to the bank's collapse, contributing to the devaluation of the baht and a regional crisis.

Saxena was arrested by RCMP in Whistler in 1996, but staved off extradition until October 2009, when the Supreme Court of Canada refused to hear his last-ditch appeal, officially ending the longest extradition proceeding in Canadian history.

The Bangkok South Criminal Court was told how Saxena had set up 60 businesses in Thailand and used them to secure loans from the bank to cover debts and running costs, but instead channelled the money into personal accounts, mostly in Switzerland.

"The defendant clearly demonstrated his intention to take funds from the damaged party to invest for his own personal use, depositing the funds into several overseas accounts," the judge said in reading the verdict.

Estimates of the money he stole from the bank vary from $60 million to $82 million. The court did not give a total.

Saxena, wearing orange prison fatigues and in a wheelchair, appeared frail and confused as the sentence was passed. He was also ordered to pay 1.13 billion baht ($35.8 million) in damages and a 1-million baht fine.

For 13 years and three months, Saxena fought extradition at every possible turn, costing Canadian taxpayers millions of dollars.

During most of this time, he lived in the relative luxury of house arrest — albeit at his own expense — first in a False Creek condo, and later in a more spacious house in Richmond's Terra Nova area.

During this period, he wreaked havoc on the financial market, mainly by promoting essentially worthless stocks that trade on the U.S. over-the-counter markets.

He conspired with Vancouver crooks and securities offenders to cheat investors, both here and abroad. Among them were Summerland bank robber Luke Sommers; as well as Toronto stockbroker Stephen Taub and West Vancouver stock promoter Don Rutledge, both certified stock offenders.

He was the consummate tar baby: Almost everybody who came within his orbit — brokers, lawyers, politicians — seemed to be caught in his web of deception. Many sued for redress, many more were sued by Saxena, who used and abused our courts for his personal purposes. (Court records show he was a plaintiff or defendant in 36 different lawsuits filed in B.C.)

Police and securities regulators, for the most part, stood by and did nothing, trusting he would soon be extradited. He also had a lawyer-like ability to orchestrate deals to keep himself legally onside, even though he was morally offside. In 2005, after it became apparent that he had arranged for European boiler rooms to flog worthless stock, he insisted he was simply an intermediary and not a party to any of the contractual arrangements. "It's a thin red line, I grant you, but it's still a red line," he told me.

He also managed to embarrass Canada internationally by plotting a military coup in Sierra Leone while in custody at the police lock-up at 222 Main Street.

After news of the planned coup leaked to the media, which forced him to cancel his plan, he cheekily told reporters there was nothing in the terms of his detention preventing him from plotting coups in foreign countries. The embarrassing part was that he was right.

His most remarkable characteristic was his patience and resilience. There are not many people who could spend so much time in a cage, albeit a gilded one, without any apparent distress.

Even on Friday, when it appeared that all was lost, he wasn't about to give up.

"We have to appeal, of course," he told reporters. "This sentence is absolutely wrong … Nobody in this country knows the financial laws. It's the Bank of Thailand and the prosecutors who are to blame."

dbaines@vancouversun.comWith files from Reuters

FACTIVA DOW JONES

BBC

Chinese suspect in smuggling case released into Canadian house arrest.

282 words
10 March 2001
07:20
BBC Monitoring Asia Pacific - Political
BBCAPP
English

Text of report by Radio TV Hong Kong audio web site on 10 March

Fugitive Lai Changxing and his wife Tsang Mingna have been released from the custody of Canadian police and allowed to return to their **luxury home** under an elaborate and costly plan for house arrest. Beijing is seeking Lai's extradition back to the mainland, where he is wanted as the alleged king-pin of a multi-billion-dollar smuggling ring. But Lai is fighting the move, saying he would likely face execution just like 14 people who have already been sentenced to death for their involvement in the racket. Francis Moriarty reports.

[Moriarty] In street clothes, no longer wearing handcuffs, and described by their lawyer as delighted to end their three-and-one-half months in detention centre, Lai and Tsang were returned to their condominium, where they will live under a house arrest scheme including electronic surveillance and round-the-clock guards, for which they will pay 13,500 US dollars a week. An immigration adjudicator rejected pleas by immigration officials to keep the pair incarcerated, releasing them instead to their luxurious residence in Burnaby, British Columbia. The couple entered **Canada** two years ago using Hong Kong passports and were later arrested. They subsequently sought asylum as refugees, and immigration officials had argued the pair should be kept in custody, because given their wealth and the likelihood of a death sentence on the mainland, they would probably try to flee if they lost their bid for refugee status and faced extradition.

Source: RTHK Radio 3 audio web site, Hong Kong, in English 1000 gmt 10 Mar 01.

Document bbcapp0020010710dx3a004wn

Lai Changxing leads very lavish lifestyle in Vancouver, court told

posted 5/04/2007 12:12:00 AM

CIV - China's most wanted man Lai Changxing is leading a lavish lifestyle in Vancouver where he rents an apartment in the super upscale Coal Harbour area, drives a $150,000 BMW and dines out every night at very expensive restaurants, according to court documents.

Interestingly, Lai has been driving in Canada for years without a license and has been observed to have an "erratic driving habit".

Lai was arrested on April 19, 2007 at 11:30 a.m. by police accusing him of breaching his release condition, just three hours before an abjudicator of the Immigration and Refugee Board delivered his decision to lift all curfew on Lai.

According to standard procedure, Lai was entitled to a detention review within 48 hours of his arrest. The transcript of the April 20 hearing shows us the first detailed description of Lai's life in Canada, after almost 8 years he came to Vancouver.

Providing all the interesting details on the detention hearing was Katherine Fast, an inland nforcement officer with the CBSA. She led a 10-officer team to conduct a 7-day close survellance of Lai Changxing in February. Fast's duty was to present facts that Lai did breach his conditions as he quite frequently leaving home before and coming home after his allowable time. Immigration and Citizenship Canada wanted to demonstrate that his lavish lifestyle has much to do with his breaching of curfews.

Fast indicated that Lai drove a $150,000 black BMW and a Lincoln Town Car. His last known address was an apartment unit on 1300 block of W. Pender, the centre of the expensive Coal Harbour area.

Lai eats out every day at least for dinner, if not lunch and dinner at "very expensive Asian restaurants mostly," Fast said.

Fast recalled one occasion in which Lai treated 6 other individuals at Kobe Japanese Restaurant on Alberni St. "They were in a private room in the back and we were informed by the staff the bill was hundreds of dollars."

The people Lai hangs around seem to be affluent, too. "There's constant meets with other people in very expensive vehicles. There was Mercedes, Lexus, BMW's. He went to very expensive homes, million dollar homes, in Shaughnessy, Surrey, Richmond," Fast said.

"Several of the homes had sophisticated surveillance equipment attached to the home. It wasn't your regular routine home alarm."

Fast described there seemed to be "every day a constant buzz."

Lai Changxing loves driving. He drives even if he's visiting a restaurant just two blocks away.

"I should mention that his driving habits and behaviour is erratic at best. He tends to drive well under the speed limit at times and then at other times, particularly one day on the highway he was recorded at going over 140, 150 kilometres an hour," Fast said.

She said that, to her best knowledge, Lai does not have a proper driver's license. "My understanding is that he continually fails his driving test."

And that may be why the Lincoln he drives is registered under a female name with him listed as the principle driver.

Throughout the 7 days, Lai was able to get away from surveillance from time to time. Fast was certain that Lai knew some "counter surveillance" tactics.

"That particular evening there were, I believe there five -- one, two, three four -- there were five vehicles parked outside Angus Drive. There were approximately 20 to 25 people that exited the house at the same time, including Mr. Lai," said Fast. "An unknown Asian female got into the BMW and blocked our lead car from following Mr. Lai."

And Lai's behaviour during the surveillance acted strange sometimes. For instance, on a Friday, Lai spent most of the day driving all over town, stopping at various places for no more than 5, 10 minutes at the most.

"He went into three separate different alleyways, left the car running, people would come to him into the vehicle. They would then get -- either get in the vehicle with him, stay there briefly, and then leave."

The government lawyer J. Davidson believed he had made a very good case that Lai constantly broke the rules and that stringent restrictions should be maintained on him.

However, the adjudicator said these arguments have been settled by another adjudicator on April 19, which lifted all his curfew.

Adjudicator Tessler said the CBSA has numerous chances to arrest Lai for repeatedly breaching his restrictions. However, CBSA has been excusing him until April 19, just three hours before the curfew review decision was to be released. The timing of the arrest was questionable.

Tessler said the detention hearing was not about appealing to a previous IRB decision. If so, CIC should address the question in a federal court.

Lai was released.

http://chineseinvancouver.blogspot.ca/2007/05/lai-changxing-leads-very-lavish.html

FACTIVA DOW JONES

Court documents say alleged dragon head laundered triad cash in Canada

BY DENE MOORE

CP
732 words
3 March 2013
17:31
The Canadian Press
CPR
English

VANCOUVER _ An accused triad leader from Macau laundered millions of dollars of dirty money in Canada as immigration officials waited over a decade for access to police wiretap information that allowed them to move to have him deported, court documents show.

Lai Tong Sang, the alleged ``dragon head'' of the Shui Fung gang who fled a bloody turf war by coming to Canada, was the subject of an investigation by the Integrated Proceeds of Crime Unit, according to documents filed with the Federal Court of Canada in Vancouver.

``I was informed that although the subject's financial record and transactions indicate trends of money laundering activity, they did not have sufficient evidence to meet the criminal standard of proof beyond a reasonable doubt,'' says the December 2011 report by Canada Border Services Agency.

However the standard of proof in an immigration matter is less than in a criminal court, it notes, and immigration officials point to a report from FINTRAC _ Canada's financial intelligence agency _ to contend there are reasonable grounds to believe Lai ``was or is'' involved in money laundering activities. From Oct. 15, 2002 to Nov. 8, 2006, investigators tracked 49 separate electronic funds transfers.

The transactions amounted to $2.1 million and US$140,000, the report stated.

Lai and his wife, accompanied by their three minor children, arrived at Vancouver airport on Oct. 28, 1996, under a permanent resident visa.

His immigration made headlines, as he was well known in Macau media as the head of the Shui Fung, or Water Room, gang.

But it wasn't until July 2011 that immigration officials completed reports alleging Lai was not admissible to Canada due to his ties to a criminal organization.

In November 2011, Lai filed an application with the Federal Court for a judicial review of the agency's decision to try and have him removed from Canada.

The then-14 year delay was ``unreasonable and prejudicial to Mr. Lai and his family,'' argued his lawyer, Peter Chapman.

``Previous investigations were done and the government apparently decided not to take proceedings to cancel Mr. Lai's permanent resident status,'' Chapman submitted to the court.

But that was not the case, say documents filed with the court.

``It should be noted that it is extremely difficult to investigate or prosecute members of organized crime, given that they are often sophisticated, very mobile, have access to vast resources and use violence or threats to intimidate witnesses,'' says a report by Citizenship and Immigration filed in court.

Evidence from wiretaps and police investigations was not able to be released at the time that Lai arrived in Canada and was the target of an assassination attempt by gang rivals, says the report.

During three days of hearings before the Immigration and Refugee Board last week, police witnesses described the intertwined criminal investigations that touched Lai's case.

The assassination plot was linked to Simon Kwok Chow, the purported leader of the rival 14K triad in Vancouver. Chow was convicted of the first-degree murder in February 2001 in an unrelated case and sentenced to life in prison.

Chapman argued there is no allegation that Shui Fung was engaged in activities that constituted indictable offences in Canada. Not so, said immigration officials.

``Information within the disclosure packages indicates that the Shui Fong were involved in various criminal activities, but not limited to, murder, assault, extortion, gang fighting, illegal gambling, and living off the avails of prostitution,'' says the report.

Lai's membership in the Shui Fung is lifelong, says the report, ``even if he is not active in criminality in Canada.''

Lai first applied for permanent residence in February 1994, an application that was referred for enhanced criminal checks because of his membership in a triad organization, say the court documents.

With that process stalled, Lai sent a letter March 15, 1996, withdrawing the application in Macau. He had filed an application in Los Angeles two weeks earlier, on March 1.

Lai did not attend his IRB admissibility hearing in person, but called in from Macau. His wife and children do live in Metro Vancouver, and immigration officials are seeking to have them removed on the grounds that material facts were misrepresented in their visa applications.

A decision is not expected in his case for several months.

20130303CPCPG1322

The Canadian Press

Document CPR0000020130304e9330003u

Search Summary

Text	Alleged dragon head laundered triad cash in Canada
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	All Regions
Language	English

Lai Tong Sang’s luxury house in Vancouver’s Fraserview neighbourhood was the target of a drive-by shooting in July 1997.

Lai Tong Sang’s luxury house in Vancouver’s Fraserview neighbourhood was the target of a drive-by shooting in July 1997.

FEBRUARY 3, 2013

Lai Tong Sang's luxury house in Vancouver's Fraserview neighbourhood was the target of a drive-by shooting in July 1997.

FACTIVA DOW JONES

TORONTO STAR

News

Family brawl enthralls Asia; Gambling tycoon sues Canadian children over alleged coup as offspring, wives fight over empire

Tony Wong **Toronto** Star

1431 words
28 January 2011
The Toronto Star
TOR
ONT
A1
English

When asked about his biggest regret, billionaire gambling magnate Stanley Ho was surprisingly candid.

"Time is something you have to sacrifice," he told me in his first Canadian media interview in 1990. "You can't go from 9 in the morning and stop at 5. That's why I admit I'm not a very good husband, and not a very good father. It's tough, because you can't spend the time."

More than two decades later, Ho's worst nightmare - perhaps the worst nightmare for any Asian family that values a sense of harmony above almost everything else - has come true.

A bitter feud between his three surviving wives and 17 children over the family empire burst into the open this week and has become Asia's leading soap opera.

Foremost among the squabbling factions are Ho's five Canadian children, including trusted confidante and businesswoman Daisy Ho, a University of **Toronto** graduate, and second wife Lucina Laam, who decorated a luxurious mansion the family still owns on the **Bridle Path**.

The faction is led by Daisy's Canadian sister Pansy Ho, owner in her own right of a gambling franchise, and one of the most prominent and powerful businesswomen in Asia.

The stakes in the bizarre saga that unfolded this week are high.

Ho transformed the sleepy former Portuguese colony of Macau into a gambling mecca in the 1960s.

Its gambling revenues are now more than three times those on the Las Vegas Strip.

And taxes on Ho's companies account for about a third of all the government revenues in Macau. Forbes places his wealth at $3.2 billion, but some analysts feel the figure could be much higher.

The 89-year-old is unquestionably China's most flamboyant billionaire. He loves ballroom dancing and is famous for a succession of wives. (He acknowledges children from four; the first wife is deceased.)

The family feud came to light this week when Ho declared his third wife, Ina Chan, and five Canadian children had improperly taken control of a 31.7 per cent stake in the holding company that controls his wealth.

He then appeared to retract that in a televised interview with family members at his side, saying he had given written consent to the transfer and no longer needed the lawyer he had hired to contest the matter.

Hours later, however, a writ of summons was filed in Hong Kong High Court, formally stating the original claim.

The feud began last month when Ho apparently handed over controlling interest of SJM Holdings, which owns 20 of Macau's 33 casinos, to Laam and Chan and their offspring. This apparently did not sit well with the family of wife No. 1, Clementina Leitao, who died in 2004. Those children say they have been left out in the cold.

"I cannot believe that my father would leave my mother's family with nothing at all," said daughter Angela Ho. "My father speaks to me often and has stated publicly about how he intends to divide his estate evenly amongst his children."

It was Leitao's standing in Portuguese society that allowed Ho to start his gambling empire, according to Angela Ho. (Macau is a former Portuguese colony.)

Relations are also believed to be tense between family members and Angela Leong, Ho's fourth wife, who has an 8 per cent share in the casino operation, which makes her a strong contender to take over that part of the business.

But so far it looks like the Canadian faction is winning.

The Canadian children and mother appear to control much of Ho's wealth through shares of Lanceford, his private holding company. Through Lanceford, Ho has a vast fortune in **real estate**, transportation, infrastructure and gaming. There are also investments in Portugal, Vietnam and North Korea.

The Canadian children retain strong ties to **Toronto**. They still own the home on High Point Rd. in the **Bridle Path**, purchased in 1987 for a record $5.5 million.

They also own the landmark Sutton Place hotel on Bay St., a popular hangout during the **Toronto** International Film Festival.

The Hos also own Sutton Place hotels in Canada and in the United States. Sources told the Star the **Toronto** hotel has been conditionally sold to a domestic buyer. That buyer has until next month to do due diligence on the **property**.

The Sutton Place Vancouver and the Sutton Place Edmonton are also "under contract," meaning that they are also conditionally sold in what could be one of the largest hotel deals this year, said the source. The U.S **property** based in Chicago has not been sold.

The Ho children keep a relatively low profile while living in **Toronto**.

Shy and retiring, Daisy Ho did her MBA at the University of **Toronto** and was the former president of the alumni association in Hong Kong. Lawrence, the youngest son, who earned his bachelor of commerce at the University of **Toronto**, is a hockey nut who plays in a league in Macau. They and Pansy are Canadian citizens.

Daisy is the chief financial officer of Shun Tak, her father's transportation and **real estate** holding company, and has long been a trusted confidante. But it has not been easy living under his giant shadow.

"Why am I my father's daughter?" she told me in an introspective interview over lunch in Hong Kong. "And if I am not my father's daughter, would I be happier?"

When I last asked in 2007 whether her father had a succession plan, Daisy Ho shook her head.

"Nobody would discuss that with dad because, for one thing, he's still going so strong. He still is very hands-on in business, although he's given us a free hand in the day-to-day operations of the company."

The drama still has to be played out. And of course Ho is still very much alive. His life story, from rags to the god of gambling, is familiar to China's one billion people.

Stanley Ho's father, the scion of one of the best and oldest families in Hong Kong, lost everything on bad stocks in the 1930s. He decamped for Saigon, leaving his wife and 13 children behind, penniless.

"People would turn their face on me when they saw me on the street. I learned how to be truly humble," Stanley once told the Star.

To avoid a lifetime of menial jobs, he worked hard and won scholarships to Hong Kong University.

"When war broke out, I started all over again in Macau, working for a Chinese, Portuguese and Japanese company," he said. "It was easy to make your million then."

After the war Ho returned to Hong Kong and invested in **real estate**. In 1962, he won the public tender for Macau's gambling monopoly.

Ho lost his monopoly when the Portuguese colony reverted to Chinese rule in 1999 when U.S. and Australian companies invaded the market. But this also created opportunities for Ho, who still controls at least a third of Macau's gambling thanks to his Canadian family forming strategic alliances.

His son Lawrence co-owns Melco Crown Entertainment with James Packer, Australia's richest man. Pansy and Daisy are co-owners of MGM-Macau, which also competes with their father's famous Lisboa brand casinos.

Despite running a major gambling company, Daisy Ho does not gamble herself. She learned her lesson after losing $20 at a casino table during a Mediterranean cruise.

Billionaire Stanley Ho poses with family members last fall at Government House in Hong Kong. A dispute over the fate of his fortune has erupted. A DYNASTY DIVIDED: Shown in the photo above are just some of the feuding Ho family members. Stanley Ho has 17 children with four women he calls his wives. The first wife is deceased. Pictured, from left, are 1: Florinda Ho, Ho's daughter by his third wife 2: Alice Ho, Ho's granddaughter by his fourth wife 3: Angela Leong, Ho's fourth wife and a key shareholder in his empire 4: Stanley Ho, billionaire gambling magnate 5: Lawrence Ho, Ho's Canadian son and partner of Australia's richest man in a casino company 6: Pansy Ho, one of Ho's Canadian children, widely viewed as her father's successor 7: Daisy Ho, another of Ho's Canadian children, CFO of one of his holding companies. AFP/GETTY IMAGES

Toronto Star Newspapers Limited

Document TOR0000020110128e71s0002p

Search Summary

Text	("bridle path" OR "post road") AND toronto AND ("real estate" OR Property)
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	English

TORONTO STAR

Greater Toronto

Fugitive's flight ends; Man accused of embezzling millions in Kazakhstan lived in luxury in King City until arrest this month

Emily Jackson Toronto Star

550 words
20 February 2012
The Toronto Star
TOR
ONT
GT1
English

A Kazakh **fugitive** accused of embezzling about $20 million from his homeland was living in a lavish King City **mansion** until his recent arrest.

Accused in Kazakhstan of **fraud**, counterfeiting and organized **crime**, Rustem Tursunbayev's life on the run from the law ended when Toronto police and the **Canada** Border Services Agency arrested him on an immigration warrant Feb. 10.

"He is believed to be inadmissible to **Canada** under the organized **criminality** sections of the Immigration and Refugee Protection Act," CBSA spokeswoman Antonella DiGirolamo wrote in an email.

Tursunbayev, 49, is believed to have lived in the GTA since he entered **Canada** as a permanent resident in July 2009, police said.

Property records show Tursunbayev and his wife, Nataliya, bought their four-bedroom, seven-bathroom **house**, complete with a pool, for $3.6 million in August 2009.

His wife chronicled the transition to Canadian life on her blog, written in Russian. "Good or bad is not yet clear. On the one hand, well, that we are in a new free country; on the other, sadly, without relatives and friends," she wrote on Dec. 30, 2009.

Last August, Interpol issued a "red notice" - which seeks the arrest of a person with a view to extradition - indicating Tursunbayev was wanted in Kazakhstan. Less than a month later, Tursunbayev sold the **mansion** to his wife for $2.

A woman who answered the phone at the King City **home** confirmed Tursunbayev was arrested, but refused to comment further.

Tursunbayev appears to have been self-employed and working in the money markets during his time in **Canada**, said **fugitive** squad Det. Rick Mooney.

Tursunbayev will remain in custody until his next detention hearing because he is "unlikely to appear for immigration processes," according to Immigration and Refugee Board spokeswoman Anna Pape.

It's not clear exactly what prompted the charges from Kazakhstan. Tursunbayev has ties to the state-owned nuclear company Kazatomprom, which was embroiled in a corruption scandal in 2009.

He served on the board of the World Nuclear Association from 2004 to 2006, the association confirmed, when he was a vice-president at Kazatomprom, according to a company news release.

In 2009, Kazatomprom's president, Mukhtar Dzhakishev, was charged with expropriation and embezzlement. He was later found guilty.

While Tursunbayev's Facebook page showed him on hikes in the woods near his new **home** and on family trips to Ottawa, Dzhakishev was languishing in prison.

Human Rights Watch has criticized Kazakhstan for not giving Dzhakishev access to legal counsel. Many believe his imprisonment and 14-year sentence are politically motivated, the organization noted in 2011.

Corruption is rife in Kazakhstan, according to a 2011 report by the Organization for Economic Co-operation and Development.

While in **Canada**, Tursunbayev followed affairs back **home**. He posted numerous articles on Kazakh politics on Facebook, as well as Transparency International's 2011 list of the most corrupt countries. **Canada** was ranked the 10th most transparent, Kazakhstan the 120th.

Rustem Tursunbayev Rustem Tursunbayev bought this mansion, seen in a real estate listing, for $3.6 million on Aug. 28, 2009. He sold it to his wife for $2 last year.

Toronto Star Newspapers Limited

Document TOR0000020120220e82k0000f

TORONTO STAR

Business

Toronto's Trump Hotel; An exclusive first look at the tallest residential tower in Canada, built by the country's youngest self-made billionaire

Tony Wong Toronto Star

1712 words
24 March 2011
The Toronto Star
TOR
ONT
B1
English

At the age of 42, Alex Shnaider has built the tallest residential tower in **Canada**.

It is a noteworthy accomplishment. But perhaps it's even more so for a rookie developer who acquired the land in 2002, when he was just 34, and already the country's youngest self-made billionaire.

But Shnaider is a man of action, not words. And self-praise does not come easily. Not even when you have owned your own Formula 1 team and soccer club. Or just happen to be the builder of the landmark Trump International Hotel & Tower in Toronto's financial district.

"Well, I think it is very nice," says Shnaider of his new project.

This gross understatement brings a snort of laughter in the opulent hotel suite that Shnaider and his partner, Val Levitan, president and CEO of Talon International Development Inc., are sitting in.

"Very nice? Alex likes to downplay everything. It is an incredible, huge accomplishment to get this built," says the more animated Levitan. "This is a true trophy building."

Certainly, the suite may not be as nice as Shnaider's 205-foot yacht that he is building, (trading in his smaller 170-foot Benetti that he used to rent for $270,000 a week when he wasn't using it), or his private Global Express jet, or the chauffeur-driven $450,000 Maybach that he comes to the interview in. Or the new **home** on the Bridle Path that he moved into just before Christmas.

But, if you are looking for a hotel in Toronto, it doesn't get much, well, nicer.

Like Shnaider, the typical Trump customer lives large.

The 950-square-ft. one-bedroom suite the partners are sitting in will rent for close to $1,000 a night. The largest suite, at 4,000 sq. ft., will have 11-foot ceilings and will be furnished with pieces by Italian couture **house** Fendi. It will go for $20,000 per night, a record price for a room in **Canada**.

And then there are the condominiums above the hotel.

Asking prices for the suites average $1,650 per sq. ft. Shnaider has yet to move into his 8,000-sq.-ft.penthouse with the 20-ft.-high ceilings, valued at more than $20 million.

The Star got an exclusive interview with Shnaider and a sneak peek at the hotel before it is scheduled to open in late spring.

Last Friday, Shnaider was given an occupancy permit for the hotel, a milestone that has taken almost nine years.

"It is a landmark building. Something that the city can be proud of," says Shnaider, slightly more effusively, later on.

"This is now part of the landscape of the city, a vital part of the skyline, a building that you will see on postcards."

The choice site at Adelaide and Bay Streets is surrounded by the city's bank towers.

The hotel has 261 rooms and suites. It also has a 18,000-sq.-ft. spa built over two floors.

The hotel is still in various stages of construction. The rooms are mostly completed, but the common areas still need significant work.

Surprisingly, there is no hint of the signature Trump brass and gold in sight. Instead, there is black marble, dark woods, and an elegant palette of cream and grey.

While the decor of the newly opened Ritz Carlton is awash in convention-centre beige and burgundy, the sleeker Trump is the style winner.

"People always ask me where is the gold?" says Mickael Damelincourt, the general manager of the Trump Hotel. "But the theme is champagne and caviar. This reflects the influence of the children. In a way, this is more Ivanka than Donald Trump," Damelincourt continues, referring to the daughter of Ivana and Donald, who is an executive vice-president at The Trump Organization.

There will, of course, be fine dining at the hotel. Sources say Todd Clarmo, the former executive chef at Canoe, will head the new restaurant at the Trump. Canoe, the Oliver and Bonacini flagship restaurant and favourite of Bay Street expense-account holders, has lately been raided for staff by the new **luxury** hotels.

Canoe's former general manager, Joanne Chimenti, and the restaurant's former chef, Tom Brodi, have already decamped to Toca at the Ritz.

Meanwhile, superstar American chef David Chang of Momofuku is opening two new restaurants at the new Shangri-La nearby.

Fashion insiders will get a first peek of the new Trump Hotel Thursday, when the grand salon ballroom will make its debut with a much anticipated fashion show by Mark Fast and Mikhael Kale during Toronto Fashion Week.

After a dearth of five-star hotels, Toronto now has a plethora of ultra-**luxury** lodgings. A new Ritz Carlton opened on Wellington Street in the entertainment district in February. The Trump will open in late spring, followed by a new Shangri-La Hotel and a new Four Seasons hotel. Smaller boutique hotels, such as the Thompson Toronto and a new Le Germain, have also opened recently.

Analysts have said that the competition, while good for consumers, means potentially tough times ahead for operators of new hotels. And there are continuing concerns over an oversupply of new condos on the market.

"I think **Canada** is still attractive to a lot of foreign wealth and prices will continue to go up," says Shnaider.

But he acknowledges that the road ahead will not be easy.

Getting this far has already been an accomplishment. The Trump Hotel has been the subject of skepticism from some people in the **real estate** community, who thought it would never get built.

"If someone had told me it would take this long to build, I would never have believed them," says Shnaider.

It has been a bumpy road. When it was launched with much fanfare back in 2000, Shnaider's property was originally supposed to be a Ritz Carlton.

But the Star revealed that the original developer had been convicted of bankruptcy **fraud**, which caused the Ritz to back out and eventually move to a new location near the entertainment district.

Shnaider's Talon eventually took control of the project. Trump is managing the hotel, but this is Shnaider's money on the line, along with minority partner Levitan.

The Trump name has not always been a guarantee of success.

Donald Trump, the American billionaire and star of TV's The Apprentice, has placed his name on everything from golf courses to vodka and mattresses.

In Chicago, the 92-storey Trump International Hotel & Tower still has almost one third of its units unsold after closing on units more than two years ago.

And in Florida, lenders foreclosed on the developer of the Trump Hollywood, where Trump had licensed his name. At the time, only 22 of the tower's 200 condos had been sold. The building has since been bought by new investors.

But, in Toronto's Trump tower, hotel rooms are 85 per cent sold. (The rooms are purchased by investors, who return them to a rental pool.) The residences above the hotel are 60 per cent sold. And Shnaider says he has confidence that the project will sell out once buyers can see the finished product.

"When you are paying that much, you want to be sure of what you're getting," says Shnaider.

One bright spot is that the Canadian economy continues to outperform the G7, and hotel rates and occupancy levels have slowly been inching up from the depths of the recession.

Luckily, Shnaider has deep pockets. Canadian Business magazine ranks him as the 23rd richest man in **Canada**, with a net worth of $2.06 billion, putting him ahead of players such as Michael Lazaridis and Jim Balsillie of Research in Motion Ltd., and Gerry Schwartz and Heather Reisman of Onex Corp. and Indigo Books.

The Russian-born Shnaider immigrated to **Canada** at the age of 13; he attended high school in Toronto, then went on to York University.

Shnaider got his break trading steel when the Soviet Union started to decentralize.

He has since divested himself from the steel business, and branched into **real estate**, retail, transportation and agriculture across Europe and North America.

Closer to **home**, Shnaider continues to invest in the hotel business. He recently purchased the landmark King Edward Hotel, along with a consortium of investors, of which he is the largest shareholder.

Shnaider has also owned a Formula 1 racing team, and a soccer club in Israel, both of which he sold.

His empire has become so vast and he is on the road so often that, until this week, he had not visited the Toronto Trump property in more than a month.

Over the last few months, a colder than normal winter has meant construction has been slower than hoped. But other aspects of the hotel have gone well.

Before Shnaider and his guests leave, Damelincourt's staff provide warm napkins and spritzers presented on a silver platter to guests so they can wash the soot of the day away before they leave the premises.

The nicety gives a hint of the five-star service that has arrived at the Trump Hotel, and harkens of things to come for a city soon to be awash in **luxury** lodgings.

The soaring lobby of the new Trump International Hotel & Tower is still under construction, but it's already possible to imagine how grand it will be once finished. It's set to open in late spring. Alex Shnaider, seen in the living area of a one-bedroom suite, is a man more of action than words. He describes the landmark Trump building in the city's financial district as "very nice." Alex Shnaider, above centre, shows off the bedroom, top left, and bathroom of a one-bedroom unit on the 12th floor. Below, workers put the finishing touches on the Grand Salon on the 9th floor. Meanwhile, building continues on the exterior of the tower at Bay and Adelaide Sts. The finished building is seen in an artist's rendering, right. David Cooper photos/Toronto Star

Toronto Star Newspapers Limited

Document TOR0000020110324e73o0002g

infomart

Canadian Business

Alex Shnaider--The Steel Magnate; Born in St.Petersburg and raised in Israel and Toronto, This entrepreneur has taken risks few members of the Rich 100 could stomach.

Canadian Business
Mon Dec 5 2005
Page: 029
Section: Lifestyle
Byline: Calvin Leung

Alex Shnaider cruises around in a Mercedes-Benz SLR McLaren, lounges on a 170-foot Benetti yacht and lives in a North York, Ont., mansion. But to enjoy those luxuries and amass his estimated $1.7-billion fortune, the entrepreneur, born in St. Petersburg and raised in Israel and Toronto, has taken risks few members of our Rich 100 would likely stomach.

In the early '90s, **Shnaider** worked as a commodities trader, buying steel from eastern European factories--using everything from coal to microwaves as currency--and selling it to other traders. The margins were high, but so were the stakes. At that time, **Shnaider** recalls, any lucrative industry in that part of the world was dangerous. "Competition was literally cutthroat," he says, "and some people would do anything to take business away from you." A savvy entrepreneur, **Shnaider** bought gifts for senior steel executives and, in some cases, hired their relatives. As well, he steered clear of politics. That may explain how he avoided the fate of seven steel execs who were reportedly assassinated in Ukraine in the '90s.

In 1994, he formed Midland Resources and registered the trading and holding company in Guernsey, the Channel Islands. His partner in the company is Eduard Shifrin, a well-connected and experienced trader with a PhD in metallurgical engineering. **Shnaider** considers teaming up with Shifrin as one of his best business decisions so far.

Another of his shrewd moves, **Shnaider** says, was participating in the industrial privatization in eastern Europe. In the late '90s, Midland began buying up shares of Zaporozhstal, a Ukrainian steel mill, and by early this decade owned 93% of it. Midland acquired that stake for roughly US$70 million and has reportedly since turned down offers of US$1.2 billion for the mill.

Today, Midland boasts US$2 billion in annual revenues, more than 50,000 employees spread across 34 countries and a diverse group of holdings, including stakes in Carnex, a meat-processing plant in Serbia; the Electric Networks of Armenia; and the planned 68-storey Trump International Hotel & Tower in Toronto. In January, Midland bought the Jordan Formula One team from Irishman Eddie Jordan for a reported US$50 million. With that foray into the glitzy arena of car racing, **Shnaider** plans to promote, among other things, Midland's auto-parts business.

Shnaider, 37, insists doing business in eastern Europe is much safer these days. Nevertheless, last year the car of the general director of a Midland steel mill in Montenegro was blown up, and authorities have yet to find the culprit. But for **Shnaider**, it seems, the rewards continue to outweigh the risks.

Edition: Final
Length: 420 words
Idnumber: 200512050020

Tone: Negative
Ad Value: $14,920
Circulation: 80,064

THE GLOBE AND MAIL

Former oil executive says he signed controversial deal 'under duress'

JEFF GRAY - LAW REPORTER
TORONTO — The Globe and Mail
Published Thursday, Apr. 04 2013, 6:44 PM EDT
Last updated Friday, Apr. 05 2013, 6:23 AM EDT

The former Russian oil executive battling Toronto billionaire Alex Shnaider testified Thursday that he felt pressured to quickly sign a loan agreement handed to him by a lawyer for Mr. Shnaider at a Moscow police station, after an officer "casually" laid his gun on the table.

Michael Shtaif, a former executive with Russian oil firms TNK-BP and Yukos who now lives in Canada, is locked in a legal fight with Mr. Shnaider, who alleges in a civil lawsuit that Mr. Shtaif and a group of co-defendants tried to defraud him of a $50-million investment in a Russian oil joint venture.

More Related to this Story

- Shnaider keen on Russian oil venture, ex-partner testifies
- Court showdown pits billionaire against ex-partners
- Changes coming fast for Supreme Court

Mr. Shtaif denies those allegations and alleges that the Russian-born Mr. Shnaider tried to push him out of the venture, bribed Russian police and influenced authorities there to pursue "spurious" charges against him.

Mr. Shnaider, whose Midland Group began in the Eastern European steel business but has expanded into real estate and other sectors, denies all of the allegations. None of the allegations have been proven. A civil trial in the case began in February and is expected to continue for weeks.

The account of how Mr. Shtaif ended up in a Moscow police station on the afternoon of July 11, 2006, involves a complicated transaction, being overseen by Mr. Shtaif and aimed at buying a Russian oil field, that went awry.

In a complex series of events relayed in court on Thursday, an advance payment of $12-million (U.S.) in promissory notes was held in safety deposit boxes in a Russian bank pending the closing of the 2006 deal. But allegations then surfaced about whether the vendor had valid title to the shares in the oil field. And an agreement about exchanging the promissory notes underwent "inadvertent" changes, giving the vendor premature access to them at the Moscow bank.

Mr. Shtaif testified that Mr. Shnaider and his partner in Midland, Eduard Shyfrin, "decided to use their police connections" to get the notes back. Mr. Shtaif said he accompanied a lawyer for Mr. Shnaider's company to a Moscow police station to file a complaint about the $12-million. While there, Mr. Shtaif testified, he was also forced "under duress" to sign a loan agreement that restructured his joint venture with Mr. Shnaider, turning the billionaire's $50-million investment into a loan and giving Mr. Shnaider majority control.

Present were Peter Ganus, an in-house lawyer for Midland in Russia, and a "Lieutenant-Colonel Kusakin" of the Russian police, Mr. Shtaif testified. The pair briefly stepped out of the room, he said, and then returned.

"When Mr. Kusakin came back, he casually pulled out a gun and put it on the table," Mr. Shtaif told court. "...He didn't point it at me ... I got the message where it was going. I signed the agreement."

Mr. Shtaif also testified that Mr. Shnaider paid a $525,000 (U.S.) "bribe" to Russian police in order to prompt them to quickly seize some of the promissory notes held in the bank. Mr. Shtaif told the court that Mr. Shnaider demanded that Mr. Shtaif himself cover this payment. A lawyer for Mr. Shnaider previously testified that the money went to "forensic consultants" to prompt police to try to recover the notes, and was not a bribe.

The issue with the promissory notes was not the first issue with the joint venture. The court has heard that the original corporate shell provided by Mr. Shtaif was a "sham" company created by a convicted Toronto fraudster, Irwin Boock, who was allegedly using the alias John Howard. Mr. Shtaif testified that he was not aware of the company's fraudulent origins, or Mr. Howard's alleged alter ego or past. The venture was later transferred to a new company, Koll Resources Ltd.

Court heard this week that a $10-million instalment toward a $70-million investment in the venture, pledged from a company controlled by the man calling himself Mr. Howard, failed to materialize. Mr. Shtaif testified that he did not intentionally mislead Mr. Shnaider about the payment.

More Related to this Story

- Pacific Rim files $315-million claim against El Salvador

Topics:

- John Howard
- United States of America
- Midland Group Inc.
- Yukos
- Toronto, Ontario

Court freezes sale of home once owned by drug smuggler; Custom-built residence 160 km east of Kamloops is valued at $1.75 million

Kim Bolan

Vancouver Sun
656 words
27 January 2011
Postmedia News
CWNS
English

A Shuswap realtor hired to sell the **house** once owned by a convicted drug smuggler who is facing new charges may lose the lucrative $1.75-million listing.

Century 21 agent Kellie Pittman confirmed Wednesday that she has been contacted by a federal government official advising her of a court order preventing the sale of the **luxury** residence in Malakwa, B.C.

Colin Hugh Martin and his common-law wife Jennifer Cahill are both facing charges of production of a controlled substance and trafficking.

They were arrested last July after a massive police raid at their **home** at 3621 Northway Road in Malakwa, which is about 160 kilometres east of Kamloops. Pittman said she was hired to sell the **house** by its current owner, Steve Ambrose, president of the numbered company, 311165 B.C., which is listed on the land title for the custom-built **house**.

"I was working with the seller. I had no contact with Jennifer or her boyfriend or whoever that is. They are the renters. The renters only," Pittman said. But she was unaware until the government contacted her that a court order was issued on Oct. 22, 2010, prohibiting the sale of the six-acre property after an application by the Public Prosecution Service of **Canada** and the RCMP's Integrated Proceeds of **Crime** section.

Cahill, Martin, 311165 B.C. and Ambrose were all supposed to be served with copies of the order. Pittman said the **house** is still listed, until "I do my due diligence first and find out more information."

Cahill, who is out on bail, was once the registered owner of the **home**, but the Land Title office lists Ambrose's company as the owner since 2005.

Martin was denied bail on his new charges in B.C. Supreme Court Thursday.

Martin also was indicted in Washington state in December 2009 on charges he conspired with others to import large amounts of marijuana and ecstasy into the U.S. and to smuggle cocaine back into **Canada** using helicopters.

The U.S. alleges Martin headed the drug gang and leased the helicopters that were used. He was also convicted in 2006 on eight counts including conspiracy to export and traffic marijuana and money laundering related to a massive cross-border smuggling ring operating in the late '90s.

He represented himself at trial after losing legal aid because, as a court ruling noted, "the Crown advised the court that there was an issue regarding the appropriateness of continued funding, as Mr. Martin's spouse was building a **home** valued in excess of $700,000."

Martin lost his appeal last November. He was ordered released on day parole in December, despite the new charges in both countries, because the Parole Board of **Canada** ruled, "there are no reasonable grounds to believe that, if released, you are likely to commit an offence involving violence before the expiration of your sentence.

"The board has concerns about your poor attitude to illicit drug production and sale and your part in the inherent violence has to be taken into account," board member Gordon McRae wrote in the Dec. 23, 2010 ruling.

"The concern is not supported by tying you to direct acts of violence.

"You are apparently facing new charges, but these do not indicate violence was present."

The **house** in which Martin has been living is described in the **real estate** listing as "custom-built to perfection" with over 6,600 sq. ft. "on 6.25 acres at the base of Queest Mountain where the deep powder snow extends the sledding season well into the spring."

"There is a second residence on the property which is under construction," the ad says. "Finish it into a snowmobilers/ skiers/hunting B&B resort."

kbolan@vancouversun.com

Canwest News Service

Document CWNS000020120913e71r010b5

FACTIVA DOW JONES

The Boston Globe

National/Foreign

CANADA GETS REPUTATION AS A HAVEN FOR FUGITIVES

Colin Nickerson, Globe Staff

1270 words
21 December 2000
The Boston Globe
BSTNGB
THIRD
A1
English

MONTREAL - As police closed in on his smuggling empire in China's Fujian province, Lai Changxing made a hasty but plush escape last year, grabbing a first-class seat on the next plane to **Canada**. There, after entering the country as a tourist, the kingpin plunked down $1.3 million for a **luxury home** in British Columbia, and was back in business.

No one knows where James J. "Whitey" Bulger went when he vanished from the view of law enforcement in 1995. But **Canada** is a good bet. The FBI recently issued "Wanted" posters printed in French for distribution in Quebec, where Boston's most notorious gangster is believed to have stashed huge sums of cash.

Canada is rapidly gaining a reputation as a place for criminals and terrorists seeking a permanent hideout under new aliases, as may be the case with Bulger, or as a temporary base of operations, as with the alleged Islamic radicals who were arrested last year in the millennial bomb plot against the United States.

"**Canada** is almost a welcome wagon for crime," said Antonio Nicaso, a Toronto-based expert on organized crime. "Here there is a much lower risk of detention or prosecution than in the United States or Europe."

A report declassified recently by the Canadian Security Intelligence Service, the country's spy agency, indicates that **Canada** is now home to more international terrorist organizations than any other country. More than 50 groups, from Sri Lanka's Tamil Tigers to the agents of Osama bin Laden, the Saudi tied to bombings of US embassies, are said to use **Canada** as a hideout and a staging ground for terrorist attacks.

The report cites a "disturbing trend as terrorists move from support roles, such as fund-raising and [weapons] procurement, to actually planning and preparing terrorist acts" from **Canada**.

This week, a report on international crime, prepared by the CIA, FBI, and other US intelligence and enforcement agencies, warned that **Canada** has become both a refuge for Asian mob figures and a significant North American gateway for Chinese gang members: "The United States faces a growing threat from Chinese organized crime groups using **Canada** as a base from which to conduct criminal activities that impact our country," said the report, which was released by the White House.

Big bucks make for an easier life on the lam. But **Canada** seems a soft touch, even for destitute criminals trying to lie low.

James Anthony Martin, now 52, headed north after allegedly gunning down a Harvard graduate in a drug deal gone bad in Cambridge. The murder occurred in 1976. For nearly a quarter-century, Martin drew welfare and other benefits in Montreal while following a career of armed robbery, petty theft, and transporting narcotics that

resulted in at least 16 arrests. But authorities never seriously checked his past even though neighbors said he had a "troubled" background in the United States.

Proximity makes **Canada** a bolt-hole for US criminals. But the country's indulgent immigration policies are making it a destination of choice for desperate characters from around the planet.

Canada's relatively loose border controls and immigration policies, coupled with a 151,524-mile coastline, are also making it a port of entry for drugs and undocumented immigrants whose destination is the United States.

Analysts say **Canada**'s approach to such immigrants, its generous welfare programs, and its underfunded law enforcement agencies, represent a more or less open invitation to criminals.

When an Algerian accused of terrorist connections was arrested entering Washington state last December, allegedly with a trunkload of bomb materials, it made headlines around the world. The suspect, Ahmed Ressam, had been living in **Canada** since 1994, securing welfare benefits - and notching up a Quebec criminal record - even though he had been caught entering the country illegally with a false French passport.

Lai Changxing wasn't seeking welfare benefits when he arrived in **Canada** in August 1999, describing himself as a simple tourist. China has a another description, calling him the country's "most wanted" **fugitive**. Among other allegations, he was accused of having bribed thousands of officials, high and low, with gifts of cash and women to protect a crime ring that smuggled $6 billion worth of vehicles, crude oil, weapons, and computers into Fujian province.

Lai's fake passport was not spotted when he presented it at Vancouver's international airport. Neither did anyone pay attention when he paid cash for a posh suburban home. Nor when he was banned from casinos in British Columbia for loan sharking. Nor when he partied with Asian crime figures near Niagara Falls, dropping as much as $600,000 a night at gaming tables.

Finally, after 15 months of protests by Chinese officials, Canadian authorities apprehended Lai on Nov. 23, but they have not sent him back. The hope was for a quick extradition, but the case has become a soap opera, with Lai loudly - if improbably - claiming to be a refugee not from justice but "political persecution."

There's little doubt that if Lai is returned home he will face a firing squad. (Fourteen cohorts have already been executed). And that leaves **Canada** in an embarrassing situation. Ottawa likes to boast of its unyielding stand against capital punishment. But officials are also desperate to combat the country's new image as an easy sanctuary for undesirable immigrants, and as a place where even absurd refugee claims can stretch for years and even decades.

"**Canada** doesn't want to be a haven for criminals," said Irene Arseneau, a spokeswoman for the Justice Ministry. "We welcome immigrants, we welcome refugees, but only when they come through the front door."

It's not clear what door James Anthony Martin used to enter **Canada** after allegedly shooting dead 28-year-old Edward Paulsen in Cambridge in 1976. But he seems to have made no attempt to follow the straight and narrow after taking up illegal residence in Montreal: He has been charged with 31 crimes over 24 years, and even served a stint in Canadian prison. But apparently no one thought to check whether the misbehaving American might actually be wanted in the United States.

It took a "cold case" investigation by Cambridge police to bring Martin back to Massachusetts in January on a murder charge.

Meanwhile, there is no proof, but strong suspicion, that one of America's most sought-after criminals, Bulger, slipped into **Canada** in 1995, skipping Boston days before a federal indictment on 18 counts of murder, as well as charges of extortion, drug-running, and racketeering.

Bulger, now 71 and suffering from heart disease, is reported to have links to Montreal's vicious West End Gang, and he is thought to have stashed quantities of unlaundered cash in safe-deposit boxes in Toronto and Montreal. In 1987, for example, Bulger is said to have tried to board a plane for Montreal at Logan Airport with a bag containing about $100,000 in $100 bills. He fled the scene.

There have been at least two "unconfirmed sightings" of Bulger in Quebec and Ontario.

"We know he's traveled extensively in **Canada**, but we are following leads all around the world," said Stuart Sturm, the FBI's legal attache to the US Embassy in Washington.

Sturm stressed that the search for Bulger is being coordinated with the Royal Canadian Mounted Police and other Canadian police agencies. "There's reason to believe he maintained money in **Canada**. So we are hoping to find him with help from our good northern neighbor."

Boston Globe Newspaper

Document bstngb0020010804dwcl00ll8

Search Summary

Text	("luxury home" OR "luxury mansion") AND canada AND fugitive
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	All Languages

Beijing goes hunting for overseas real estate bought with dirty money

By Heather Timmons @HeathaT November 5, 2013

"You can't just steal money from China and then enjoy life in Canada." Reuters/Mark Blinch

Seizing Bo Xilai's French villa may be just the beginning.

China's corrupt officials and crooked businessmen have smuggled billions of dollars overseas, much of which has ended up in real estate in the United States, Canada, Australia and the United Kingdom—particularly in high-end neighborhoods in London, New York, Los Angeles, Sydney and Toronto. Now the Chinese government is embarking on a worldwide hunt to seize the properties with help from foreign governments, according to asset recovery and anti-corruption specialists.

Since Wang Qishan, the Communist Party chief tapped to head China's new anti-corruption drive, took office last fall, he has been pushing to crack down on capital flight from the country. In recent months, Chinese officials have quietly said they are specifically targeting foreign assets, and sought help from organizations like the OECD, anti-corruption groups and the foreign government agencies including the US Commerce Department about their newly aggressive pursuit of overseas real estate.

Chinese officials "are interested in understanding where the assets are" in the US, and "the US has said it will work with them," said Nathaniel B. Edmonds, a former Department of Justice official and a partner with the Washington DC law firm Paul Hastings. In July, Canada and China agreed to seize, share and return the proceeds of crime.

Beijing's interest in hunting down the proceeds of corruption takes place amid a similar push around the globe, with countries like Libya seeking to take back the assets that their corrupt officials have

squirreled away. "There is an increased push to use asset recovery mechanisms in the context of corruption globally," said Faisal Osman, a barrister with the London firm ARM Stolen Asset Recovery.

Following the money

President Xi Jinping's corruption crackdown has resulted in a surge of convictions—in the first quarter of this year alone, China's prosecutors handled nearly 3,700 corruption cases involving $87.5 million. And the campaign has claimed some prominent scalps, many of which involved prominent foreign property holdings. When the Jinan People's Court sentenced former Politburo member Bo Xilai to life in prison in September, it also announced plans to seize a villa owned by his wife on the French Riviera. Separately, a home in Walnut, California, believed to be owned by ex-railway minister Zhang Shuguang, is also a likely target for Beijing's asset hunt.

Those high-profile cases may be just the beginning.

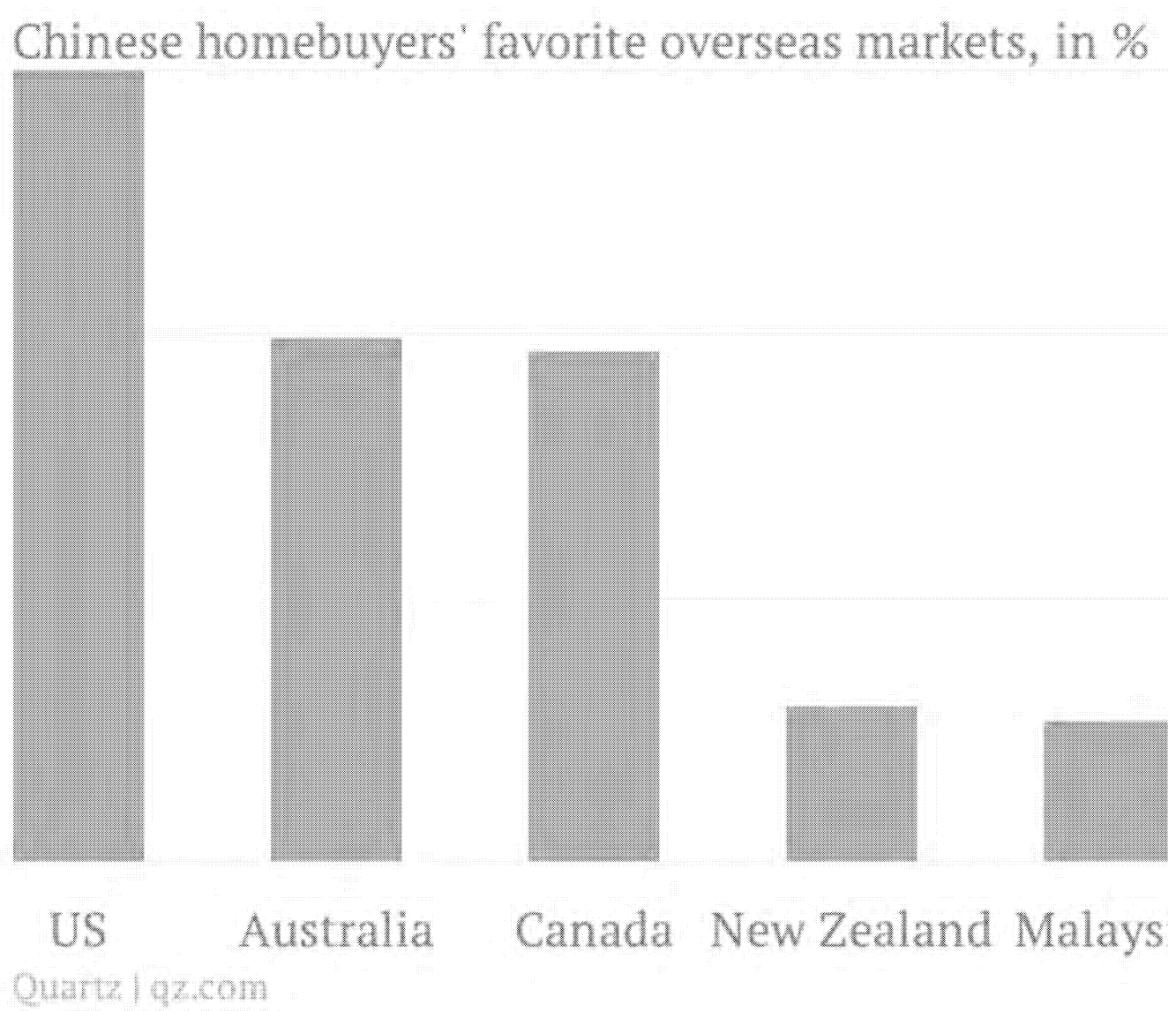
Estimating exactly how much corruption-tinged cash has fled China in recent years is difficult, but Ran Liao, senior program coordinator for Transparency International, a non-profit that works with governments and the private sector to curb corruption, said estimates run as high as 500 billion yuan ($82 billion) taken overseas in recent years. Other mind-boggling estimates abound:

- A leaked report from China's central bank estimated that from the early 1990s to 2008, some 18,000 officials and employees of state-owned enterprises pilfered a total of 800 billion yuan ($123 billion) from state coffers, with the culprits most likely to flee to the US, Canada, Australia and the Netherlands.
- China's anti-corruption unit, the Central Commission for Discipline Inspection, predicted in another leaked report (link in Chinese) that $1 trillion may have fled China in 2012.
- "Grey income"—household revenue above what's declared officially—reached an estimated $1 trillion in 2011, according to the China Society of Economic Reform.

For a corrupt official with money to invest, putting funds directly into an overseas bank or stock market can be risky, because financial institutions are required by global anti-money laundering agreements to report suspicious funds. But real estate agents in most countries have no such requirements. So when Chinese buyers land with suitcases full of cash, as they have in recent months, real estate deals can get done quickly.

Chinese buyers spent $30 billion on overseas real estate in 2012, estimates Juwai.com, a property website. Of that, $9.1 billion went to the United States and much of it specifically to California. And almost 70% of the purchases made by Chinese buyers in the United States were made entirely in cash, according to the most recent report from the National Association of Realtors.

Australian regulators approved $4 billion in real estate purchases by Chinese investors in the 2011/12 fiscal year (pdf, pg. 30), the most recent figures available. Canada keeps no hard data about foreign investors in real estate, but Chinese buyers in one year outnumbered local buyers in Vancouver by a three to one margin. They also bought 27% of new homes sold in London last year.



Hunting "naked officials"

The soon-to-retire Chinese bigwig who has stashed money and relatives abroad in preparation for his escape is such a common character in China that it has its own phrase: luo guan, or "naked official."

Some of them have laid the groundwork for years; one common ploy is to send a son or daughter overseas to a private university as a way to legitimize sending funds out of China. For example, the leaked Chinese central bank report on corruption showed that former ministry of finance official Xu Fangming deposited roughly 1 million yuan ($164,000) into the bank account of a son studying abroad. Perhaps not coincidentally, the number of Chinese students studying abroad has jumped in recent years. In the United States, it more than doubled to 194,000 in the 2011/2012 school year from five years ago.

Another popular strategy for gaining a foothold overseas is securing a foreign passport through "immigrant investor" programs.

The ultimate goal in transferring money out of China, said Transparency International's Liao, is that either the official or his offspring will have a happy life after they leave China. The new crackdown on overseas assets is designed to stop this process.

"The government wants to make them hopeless," Liao said. The message is "You can't just steal money from China and then enjoy life in Canada."

A tough road to recovery

Whether the Beijing's hunt for overseas properties will be a success, and perhaps even impact home prices in Los Angeles or London, remains to be seen.

Seizing and recovering assets in a foreign country can be a tough slog for any government, experts in the field say. While China and most Western nations are signatories to the United Nations Convention Against Corruption, in which countries pledge to help each other recover the stolen funds, the process is lengthy, arduous, and fraught with diplomatic and legal complications.

In the United States, for example, the party hoping to seize a home needs to prove that it was purchased entirely with funds derived through corruption. "In drug-related cases you seize the house and the car," quickly and authoritatively, said Edmonds. But corruption-related cases are often more complicated, because tainted funds are mingled with other, legitimate, funds, he said.

Another glaring vulnerability in any US-Chinese cooperation on asset seizure is the lack of a "Mutual Legal Assistance Treaty" between the two countries, which allows governments to seize foreign assets related to crime, said Daniel F. Roules, a Shanghai-based partner with Squire Sanders. That means Chinese authorities need to rely on cooperation from their US counterparts.

And while US government officials have pledged to help, Laio of Transparency International said that Chinese officials he's spoken with aren't getting as much assistance as they would like. The US State Department and Department of Justice declined to comment.

Jurisdiction shopping in Britain

British courts, on the other hand, see themselves as "world leaders in asset recovery," Osman said, because there are powerful laws on the books, a long line of precedents and relatively straightforward laws.

A 10 million pound ($16 million) home in Hampstead Garden Suburb, a wealthy London neighborhood, purchased by Saadi Gaddafi, son of the deposed Libyan dictator, was seized in 2012 by the Libyan government after British courts ruled that Saadi could not have made enough money to purchase it on his military salary. Often officials hoping to pursue property they believe was purchased by the fruits of corruption will "get a judgment here [in the UK] and get it enforced in another jurisdiction," Osman said.

A UK judgement can sometimes be used successfully in the United States, as it was to seize a mansion in Houston and two Merrill Lynch brokerage accounts belonging to Nigerian governor James Onanefe Ibori.

Whether the Chinese campaign to halt corruption and seize overseas assets will have real impact on property markets in the United States, Australia and Canada has less to do with international laws than it does what happens in Beijing in coming months.

"What it comes down to is political will," said Osman. Given the changing winds of politics, a push towards recovering assets of one person or group can sometimes be halted abruptly. "These by their very nature are lengthy proceedings and sometimes the political will fades," he said. In one case he worked on involving a South Asian country, "the guys' assets we were tracing a few years ago are now the guys in power."

Ivy Chen and Jennifer Chiu contributed reporting.

Canada froze billions in assets to support Arab Spring: RCMP

Jim Bronskill
Ottawa — The Canadian Press
Published Sunday, Jul. 15 2012, 4:59 AM EDT
Last updated Sunday, Jul. 15 2012, 5:18 AM EDT

Canadian authorities red-pencilled almost $4.3 billion in suspect assets belonging to dictators, allegedly corrupt officials and others in response to the Arab Spring uprisings, newly disclosed documents say.

An RCMP briefing note says the national police force's federal policing branch worked with the Foreign Affairs Department, Public Safety, security intelligence agencies and Canadian banks to "identify and freeze" the assets.

More Related to this Story

- Former wartime PM calls for grand coalition after Libyan election
- Sheema Khan What the Brotherhood will mean for women

The note, obtained by The Canadian Press under the Access to Information Act, paints a picture of the extent to which Canadian officials toiled behind the scenes to drain the financial lifeblood of Arab dictatorships.

The agencies relied on an array of sanctions and legislative tools to freeze money and property linked to regimes that toppled in Egypt, Libya and Tunisia, as well as Syria, whose leadership has so far withstood intense pressure from opponents. Some of the probes continue.

However, privacy law and the confidentiality surrounding investigative efforts means only a portion of the $4.3 billion can be discussed and accounted for publicly.

Foreign Affairs says the vast majority of $2.2 billion that Canada seized under the auspices of United Nations Act sanctions has been released to the Libyan National Transitional Council following the demise of Moammar Gadhafi's regime.

An undisclosed amount seized under the Special Economic Measures Act was also released by last September. The act, known as SEMA, allows cabinet to impose sanctions when "a grave breach of international peace and security" has occurred and likely will result in a serious crisis.

Concerning Egypt and Tunisia, authorities zeroed in on residential property valued at $2.55 million and bank accounts containing a total of $122,000 using the Freezing of Assets of Corrupt Foreign Officials Act.

As the name suggests, the act allows Ottawa, upon the request of a foreign state, to temporarily freeze assets that former dictators and their entourage have placed in Canada.

"The investigation to identify assets is ongoing," said Foreign Affairs spokesman Jean-Bruno Villeneuve.

"We're working with both countries to transfer assets back to their citizens, but we require more information from the Tunisians and the Egyptians to be able to do so under Canadian law."

RCMP Cpl. Stephane Gagne of the force's proceeds of crime division confirmed that investigations continue. "In some of those files, the ball is in the other country's court."

The law essentially gives newly installed governments time to get their "ducks in a row" and show Canada that the corrupt officials in question indeed owned the assets, usually paving the way for return of the monies to the new government, said Gagne.

For reasons of privacy and commercial confidentiality, Foreign Affairs could not provide details about these amounts.

Undisclosed assets linked to Syria were also frozen under the Special Economic Measures Act.

In some cases, the money identified by authorities and Canadian banks ends up being unfrozen and freed for use by its owners. For instance, said Gagne, some "honest Canadians" working in Libya had their paycheques temporarily frozen.

Tunisians in Montreal protest Ben Ali family

Community members camp outside hotel

CBC News Posted: Jan 27, 2011 9:20 AM ET Last Updated: Jan 27, 2011 4:23 PM ET

About 60 members of Montreal's Tunisian community held a quiet demonstration outside the Château Vaudreuil Wednesday evening and into the morning because they believe relatives of the ousted president of Tunisia are hiding in the hotel.

Belhassen Trabelsi, brother-in-law of Zine el Abidine Ben Ali, and his family are believed to have flown into Montreal on a private jet a week ago, and apparently booked into the sprawling hotel complex just off the west end of the Island of Montreal.

> **'Canada will use all the tools at its disposal to co-operate with the international community in dealing with members of the former regime. They are not welcome — I'll be very clear — we do not welcome them in out country.'**
>
> *—Prime Minister Stephen Harper, speaking in Morocco*

This has outraged Tunisians in the city because the billionaire businessman has been accused of stealing large amounts of money from Tunisia.

They want his Canadian assets frozen by the government, and his extradition to Tunisia.

Immigration Minister Jason Kenney has confirmed that some members of the ousted Tunisian president's family are in Canada, and that they already have permanent resident status. He would not give their names, he said, because of privacy laws.

Speaking in Morocco, Prime Minister Stephen Harper said there will be no welcome mat in Canada for Ben Ali or his family.

"Canada will use all the tools at its disposal to co-operate with the international community in dealing with members of the former regime," he said in Rabat following a meeting with Morocco's prime minister and foreign minister.

"They are not welcome — I'll be very clear — we do not welcome them in out country," Harper said.

He said Canada welcomes the political change happening in Tunisia.

Tunisia's transitional government has issued an arrest warrant for Ben Ali, who was driven out of the country last week, accusing him of taking money out of the North African country illegally. It also asked Interpol to help track down Ben Ali and his family.

Ben Ali is also charged with illegally acquiring real estate and other assets abroad.

Tunisia also wants Ben Ali's wife, Leila Trabelsi, arrested. French media have reported she left Tunisia with millions in gold bullion.

Arrest warrants were also issued for other family members, and Tunisian news sources say Trabelsi is included in the warrant.

'A lot of angry Tunisians'

But Public Safety Minister Vic Toews isn't saying if Canada will act on that warrant:

"They are not welcome in Canada, but beyond that I can't say anything because there are potential proceedings that would affect them," Toews said.

Montrealer Haroun Bouazzi said Wednesday that Tunisians in the city are thrilled to hear that Interpol is after Trabelsi.

Bouazzi speaks for a group of Tunisian expatriates fighting for justice in their homeland — the Collectif de solidarité au Canada avec les luttes sociales en Tunisie.

"Now I know that there are a lot of angry Tunisians. The first thing we knew, that these people were in a hotel somewhere in the West Island, I know that some Tunisians went in every hotel looking for these people," Bouazzi said.

A diplomatic cable made public by WikiLeaks from the former U.S. ambassador to Tunisia, Gordon Gray, makes it clear why he's not liked.

The cable describes the Trabelsi family in Mafia-like terms.

The family provokes the greatest ire from Tunisians, the cable says.

Belhassen Trabelsi, the ambassador went on to say, is the most notorious family member, and is rumoured to be involved in a wide range of corrupt schemes.

canada.com

Ottawa asked to speed up seizure of ex-dictator's assets

After a year of delays, Tunisian-Canadians are urging the government to act now to seize assets embezzled by the family of deposed Tunisian dictator Zine El Abidine Ben Ali and hidden in Canada.

BY NATIONAL POST MARCH 15, 2012

After a year of delays, Tunisian-Canadians are urging the government to act now to seize assets embezzled by the family of deposed Tunisian dictator Zine El Abidine Ben Ali and hidden in Canada.

"We don't understand why Canada is not acting faster and in a more rigorous way," said Sonia Djelidi, spokeswoman for the Tunisian Collective of Canada. "The Tunisian people need the money."

Foreign Affairs Minister John Baird released additional information on the seizure of the family's funds - stolen from Tunisia's public coffers during decades of corrupt rule - in a response to a question by NDP foreign affairs critic Helene Laverdiere Wednesday.

Mr. Baird said the snare is closing around family members of the deposed Tunisian dictator, whose assets are forfeit under the Freezing Assets of Corrupt Foreign Officials Act, passed in March 2011. Once recovered, the law says, the money would be returned to the Tunisian government.

The government has publicly listed the names of 123 members of the Ben Ali clan on a website as "politically exposed foreign persons," a list that reads like a veritable family tree.

All those listed are subject to an asset freeze, which prohibits anyone in Canada from making any business or financial transaction with them. "[I] can confirm that any real, personal, movable or immovable property owned by members of the Ben Ali family and located in Canada is subject to being frozen," Mr. Baird wrote.

He said the full list of the Ben Ali family's assets cannot be released, because of the ongoing investigation searching for assets stashed in Canada over the years. "However, [the government] can confirm that over $2.5-million in assets have been frozen, including a residential property valued at $2.55-million and bank accounts in the amount of $122,000."

The ouster of former president Ben Ali in January 2011 marked the beginning of the Arab Spring revolutions.

More than a year later, Ms. Djelidi said, other countries have returned money stolen by the Ben Ali family to the cash-poor Tunisian government. But here in Canada, she said, Ben Ali's brother-in-law Belhassen Trabelsi continues to live off the family's illgotten gains.

Libya claims stake in Saadi Gaddafi's $1.6M Toronto condo

STEWART BELL | October 31, 2012 12:13 AM ET
More from Stewart Bell | @StewartBellNP

The condo building at 10 Navy Wharf Cr. that houses the condo owned by Saadi Gaddafi. Tyler Anderson/National Post

Libya claims stake in Saadi Gaddafi's $1.6M Toronto condo

TORONTO — The Libyan government has formally claimed a stake in a $1.6-million Toronto penthouse owned by late dictator Colonel Muammar Gaddafi's son, who bought it in 2008 but seldom ever used it.

Lawyers representing the Libyan embassy in Ottawa filed an application with the Ontario government land registry office on Oct. 10 asserting an interest in Saadi Gaddafi's luxury condo near the Toronto waterfront.

The notice said the government of Libya was claiming a right to the property under United

Nations Security Council resolutions that froze the worldwide assets of the Gaddafi family.

Related

Lien placed on Saadi Gaddafi's luxury Toronto condo for unpaid fees

Ottawa puts freeze on Saadi Gaddafi's $1.6M Toronto condo

Hand Saadi Gaddafi's Toronto penthouse over to Tripoli: Libyan envoy

The Libyan chargé d'affairs, Sulaiman A. Mohamed, could not be reached for comment Tuesday. The law firm representing the embassy on the case, Borden Ladner Gervais LLP, declined to comment.

But Rick Roth, press secretary to Foreign Affairs Minister John Baird, said Canada had been working with Libya to ensure that "corrupt foreign leaders are held accountable for their actions" according to the law.

"It is for the Libyan government to determine, in consultation with its legal counsel, whether to take steps to claim a right to the property under Ontario law," he said. "We are in contact with the government of Libya and will continue to work constructively with them on these matters."

Saadi Gaddafi, the third son of Muammar Gaddafi, in 2005. Tim Wimborne / Reuters files

Since toppling the Libyan dictatorship last year with the help of NATO, the new regime in Tripoli has been trying to recover the Gaddafi family's assets, arguing they rightly belong to the Libyan people.

The Gaddafis spent billions on luxury properties, cars, jets and investments during the four-decade Libyan dictatorship. Mr. Gaddafi, 39, bought the penthouse four years ago while visiting Canada to study English and meet executives of SNC-Lavalin, the Montreal-based firm that has won several major construction contracts in Libya.

Following the start of the 2011 Libyan revolt, the UN Security Council froze the assets of Gaddafi family members. Saadi Gaddafi was included in the sanctions due to his "command of military units involved in the suppression of demonstrations."

Saadi Gaddafi has called for an uprising against the democratically elected Libyan government and has threatened to return to Libya to carry on his father's brutal legacy

But the Toronto condo apparently went unnoticed by the Canadian government until the National Post reported on it last December. A week after the story was published, the Department of Justice froze the property and Libya's top diplomat in Canada said he wanted it handed over to his government. But Libya only took formal action three weeks ago.

Michael Lamb, who teaches real estate law at the University of Western Ontario, said the move means Mr. Gaddafi cannot sell the 40th-floor suite at 10 Navy Wharf until the Libyan government's claim has been dealt with by the courts. "He'd have to apply to the court to have it removed," Mr. Lamb said.

Mr. Gaddafi visited Montreal and Toronto several times, most recently in 2009. As rebel forces were advancing in Tripoli, private contractors allegedly made plans to fly him to exile in Venezuela, the Bahamas, Mexico or Canada.

But he instead fled by land to neighbouring Niger, where he has lived in exile for more than a year. While he cannot leave due to the UN sanctions, which include a travel ban, two weeks ago the U.S. Treasury accused a South African woman, Dalene Sanders, of approaching officials in Uganda about giving him asylum.

"Saadi Gaddafi has called for an uprising against the democratically elected Libyan government and has threatened to return to Libya to carry on his father's brutal legacy," the Treasury said in a statement.

"Additionally, he has claimed to be in contact with a number of people who are willing to help him with his revolt. Saadi Gaddafi's ongoing activities and the potential misuse of resources at his disposal pose a direct threat to Libya's democratic transition."

A former professional soccer player, Mr. Gaddafi was known for his lavish lifestyle. In addition to the Toronto condo, he owned a $16-million London mansion with eight bedrooms, an indoor swimming pool and big-screen TVs in every room. In March the British courts ordered him to hand it over to the Libyan government.

Meanwhile, Libya is selling the $7-million Ottawa mansion that had served as the ambassador's official residence during Col. Gaddafi's reign. It sprawls over 10,000 feet and includes a dog shower, the Ottawa Citizen reported.

National Post

FACTIVA DOW JONES

Brokers gone bad

Andy Holloway

Financial Post
891 words
20 April 2010
Canwest News Service
CWNS
English

A look at some of the reasons American state regulators have denied mortgage broker licences to applicants makes for interesting reading: Theft, forgery, drugs, securities **fraud**. A certain Douglas Dodd, aka too many aliases to list here, was denied by Washington for a laundry list of items including theft, assault, guns and multiple drug convictions.

Such information is rarely made public in **Canada**, but criminal-record checks - and they are done here - only catch people who've been bad in the past. There's plenty of opportunity for licensed brokers to turn bad in the future. After all, they're in possession of very personal information about their clients. They have to be. Whether it's a bank or a broker, consumers must provide income statements and allow credit checks - information that can be used for fraudulent purposes in the wrong hands.

Fortunately, most brokers are fine and upstanding businesspeople. The Canadian Association of Accredited Mortgage Professionals (CAAMP), a professional development association, in 2009 received 85 ethics complaints, which isn't bad considering it has more than 12,000 members. But more people tend to complain to the provincial regulatory bodies. For example, the Financial Services Commission of Ontario (FSCO), the agency that licenses mortgage brokers in the province, in 2009 reviewed 161 complaints, resulting in 91 licence suspensions and $98,050 in fines.

Most of the complaints and charges - just as in other provinces - seem mundane. For example, the Ontario regulator made headlines in early 2009 after it sought to fine and revoke the licences of 79 brokerages for failing to have errors and omissions insurance. It sounds ominous, but the sweep really was just a result of implementing the then-year-old Mortgage Brokerages, Lenders and Administrators Act. Under the old system, brokerages were not required to have such insurance, which gives consumers some recourse when brokers make a mistake - a bit like malpractice insurance for doctors. Apparently, quite a few brokers missed the memo that it was now mandatory.

More interestingly, one submortgage broker in B.C. repeatedly processed applications that supplied federal Notice of Assessments as proof of income. The problem? An old name for the **Canada** Revenue Agency was on the letterhead, making the document a case for **fraud**, not a mortgage. That broker's licence was suspended by the province's Financial Institutions Commission (FICOM) later that year.

Advising or helping clients to tell a lie - even a white lie - on any application is one sure sign of a bad broker. That's because people who advise others to lie are likely to lie themselves. Another bad sign is when brokers pressure clients into accepting a mortgage - an indication they would rather be paid quickly than find the right product. Consumers should never accept a deal that they can't understand or feel they can afford. In Ontario, brokers must provide consumers a 72-hour cooling off period before signing a mortgage agreement.

CAAMP members must abide by a code of ethics and all brokers should have a privacy agreement that prevents them from sharing client information without permission.

One big red flag to look for, says Jim Murphy, CEO and president of CAAMP, is when a broker asks for an upfront fee. In certain **private mortgage** deals, there may be some additional legwork that requires a consumer to pay such a fee, but "by and large mortgage brokers do not do that for conventional mortgages. They're paid by the lender." In Ontario, for example, a broker cannot ask for a deposit on a mortgage worth less than $300,000 until a deal is done.

Other signs of trouble are a little less obvious, says Murphy, but can be revealed by checking with the provincial regulator to make sure the broker is licensed and asking the broker questions such as: Does the broker have an office? Who are the lenders they deal with? Why are you recommending this particular mortgage? "People getting a mortgage should be asking lots of questions," says Murphy.

Consumers should also be wary about submitting detailed online mortgage applications. The British Columbia Financial Institutions Commission in 2008 issued a consumer alert after coming across such scams. It advises potential borrowers to never provide their social insurance number online and only provide sensitive financial information when they have verified the legitimacy of the mortgage lender.

But mortgage brokers can be victims, too. An alert published by the Independent Mortgage Brokers Association of Ontario warns brokerage owners to watch out for agents who join only to get access to credit reports via a brokers' electronic delivery system. The kind of information found on credit reports can be used to apply for credit cards. The association advises brokers to not allow anyone access to the mortgage application delivery system until they are properly registered with the provincial regulator.

There are steps consumers can take if they suspect a broker hasn't acted in their best interests or something more nefarious such as outright theft or a privacy breach. They can lodge a compliant with CAAMP if the broker is a member. CAAMP has an ethics committee and it can revoke membership.

But consumers should really be complaining to the provincial regulator. "They're the ones who can pull licences, suspend licences or undertake fines," says Murphy.

Canwest News Service

Document CWNS000020100420e64k00711

Search Summary

Text	"private mortgage*" AND fraud AND canada
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	English

FACTIVA DOW JONES

THE VANCOUVER SUN

BusinessBC

Mortgage fraud hits $1.5b a year: Easy to do, often lucrative, real estate agents say it is growing quickly across Canada

Mario Toneguzzi

Calgary Herald
1005 words
20 March 2006
Vancouver Sun
VNCS
Final
E4
English

CALGARY

CALGARY -- Mortgage **fraud** has become a billion-dollar industry in **Canada** and a growing concern to the real estate and financial sectors.

Although difficult to put an exact number on, organizations such as the Quebec Association of Real Estate Agents and Brokers suggest the criminal activity amounts to an estimated $1.5 billion a year across the country.

"We believe that only criminal prosecution of mortgage **fraud** will deter unscrupulous operators in the marketplace," said Bev Andre, chairwoman of the Real Estate Council of Alberta, "and that only through prosecution can those who commit **fraud** be made to bear its costs."

Ron Esch, executive vice-president of the Calgary Real Estate Board, calls mortgage **fraud** a "huge problem because it does involve a lot of money -- ill-gotten gains."

"It's relatively easy to commit mortgage **fraud**," said Esch. "Obviously you're doing a criminal act but it's a criminal act not that difficult to do."

In B.C., independent mortgage lender Gordon Altman gave an elderly White Rock man a $250,000 mortgage against a $500,000 house he said he planned to sell.

The man and his identification had already been verified by a lawyer who provided legal advice, and by a mortgage broker known to Altman.

It wasn't until Altman checked with the White Rock realtor who was handling the listing that he discovered the man didn't own the house and had fooled them all in a brazen scam.

When Altman told the realtor he held a mortgage against the property, she said that would have been impossible.

"She said 'There is no mortgage, and couldn't be because the owner is dead,' " Altman said in an interview.

Mortgage **fraud** occurs in two ways.

- The first involves individuals fabricating their qualifications for a mortgage when buying a house.

- The second involves **fraud** for profit -- a growing concern -- where someone intentionally defrauds a lender or a homeowner of their interest in a property.

The latter is often accomplished by identity theft. Ownership of a property is transferred fraudulently from the rightful owner to the criminal who then sells or mortgages that interest and makes off with the funds.

The problem is becoming more prevalent as technology makes it easier to falsify documents and create identities, say experts in the field.

"It's huge," says Det. Robbie Robertson of the commercial crime unit with the Calgary Police Service. "I've been aware of it for over three years . . . There's a huge, huge effect of this."

For example, following a six-month investigation last fall, the police commercial crime unit in conjunction with Alberta Government Services charged Lloyd Lewis Mason, 33, of Calgary, with one count of **fraud** and one count of **fraud** in relation to making a false registration of title.

The case involved the unlawful transfer of a title to a property to another person without the knowledge of the true owner. That person then took out an almost $110,000 mortgage on the property.

The **fraud** came to light when the true owner attempted to pay property taxes and the City of Calgary notified them that they no longer owned the property.

This was a case of identity theft where the object of the stolen identity was to fraudulently obtain mortgage money.

According to Alberta Justice, the accused was recently convicted and sentenced to four years in prison and ordered to make restitution of $109,905.

Wayne Proctor, regional director, Pacific region for First Canadian Title (a title insurer), said the magnitude of the problem is a rough guess because most of the **fraud** victims are mortgage lenders and in a lot of cases they may suffer a loss and may not know it's mortgage **fraud** or not specifically identify it as mortgage **fraud**.

"The rough estimate of the problem that the Canadian Institute of Mortgage Brokers and Lenders made a few years ago was $300 million," said Proctor. "But there's more recent estimates that would indicate it's probably closer to a billion dollars.

"In our discussions with regulators, with mortgage brokers and realtors and others connected to the real estate industry, it is pretty well a consensus that it is a growing problem. One of the reasons could be the awareness of potential fraudsters that this is a relatively easy **fraud** to commit. The payoff is very large as compared to other types of minor crime."

Esch said there needs to be more resources committed to the problem here and more "serious jail time" for those convicted of mortgage **fraud**.

"The problem won't go away until there are more checks and balances put in place," Esch said.

- - -

Real estate **fraud** developments

- First Canadian Title estimates the average case of real estate **fraud** to be in the range of $300,000 while in comparison the RCMP estimates the average credit-card **fraud** case in **Canada** to average about $1,200.

- In 2000, real estate-title **fraud** claims accounted for only six per cent of total dollars paid in claims at First Canadian Title.

By 2005, that number reached 33 per cent.

- Law-enforcement officials and lenders believe that 10 to 15 per cent of all mortgage applications contain false information.

- According to the Quebec Association of Real Estate Agents and Brokers, mortgage **fraud** amounts to an estimated $1.5 billion a year in **Canada**.

- The Real Estate Council of Alberta estimates there were about $275 million in fraudulent mortgage loans in Alberta in the 2001-2002 fiscal year based on transactions investigated.

Source: First Canadian Title and Real Estate Council of Alberta

Ran with fact box "Real estate fraud developments", which has been appended to the end of the story.

Colour Photo: Steve Bosch, Vancouver Sun Files / Gordon Altman, a private mortgage lender, was victimized by a fraud artist who illegally got title to a property.

Vancouver Sun

Document VNCS000020060320e23k00039

Search Summary

Text	"private mortgage*" AND fraud AND canada
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	English

TORONTO STAR

Greater Toronto

Lawyer faces fraud charges; RCMP also lay charges of money laundering after raids on Etobicoke home, Concord law office

Jennifer Yang Toronto Star

472 words
9 June 2012
The Toronto Star
TOR
ONT
GT1
English

A two-year international drug investigation has led to the arrests of a 71-year-old lawyer and his employee, who now face charges of **money laundering** and possessing the proceeds of crime.

Lawyer Kenneth James of Etobicoke - who is also charged with fraud - has an extensive history of troubles, including a 2006 bankruptcy filing, past allegations of fraud and ongoing professional misconduct hearings.

But his co-accused, 61-year-old Rosemary Cremer, is known to her neighbours in Etobicoke as a sociable, "lovely" lady who seems to keep a low profile.

"I've known her for maybe 10 to 12 years," said Pauline Firkin, who lives next door. "This is a complete shock."

On Thursday, the RCMP executed a search warrant at Cremer's modest bungalow on Willowridge Rd. Police also raided the Concord location of James's law office, James and Associates, on Steeles Ave.

James and Associates, which also has an office in Brampton, was first searched in December, said RCMP Det. Insp. Derek Matchett, with Toronto's Integrated Proceeds of Crime Unit.

Matchett said the criminal charges stem from a drug investigation launched by the RCMP in May 2010. That investigation - which has resulted in arrests and the freezing of more than $7 million in assets - is covered by a court-ordered publication ban so he cannot divulge any details, he said.

Bail proceedings against Cremer and James are also subject to a publication ban, Matchett said Friday afternoon.

But speaking prior to the ban, he said the RCMP alleges proceeds of crime were laundered through companies believed to be under James's control, including James and Associates, Eveline Holdings Inc. and Sterling Capital Inc.

"What we're talking about is drug traffickers who make millions of dollars and then need to place that money into financial institutions - or to 'clean' it, for lack of a better word," Matchett said.

In a massive 2011 **mortgage fraud** case involving more than $5 million, a Superior Court judge noted that fraudulently obtained funds were moved through several accounts, including one belonging to James and Associates.

James has also been embroiled in several civil cases, including a 1990 lawsuit where he and several other defendants were accused of fraud and conspiracy by trustees of the Church of Jesus Christ of Latter-Day Saints.

The action was eventually discontinued by the church and then dismissed by a judge.

In 2006, James filed for bankruptcy and declared that he had $4,505,000 in liabilities and $1,418,500 in assets.

The Law Society of Upper Canada has accused him of professional misconduct involving mortgage transactions. The case is ongoing.

With files from Kate Allen and Tara Walton

Toronto Star Newspapers Limited

Document TOR0000020120609e86900047

TORONTO STAR

News

Mortgage scam probed in Toronto house flips; Seven homes in the Junction were taken on a wild real estate ride that ended in a lawyer's suspension

Tony Van Alphen Toronto Star

2004 words
7 January 2012
The Toronto Star
TOR
ONT
A1
English

Something strange was going on in the Junction.

At least seven modest homes, all on avenues in the working-class west end of Toronto, experienced a pattern of flips and price jumps as much as 60 per cent in less than a day.

Most of the deals didn't include deposits. Purchasers got money back. Mortgages exceeded the value of homes. The same buyers and private lenders popped up in many sales.

In one sale, a buyer effectively sold a home to herself.

A few sales even involved a notorious real estate agent who ended up in prison last year for helping mastermind marijuana grow operations in scores of other houses across Toronto.

And behind all the 2003-2005 deals that often defied common sense is a freewheeling lawyer - Ron Allan Hatcher - representing multiple parties and running roughshod over his profession's rules of conduct.

A real estate expert, Jerry Udell, reviewed the complex and convoluted deals for the Law Society of Upper Canada in a subsequent disciplinary case. He concluded that all of them pointed to one thing - **mortgage fraud**.

A lot of it.

Mortgage fraud remains a serious problem in the real estate industry. In the U.S., it undermined the housing market during the bubble years of 2004-2005 and brought it crashing down.

But proving fraud in the U.S. and Canada can be time-consuming and elusive.

Finding victims is sometimes even harder. In the case of the seven Junction houses, police never laid charges or opened a criminal investigation.

The Ontario Real Estate Council, which regulates the industry, confirmed in November that it had opened an investigation into the transactions involving the houses and possibly more properties.

Except for a one-year suspension for professional misconduct against lawyer Ron Allan Hatcher by a law society panel recently, no one has experienced repercussions from the flips and other financial gymnastics involving those houses.

In response to requests from the Star for an interview, Hatcher noted in a brief email that the law society found "there was no fraud" and he suggested waiting for the panel's reasons and "all of the relevant facts."

The law society's panel ruled in October 2011 Hatcher engaged in professional misconduct for "participating in or knowingly assisting in dishonest or fraudulent conduct" by clients obtaining mortgage funds under "false pretenses."

It also found Hatcher, who became a lawyer in 1994, wasn't honest or candid with clients, didn't disclose conflicts of interest to them, or meet the standard of a "competent lawyer."

Former clients have also won at least two default judgments totalling more than $230,000 against him in civil courts for deficient work on house loans.

Mortgage fraud usually involves people falsifying information such as property values on loan applications so they can gain larger amounts of funds.

In many cases, they default on payments and mortgage funds disappear.

A normal real estate transaction involves a seller receiving money for a home.

But in the case of these seven houses, buyers received unexplained or unaccounted funds as well.

Flips at much higher prices would follow, with a combination of mortgages from financial institutions and private lenders.

In some instances, there were two flips on the houses.

In the final flip, the purchaser would gain as much institutional financing as possible based on the much higher prices negotiated between familiar players in each case.

While the law society panel focused on Hatcher's conduct in its deliberations, a stinging review of Hatcher's work by real estate lawyer Udell cited more than 20 "red flags" of "potential fraud" in the transactions.

One of the more curious series of transactions involved 148 Edwin Ave,. where Ivor Pinkett and his sister-in-law Helen Pinkett closed a deal to buy a house for $270,000 on Nov. 17, 2003. Their names would appear repeatedly in The Junction juggling.

The Pinketts' real estate agent for the purchase was high-flying Sau San (Jennifer) Wu, who would plead guilty to marijuana cultivation, tax evasion, utilities fraud, **money laundering** and violating bail conditions in May of this year.

Wu admitted acting as an agent in renting 54 houses to marijuana farmers and received a 61/2-year prison term. None of the grow operations involved the seven houses, according to police.

Hatcher represented both the buying Pinketts on the Edwin Ave. sale and private lenders, who provided a $279,000 mortgage - more than the actual purchase price.

A numbered company for the Pinketts then flipped the Edwin Ave. house for $310,000, or 15 per cent more. Oddly, the deal closed Nov. 14, three days before the first transaction.

The expert review by Udell, a Windsor lawyer with 35 years experience, said the price "was significantly inflated."

Furthermore, one of the buyers was Helen Pickett, who effectively bought the house from herself. There was to be a downpayment of $5,000, but the review couldn't find any record of it.

"The second agreement makes no sense and is an obvious sham," said Sean Dewart, a lawyer for the law society, in a brief at Hatcher's disciplinary hearing.

Hatcher ran into further conflicts in the latter transaction by acting for the Pinketts' numbered company (now the seller), and lender Bridgewater Financial Services, which provided a first mortgage of $284,580.

He also arranged for two more mortgages on the property totalling almost $100,000, which easily exceeded the purchase price again.

Udell's review for the law society said although Hatcher complied with a rule limiting mortgage amounts while representing borrower and lender, he should have declined the work in "such a clearly manipulated mortgage transaction."

The review also said Hatcher may have "misled" Bridgewater by telling the financial firm he held $37,100 in a trust account for Helen Pickett's downpayment.

In fact, the property was bought with no equity.

In July 2004, Helen Pinkett defaulted and the property was sold under a power of sale process to another investor who was involved in a transaction on one of the other seven houses. Bridgewater collected $265,000, almost $20,000 less than its original mortgage investment.

Udell's review said Hatcher's multiple positions in the transactions were "extremely unusual."

It should have put Hatcher "on alert for a potential fraud" in connection with no deposits, price increases and mortgages exceeding 100 per cent.

He also failed to inform lender clients about the oddities, the review noted.

Ivor Pinkett, a house painter by trade, acknowledged buying and selling some of the houses, but stressed he didn't make any money and never suspected improprieties. Nor was he aware of the law society's case against Hatcher.

The Pinkett's also worked on renovating the homes to boost their value in a resale.

"There were flips all over the map," he recalled. "On some of the houses I worked on, we just walked away and never made anything."

He described Hatcher as a "nice guy and straight up," but added he was unaware about the suspension and hadn't talked to him in years. Helen Pinkett described him as "one of the nicest men I've ever met."

Meanwhile, the Edwin Ave. property continued to sell in transactions that involved some of the same players in previous Hatcher deals.

In 2006, the house sold for $450,000 under another power of sale, with the buyer receiving most of the financing from Money Connect Home Lending.

The listing described the home as "completely renovated."

The owner defaulted in 2009 and Money Connect conducted yet another power of sale.

This time, the house sold for $360,000, leaving Money Connect with a loss. The listing indicated "renovations started."

Transactions at a house on 176 St. Clarens Ave. again featured Hatcher representing the Pinketts as buyers.

There was a second flip with a 64-per-cent price increase in 14 months - from $329,000 to $540,000 - with no deposits and private lenders providing more than 100 per cent financing.

In that flip, which the society review described as "suspicious," Hatcher took on a new role - buyer.

Hatcher, his wife and mother bought the house when the owner who purchased from the Pinketts defaulted.

The price had also soared despite a gutting of the house, which made it uninhabitable.

The review also found that "substantial" funds were paid to renovate the property before closing the deal to the Hatcher family and the work was ultimately paid for by sale proceeds.

Udell said he had never seen such a practice in more than three decades of work.

Fellow lawyer Dewart had a blunt assessment of the St. Clarens transactions: "It was a sham and a fraud," he told the society.

He also charged in a brief to the law society that Hatcher had participated in transactions which he knew were frauds.

While admitting the failure to notify lender clients about jumps in property prices was "unprofessional and negligent," Hatcher insisted those actions didn't support allegations of complicity in fraud.

It remains a mystery whether Hatcher gained anything financially.

In his filings with the law society, Hatcher said there was no evidence he received excessive fees or payments on any of the seven properties.

TD Canada Trust, the Bank of Nova Scotia and Bridgewater Financial Services - which provided some of the mortgages for the properties - would not comment on whether they lost money.

Money Connect Home Lending, did not respond to inquiries.

Mortgage fraud can also have an impact on the local real estate market.

For example, quick house flips and a jump in prices can artificially raise the value of neighbouring properties.

In this case, it is unclear whether the big price increases or a general uptick in the market pushed up values on the same streets or nearby.

So where are the victims?

One veteran real estate lawyer who looked at the seven deals said it is possible that there were no victims because significant increases in market value swept away any possible losses.

"It appears the deals were designed to artificially inflate property values to get higher mortgage amounts than should be permitted," said the lawyer, who requested anonymity.

"But in these cases, everyone just got lucky and no one got hurt because market values eventually increased so much in Toronto. In the case of the banks, perhaps they just didn't do their due diligence and looked the other way. If property values had remained stagnant, it may have become a police matter."

In its arguments, law society staff told Hatcher's hearing that financial damage is not necessary to prove fraud under the law.

Some real estate officials say there is an industry impression that police only pursue major incidents of possible **mortgage fraud**.

However, Det. Sgt. Cam Field, who heads the Toronto Police Service financial crimes section, counters that his department will devote the staff and time if there is evidence of **mortgage fraud**.

"We know, based on the information from the law society, the potential of more victims in this alleged scheme," Fields noted. "If people think they were criminally defrauded, we strongly suggest they contact us."

In addition to the suspension and an order for $30,000 in costs, the law society rapped Hatcher with a reprimand and $2,000 in further expenses for failing to co-operate in the investigation of his conduct.

But society staff said the penalties aren't enough. They have appealed to a higher society panel to disbar Hatcher.

A law society panel recently gave lawyer Ron Allan Hatcher a one-year suspension for professional misconduct for his role in the Junction deals. Lawyer Ron Allan Hatcher was at the centre of a complex assortment of real estate deals that led to his suspension. Dale Brazao/TORONTO StAR Dale Brazao/Toronto Star

Toronto Star Newspapers Limited

Document TOR0000020120107e8170002o

News

Global fraudster faces new charges

Salim Damji pleaded guilty five years ago to defrauding up to 6,000 investors around the globe of some $78 million by conning them into believing he owned the rights to a tooth-whitening spray that would make them millionaires.

By: Betsy Powell Crime Reporter, Published on Wed Apr 11 2007

Salim Damji pleaded guilty five years ago to defrauding up to 6,000 investors around the globe of some $78 million by conning them into believing he owned the rights to a tooth-whitening spray that would make them millionaires.

For a crime that's considered one of the largest single frauds in Canadian history, Damji was sentenced to six years and three months in prison – a term slammed by some investors as too lenient.

Yesterday, the same Toronto investigator who arrested him in 2002 charged him again. But this time it was for allegedly committing a crime on a much smaller scale: cheque fraud.

Det. Jeff Thomson of the fraud squad charged Damji, now 37, with one count of fraud over $5,000, uttering a forged document and conspiracy to commit an indictable offence for allegedly arranging deposit of a stolen cheque made out for $8,000 into someone's bank account.

"A tiger doesn't change his stripes," Thomson said yesterday after charging Damji at the Toronto (Don) Jail.

Thomson believes if he's stooping to cheque fraud, it's likely he doesn't have the stash of cash that many suspected. "Gambling has been a problem for him in the past and appears it could be at the root of the problem now," he said.

One of the conditions of his release is that he participates in "treatment/programming to address gambling addiction," according to National Parole Board documents.

While he pleaded guilty in November 2002 and expressed remorse, Damji initially claimed it wasn't greed but threats by Mob figures that led him down the path to large-scale fraud.

Damji told investors he owned a tooth-whitening product called "Instant White" and that he was about to sell the rights to the giant Colgate Palmolive Corp. Damji promised $20 back on every dollar invested, a 2,000 per cent return.

It was called an affinity fraud because Damji's targets were exclusively members of his religious community, the Ismailis. They are a sect of Islam, followers of the Aga Khan. He had credibility because prominent people believed in him, one investor said at the time.

The scheme started to come undone when Colgate denied the purchase.

His lawyer told the court Damji was also "forced" to buy nine luxury cars worth $500,000 just to

show he was successful while funnelling millions from investors to organized crime lords in Costa Rica and Jamaica.

He spent about $4 million on property, including an $800,000 waterfront condominium, paid for in cash, two houses in Markham and a small strip mall in midtown Toronto, worth over $2 million.

And he was generous with other peoples' money.

An Internet search found an announcement that the Aga Khan Foundation Canada's Partnership Walk received its "largest-ever corporate donation," a $1.5 million gift from "Dr. Salim Damji and family."

But according to the parole board, Damji now admits the fraud was fuelled by his gambling addiction and that he has received various treatment regimens, the documents indicate.

The board said he bet up to $500,000 at a time – a compulsion stemming from low self-esteem as he bought "people's love with money and gifts."

.

Back in and out of jail since his original parole in December 2003, Damji was finally granted day parole last October, records show. Damji appears in a Toronto court tomorrow.

South China Morning Post 南華早報

Ice Queen pledged to sell fast food

Wednesday, 28 February, 1996, 12:00am

From ALAN MERRIDEW in Vancouver

THE world's most notorious woman drug trafficker was allowed to settle in Canada because she promised to run a fast-food chicken franchise, according to a Toronto newspaper.

Hong Kong-based Lee Chau-ping, known as the Ice Queen, made only two short trips to La Ronge, Saskatchewan, before the authorities approved her immigration as an entrepreneur willing to invest C$170,000 (about HK$958,000), the Globe and Mail reported.

The paper said Lee, her husband - with whom she had not lived for at least two years - and their two school-age children were admitted as immigrants in Vancouver on May 22, 1992.

They had been briefly interviewed at a Canadian immigration office in Seattle, in the United States.

Less than a week earlier, Guangdong authorities had raided and shut down several of her factories making the drug ice.

Lee disappeared from Canada 18 months later leaving her children, her husband and more than CS$1 million in assets.

She faces criminal charges in Hong Kong, China, Thailand and Canada and is on the Interpol wanted list.

The Canadian Government wants to strip her of her Canadian assets including a C$800,000 house in Vancouver's Kerrisdale area, a house in British Columbia, and jewellery.

The Globe said Hong Kong authorities were 'shaking their heads about how easy it is for Asian criminals to get into Canada'.

'Their amazement echoes longstanding criticism from several quarters that the federal Government's business immigration programme really amounts to selling passports to the carriage

trade and to criminals,' the paper said.

Topics: Hong Kong
Indictment
Vancouver
British Columbia
Hong Kong

Grant Thornton

Reporting Entity Sector Profiles: DPMS Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

DPMS Sector NAICS Codes

Identified as regulated activity

Code	Description
339910	Jewellery and silverware manufacturing
418920	Mineral, ore and precious metal merchant wholesalers
423940	Jewellery, watches precious stone, and precious metal merchant wholesalers
448310	Jewelry Stores
522299	All other non-depository credit intermediation (Pawn shops)
523210	Securities and commodity exchanges
523990	All other financial investment activities

Identified as unregulated activity

Code	Description
212220	Gold and silver ore mining
212221	Gold ore mining
212222	Silver ore mining
33141	Non-ferrous metal (except aluminum) smelting and refining
522299	All other non-depository credit intermediation (Pawn shops)

Using NAICs codes, searches for statistical data on the DPMS industry were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

DPMS Sector SIC Codes

Identified as regulated activity

Code	Description
3911	Jewellery, precious metal
5094	Precious Stones, Metals, Watches, Jewellery
5933	Pawn Shops
5944	Jewelry Stores
6413	Commodity Brokers
6422	Commodity Exchange
8792	Jewellery retailing

Identified as unregulated activity

Code	Description
104	Gold and silver ores
1041	Gold ores
1044	Silver ores

Please note that the SIC-C has been replaced by NAICS Canada. Once implementation of NAICS Canada is complete, the SIC-C will be discontinued.

Establishments: Jewellery and silverware manufacturing (NAICS 33991)

Number of establishments in Canada by type and region: December 2012 Jewellery and Silverware Manufacturing (NAICS 33991)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	29	48	77	8.7%
British Columbia	70	91	161	18.1%
Manitoba	11	6	17	1.9%
New Brunswick	4	4	8	0.9%
Newfoundland and Labrador	3	3	6	0.7%
Northwest Territories	1	0	1	0.1%
Nova Scotia	5	4	9	1.0%
Nunavut	0	0	0	0.0%
Ontario	135	217	352	39.6%
Prince Edward Island	2	0	2	0.2%
Quebec	134	111	245	27.5%
Saskatchewan	7	2	9	1.0%
Yukon Territory	2	1	3	0.3%
CANADA	403	487	890	100%
Percent Distribution	45.3%	54.7%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Jewellery and Silverware Manufacturing (NAICS33991)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	19	10	0	0
British Columbia	42	28	0	0
Manitoba	5	5	1	0
New Brunswick	2	2	0	0
Newfoundland and Labrador	3	0	0	0
Northwest Territories	0	1	0	0
Nova Scotia	4	1	0	0
Nunavut	0	0	0	0
Ontario	85	49	1	0
Prince Edward Island	2	0	0	0
Quebec	83	51	0	0
Saskatchewan	7	0	0	0
Yukon Territory	2	0	0	0
CANADA	254	147	2	0
Percent Distribution	63.0%	36.5%	0.5%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Mineral, ore and precious metal wholesaler-distributor (NAICS 41892)

Number of establishments in Canada by type and region: December 2012 Mineral, Ore and Precious Metal Wholesaler-Distributors (NAICS 41892)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	7	5	12	9.4%
British Columbia	10	10	20	15.6%
Manitoba	2	2	4	3.1%
New Brunswick	1	0	1	0.8%
Newfoundland and Labrador	1	1	2	1.6%
Northwest Territories	0	0	0	0.0%
Nova Scotia	2	1	3	2.3%
Nunavut	0	0	0	0.0%
Ontario	27	35	62	48.4%
Prince Edward Island	0	0	0	0.0%
Quebec	11	10	21	16.4%
Saskatchewan	0	2	2	1.6%
Yukon Territory	1	0	1	0.8%
CANADA	62	66	128	100%
Percent Distribution	48.4%	51.6%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Mineral, Ore and Precious Metal Wholesaler-Distributors (NAICS41892)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	4	3	0	0
British Columbia	5	4	1	0
Manitoba	0	2	0	0
New Brunswick	0	1	0	0
Newfoundland and Labrador	1	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	2	0	0	0
Nunavut	0	0	0	0
Ontario	17	10	0	0
Prince Edward Island	0	0	0	0
Quebec	8	2	1	0
Saskatchewan	0	0	0	0
Yukon Territory	1	0	0	0
CANADA	38	22	2	0
Percent Distribution	61.3%	35.5%	3.2%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Jewellery stores (NAICS 44831)

Number of establishments in Canada by type and region: December 2012 Jewellery Stores (NAICS 44831)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	307	155	462	10.6%
British Columbia	369	276	645	14.8%
Manitoba	83	42	125	2.9%
New Brunswick	54	23	77	1.8%
Newfoundland and Labrador	21	5	26	0.6%
Northwest Territories	6	0	6	0.1%
Nova Scotia	47	19	66	1.5%
Nunavut	0	0	0	0.0%
Ontario	1,032	810	1,842	42.2%
Prince Edward Island	8	5	13	0.3%
Quebec	642	360	1,002	23.0%
Saskatchewan	59	37	96	2.2%
Yukon Territory	4	1	5	0.1%
CANADA	2,632	1,733	4,365	100%
Percent Distribution	60.3%	39.7%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Jewellery Stores (NAICS44831)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	131	174	2	0
British Columbia	192	176	1	0
Manitoba	31	52	0	0
New Brunswick	29	25	0	0
Newfoundland and Labrador	10	11	0	0
Northwest Territories	3	3	0	0
Nova Scotia	28	18	1	0
Nunavut	0	0	0	0
Ontario	587	441	2	2
Prince Edward Island	2	6	0	0
Quebec	387	250	3	2
Saskatchewan	25	34	0	0
Yukon Territory	2	2	0	0
CANADA	1,427	1,192	9	4
Percent Distribution	54.2%	45.3%	0.3%	0.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Securities and commodity exchanges (NAICS 52321)

Number of establishments in Canada by type and region: December 2012 Securities and Commodity Exchanges (NAICS 52321)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	12	26	38	14.4%
British Columbia	15	43	58	22.1%
Manitoba	2	8	10	3.8%
New Brunswick	2	2	4	1.5%
Newfoundland and Labrador	2	0	2	0.8%
Northwest Territories	0	0	0	0.0%
Nova Scotia	2	4	6	2.3%
Nunavut	0	0	0	0.0%
Ontario	26	77	103	39.2%
Prince Edward Island	0	0	0	0.0%
Quebec	6	28	34	12.9%
Saskatchewan	1	7	8	3.0%
Yukon Territory	0	0	0	0.0%
CANADA	68	195	263	100%
Percent Distribution	25.9%	74.1%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Securities and Commodity Exchanges (NAICS 52321)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	8	4	0	0
British Columbia	13	1	1	0
Manitoba	1	1	0	0
New Brunswick	2	0	0	0
Newfoundland and Labrador	0	2	0	0
Northwest Territories	0	0	0	0
Nova Scotia	1	1	0	0
Nunavut	0	0	0	0
Ontario	10	11	3	2
Prince Edward Island	0	0	0	0
Quebec	2	3	1	0
Saskatchewan	0	1	0	0
Yukon Territory	0	0	0	0
CANADA	37	24	5	2
Percent Distribution	54.4%	35.3%	7.4%	2.9%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Other financial investment activities (NAICS 5239)

Number of employer establishments by employment size category and region: December 2012 Other financial investment Activities (NAICS5239)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	1,274	389	32	9
British Columbia	1,839	504	39	5
Manitoba	368	121	9	8
New Brunswick	142	47	2	1
Newfoundland and Labrador	56	21	1	0
Northwest Territories	6	14	1	0
Nova Scotia	177	67	8	2
Nunavut	2	4	0	0
Ontario	3,947	1,281	131	47
Prince Edward Island	43	14	0	0
Quebec	1,517	710	43	9
Saskatchewan	301	114	11	1
Yukon Territory	13	6	0	0
CANADA	9,685	3,292	277	82
Percent Distribution	72.6%	24.7%	2.1%	0.6%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Other financial investment Activities (NAICS5239)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	1,274	389	32	9
British Columbia	1,839	504	39	5
Manitoba	368	121	9	8
New Brunswick	142	47	2	1
Newfoundland and Labrador	56	21	1	0
Northwest Territories	6	14	1	0
Nova Scotia	177	67	8	2
Nunavut	2	4	0	0
Ontario	3,947	1,281	131	47
Prince Edward Island	43	14	0	0
Quebec	1,517	710	43	9
Saskatchewan	301	114	11	1
Yukon Territory	13	6	0	0
CANADA	9,685	3,292	277	82
Percent Distribution	72.6%	24.7%	2.1%	0.6%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Gold and silver ore mining (NAICS 21222)

Number of establishments in Canada by type and region: December 2012 Gold and Silver Ore Mining (NAICS 21222)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	2	10	12	5.7%
British Columbia	33	51	84	40.0%
Manitoba	2	1	3	1.4%
New Brunswick	0	0	0	0.0%
Newfoundland and Labrador	1	0	1	0.5%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	1	1	0.5%
Nunavut	1	0	1	0.5%
Ontario	23	11	34	16.2%
Prince Edward Island	0	0	0	0.0%
Quebec	19	0	19	9.0%
Saskatchewan	2	0	2	1.0%
Yukon Territory	30	23	53	25.2%
CANADA	113	97	210	100%
Percent Distribution	53.8%	46.2%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Gold and Silver Ore Mining (NAICS21222)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	1	1	0	0
British Columbia	21	11	0	1
Manitoba	0	1	1	0
New Brunswick	0	0	0	0
Newfoundland and Labrador	0	1	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	1	0
Ontario	7	8	5	3
Prince Edward Island	0	0	0	0
Quebec	2	5	10	2
Saskatchewan	0	0	2	0
Yukon Territory	19	11	0	0
CANADA	50	38	19	6
Percent Distribution	44.2%	33.6%	16.8%	5.3%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Non-ferrous metal (except aluminum) smelting and refining (NAICS 33141)

Number of establishments in Canada by type and region: December 2012 Non-Ferrous Metal (except Aluminum) Smelting and Refining (NAICS 33141)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	3	1	4	10.3%
British Columbia	1	0	1	2.6%
Manitoba	1	0	1	2.6%
New Brunswick	1	0	1	2.6%
Newfoundland and Labrador	1	0	1	2.6%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	0	0	0.0%
Nunavut	0	0	0	0.0%
Ontario	11	1	12	30.8%
Prince Edward Island	0	0	0	0.0%
Quebec	16	3	19	48.7%
Saskatchewan	0	0	0	0.0%
Yukon Territory	0	0	0	0.0%
CANADA	34	5	39	100%
Percent Distribution	87.2%	12.8%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Non-Ferrous Metal (except Aluminum) Smelting and Refining (NAICS33141)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	1	1	1	0
British Columbia	0	0	0	1
Manitoba	0	0	0	1
New Brunswick	0	0	0	1
Newfoundland and Labrador	0	0	1	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	2	4	3	2
Prince Edward Island	0	0	0	0
Quebec	4	6	2	4
Saskatchewan	0	0	0	0
Yukon Territory	0	0	0	0
CANADA	7	11	7	9
Percent Distribution	20.6%	32.4%	20.6%	26.5%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: non-depository credit intermediation (includes pawn shops) (NAICS 522299)

Number of establishments in Canada by type and region: December 2012 All Other Non-Depository Credit Intermediation (NAICS 522299)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	166	553	719	12.8%
British Columbia	228	580	808	14.4%
Manitoba	33	127	160	2.8%
New Brunswick	33	39	72	1.3%
Newfoundland and Labrador	16	17	33	0.6%
Northwest Territories	5	4	9	0.2%
Nova Scotia	34	63	97	1.7%
Nunavut	2	1	3	0.1%
Ontario	515	2,098	2,613	46.4%
Prince Edward Island	7	9	16	0.3%
Quebec	221	750	971	17.3%
Saskatchewan	39	79	118	2.1%
Yukon Territory	4	4	8	0.1%
CANADA	1,303	4,324	5,627	100%
Percent Distribution	23.2%	76.8%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 All Other Non-Depository Credit Intermediation (NAICS522299)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	92	71	2	1
British Columbia	131	94	3	0
Manitoba	24	8	1	0
New Brunswick	13	20	0	0
Newfoundland and Labrador	8	8	0	0
Northwest Territories	3	2	0	0
Nova Scotia	14	20	0	0
Nunavut	1	1	0	0
Ontario	316	187	9	3
Prince Edward Island	4	3	0	0
Quebec	109	107	4	1
Saskatchewan	20	17	2	0
Yukon Territory	2	1	1	0
CANADA	737	539	22	5
Percent Distribution	56.6%	41.4%	1.7%	0.4%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Using SIC codes, searches were carried out on Onesource as well as Lexis to extract statistical data on the DPMS sector from Duns Market Identifiers.

SIC Code 5944 – Jewelery Stores

Provinces	Number of Establishments
Alberta	326
British Columbia	358
Manitoba	99
New Brunswick	65
Newfoundland	28
Nova Scotia	69
Northwest Territories	9
Ontario	1010
PEI	13
Quebec	670
Saskatchewan	76
Yukon	6
Grand Total	2729

Source: Lexis (Duns Market Identifiers)

SIC Code 5944 – Jewelery Stores

Province	Number of Establishments
Alberta	440
British Columbia	710
Manitoba	115
New Brunswick	89
Newfoundland and Labrador	41
Northwest Territories	9
Nova Scotia	95
Ontario	1760
Prince Edward Island	18
Quebec	1088
Saskatchewan	103
Yukon	5
Grand Total	4473

Source: OneSource

Two sources (Lexis and Onesource) were used for this search to illustrate the difference in results depending on the source.

Using NAICs codes, we carried out similar searches on Onesource.

SIC Code 5944 – Jewelery Stores

Province	Number of Establishments
Alberta	440
British Columbia	708
Manitoba	115
New Brunswick	89
Newfoundland and Labrador	41
Northwest Territories	9
Nova Scotia	95
Ontario	1760
Prince Edward Island	18
Quebec	1087
Saskatchewan	103
Yukon	5
Grand Total	4470

Source: OneSource

Searches were carried out on OneSource using NAICs and SIC codes relevant to Precious Metals/Bullion.

NAICS Code	NAICS Code Description	Number of Establishments
21222	Gold Ore and Silver Ore Mining	9
212221	Gold Ore Mining	1,176
21221/212210	Iron Ore Mining	48
339910	Jewelry and Silverware Manufacturing	891
423940	Jewelry, Watch, Precious Stone, and Precious Metal Merchant Wholesalers	667
331410	Nonferrous Metal (except Aluminum) Smelting and Refining	44
212222	Silver Ore Mining	68
Grand Total		2,903

NAICS code 423940 - Jewelry, watch, precious stone, and precious metal merchant wholesalers

Provinces	Number of Establishments
Alberta	38
British Columbia	110
Manitoba	13
New Brunswick	2
Newfoundland and Labrador	1
Northwest Territories	1
Nova Scotia	14
Ontario	332
Quebec	150
Saskatchewan	4
Yukon	2
Grand Total	667

SIC Codes	SIC Code Description	Number of Establishments
104	Gold and Silver Ores	9
1041	Gold Ores	1173
3911	Jewellery, Precious Metal	547
5094	Jewellery, Watches, Precious Stones, and Precious Metals	661
5944	Jewellery Stores	4473
3339	Primary Smelting and Refining of Nonferrous Metals, Except Copper and Aluminum	44
3341	Secondary Smelting and Refining of Nonferrous Metals	13
1044	Silver Ores	67
Grand Total		2514

SIC code 5094 - Jewellery, watches, precious stones, and precious metals

Province	Number of Establishments
Alberta	38
British Columbia	109
Manitoba	13
New Brunswick	2
Newfoundland and Labrador	1
Nova Scotia	14
Ontario	328
Quebec	150
Saskatchewan	4
Yukon	2
Grand Total	661

NAICS -522298 - All other non-depository credit intermediation (this classification code includes pawn shops)

Province	Number of Establishments
Alberta	77
British Columbia	106
Manitoba	34
New Brunswick	19
Northwest Territories	1
Nova Scotia	13
Ontario	180
Prince Edward Island	3
Quebec	145
Saskatchewan	36
Yukon	2
Grand Total	616

See below for the Onesource NAICS tree.

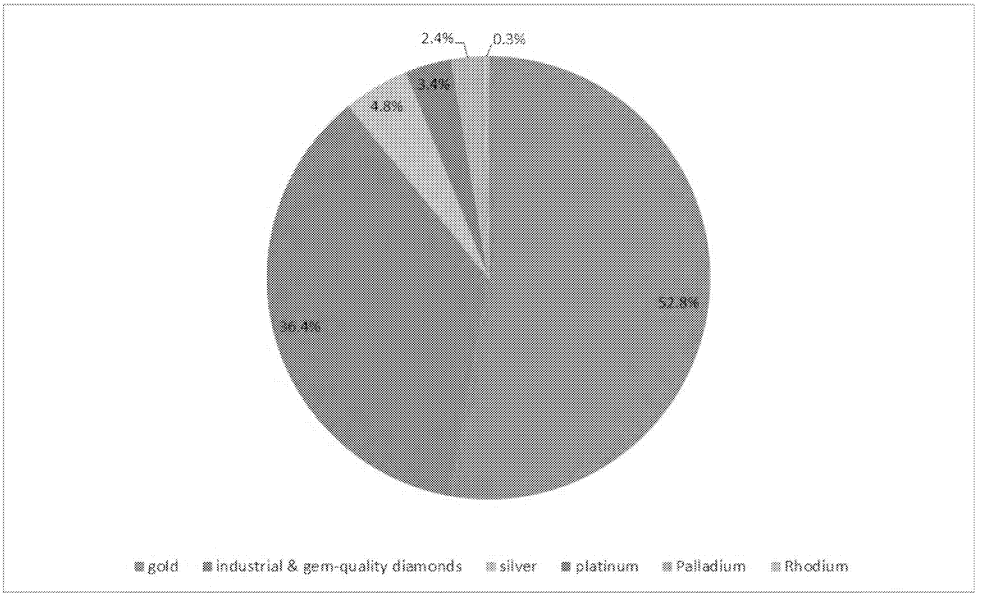
Canada precious metals & minerals market value: $ million, 2008-2012

Year	$ million	C$ million	€ million	% Growth
2008	6,557.5	6,556.4	4,7662.2	
2009	5,921.3	5,920.3	4,303.8	(9.7%)
2010	7,809.0	7,807.7	5,675.9	31.9%
2011	11,554.6	11,552.7	8,398.3	48.0%
2012	10,724.7	10,722.9	7,795.0	(7.2%)
CAGR:2018-2012				13.1%

(MarketLine – October 2013)

Category segmentation (Marketline)

Category	2012	%
Gold	5,664.4	52.8%
Industrial & gem-quality diamonds	3,889.0	36.4%
Silver	511.2	4.8%
Platinum	361.3	3.4%
Palladium	259.0	2.4%
Rhodium	29.7	0.3%
Total	10,714.6	100%



Geography segmentation (Marketline)

Geography	2012	%
United States	14,236.1	28.5%
Canada	10,724.7	21.5%
Mexico	8,930.7	17.9%
Rest of the Americas	15,999.2	32.1%
Total	49,890.7	100.0%

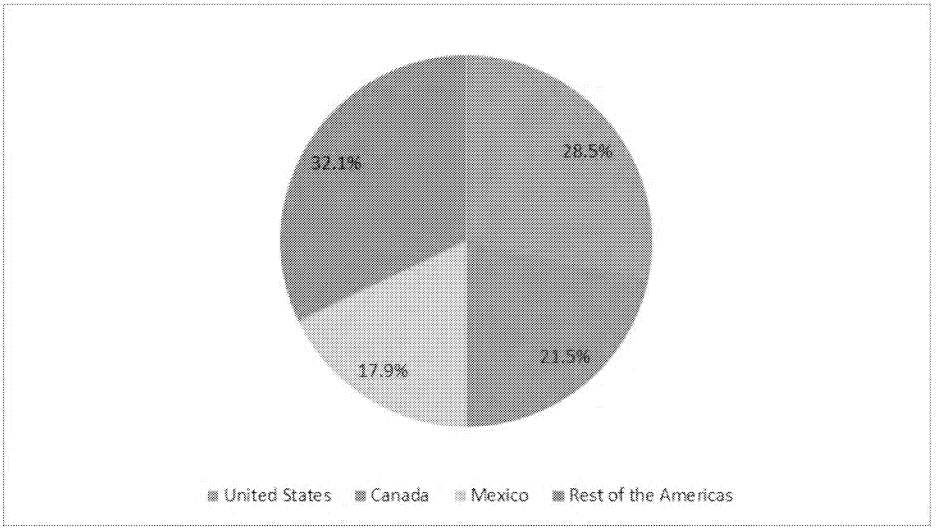


Table 3 Canadian KPCs issued for exports to Participants in 2012

Participant	Q1	Q2	Q3	Q4	Total Count
Armenia	0	1	1	2	4
Australia	0	1	0	0	1
China	0	5	0	5	10
European Community	46	32	38	33	149
India	16	11	17	15	59
Israel	6	3	4	4	17
Norway	1	0	0	0	1
South Africa	1	4	1	3	9
United Arab Emirates	0	1	0	2	3
United States	2	2	8	6	18
Vietnam	0	1	3	5	9
TOTAL	72	61	72	75	280

Source: KPC based data collected by NRCan under the authority of the Minister of NRCan

Table 1: **Production, Exports and Import of rough diamonds in major Producing countries – 2012**

	Production		Import		Export	
Country name	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)
Botswana	20.55	2.98	7.49	2.14	23.35	3.99
Russian Federation	34.93	2.87	0.14	0.15	29.81	3.90
Canada	10.45	2.01	0.76	0.16	11.12	2.16
Angola	8.33	1.11	0	0	9.20	1.15
South Africa	7.08	1.03	11.47	1.08	8.01	1.36
Namibia	1.60	0.90	0.13	0.16	1.68	0.98
Zimbabwe	12.06	0.64	0	0	14.96	0.74
DRC	21.52	0.18	0	0	19.56	0.26

Source: KP statistics[53]

Table 4 2012 Foreign KPCs received by Canada as of April 11, 2012

Participant	Q1	Q2	Q3	Q4	Total Count
Armenia	2	2	7	4	15
China, People's Republic of	0	0	0	1	1
Democratic Republic of Congo	1	0	0	0	1
European Community	35	33	26	31	125
India	0	1	5	3	9
Israel	4	3	2	3	12
Sierra Leone	0	2	0	0	2
South Africa	1	2	1	0	4
United Arab Emirates	1	3	0	0	4
United States	22	26	30	18	96
TOTAL	66	72	71	60	269

Source: KPC based data collected by NRCan under the authority of the Minister of NRCan

414410	Jewellery and Watch Wholesaler-Distributors CAN
	This Canadian industry comprises establishments primarily engaged in wholesaling jewellery, watches, silverware, table flatware, hollowware, and cutlery of precious metal.

Search of Alphabetical Index in NAICS 2007

414410	Clocks, mechanical, wholesale
	Coins, wholesale
	Diamonds (gems), wholesale
	Diamonds, jewellery, wholesale
	Gem stones, wholesale
	Hollowware, table, sterling and silverplate, wholesale
	Imitation stones and pearls, jewellery, wholesale
	Jewellers' findings, precious metal, wholesale
	Jewellery, wholesale
	Silverware and plated ware, wholesale
	Stones, precious, wholesale
	Table flatware and hollowware, sterling and silverplate, wholesale
	Watches , wholesale

Appendix B: Case examples and typologies

The enclosed articles have been sourced from; news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. US investigation links Lebanese Canadian Bank to Hezbollah, Deutsche Welle, December 20, 2011
2. Murky sources of Hizbollah's funding, Straits Times, December 15, 2011
3. SA role in diamond trade slammed, All Africa News, July 7, 2011
4. Organized crime fuelling growing global threat: UN, Waterloo Region Record, June 18, 2010
5. Report exposes Mnangagwa and Mujuru involvement in Marange, All Africa News, June 16, 2010
6. 'Blood diamond' smuggling worries Ottawa: N.W.T. diamond boom has federal government concerned about crime, Edmonton Journal, September 7, 2008
7. Our Far North diamonds a target for smugglers: Money laundering. Boom in mining during last decade, Montreal Gazette, September 5, 2008
8. Police allege blood diamonds found hidden in clothing of man at Edmonton airport, The Canadian Press, February 20, 2008
9. Ex-Madoff programmers wanted payment in diamonds: Jury told, National Post, December 11, 2013
10. Military fraud probe uncovers jewelry stash, Vancouver Sun, October 5, 2013
11. Portus founder ordered to pay $320k; Mendelson also slapped with ban from trading, The Toronto Star, December 1, 2012
12. Portus' Manor must pay $8.8M; Doesn't have it, National Post, August 28, 2012
13. Chasing Manor's Millions: Seven years after the spectacular collapse of his firm, Portus, the mystery persists: What became of the diamonds that Boaz Manor bought with investors' money? The Globe and Mail, October 26, 2012
14. Portus' Manor bought 22-carat diamond with fund investments, Bloomberg.com, October 14, 2005
15. UBS snitch gets US$104M payoff; U S tax-scam reward contrasts with Canada, National Post, September 12, 2012

16. Ponzi loot on auction; Millions in Rotschild scam, The Windsor Star, July 14, 2011

17. Persian rugs, biker bling, other loot for sale; Police recovered property auction displays what people have lost, not including their sense of security, The Globe and Mail, April 20, 2011

18. Lacroix sentenced to 13 years; Former Norbourg head given time for his role in a $130-million fraud that claimed 9,200 victims, The Globe and Mail, October 9, 2009

19. Sentencing hearing delayed for Man., addictions centre head who defrauded Ottawa, The Canadian Press, December 12, 2008

20. Ill-gotten jewelry goes to auction, Calgary Herald, November 14, 2008

21. Diamond exports face new threat, All Africa News, June 16, 2010

22. Crime syndicate exposed: Police 'They themselves believe they're untouchable' Unsolved killings; A dozen alleged members of deadly Shower Posse among 78 people nabbed in 100-officer sweep, The Toronto Star, May 5, 2010

23. Former official with US consulate in Toronto sentenced to 1 year in visa bribery scheme, The Canadian Press, July 29, 2009

24. Guilty plea in crime ring stung by lost luggage; Bank robbery proceeds used to finance terror, National Post, March 8, 2008

25. Dubai refinery Kaloti, DMCC caught in $5bn global gold scandal, Arabian Business, February 26, 2014

26. Dubai refiner Kaloti Group linked to conflict gold scandal by E&Y whistleblower, International Business Times, February 26, 2014

27. Confidential papers raise fears over conflict gold, The Guardian, February 26, 2014

28. Gold rush hits Calgary precious metals dealers, Calgary Herald, August 10, 2011

29. Nothing to declare: Russian busted smuggling 26,000 diamonds, RT.com, March 11, 2013

30. Rush to cash in gold attracts tarnish of possible scams, The Globe and Mail, November 11, 2010

31. Bling losing its lustre, The Toronto Star, July 15, 2009

32. Stop buying and selling blood diamonds, Rappaport Magazine, February 2010

33. Canada to unveil diamond market, The Globe and Mail, January 28, 2010

34. Skilled immigrants staff Sudbury gem plant, October 14, 2009

35. RCMP issues warning on diamonds, Financial Post, August 10, 2011

36. Peoples gets new parent, National Post, February 20, 2014

US investigation links Lebanese Canadian Bank to Hezbollah

1,138 words
20 December 2011
07:45
Deutsche Welle
DEUEN
English

A US investigation has revealed that proceeds from drug smuggling and other criminal enterprises have been laundered through a prominent Lebanese bank and used as funding for militant group Hezbollah.

A six-year investigation by the United States into the inner workings of the Lebanese Canadian Bank (LCB), one of Beirut's many secretive financial institutions, has revealed an intricate web of money laundering and criminal activity through which the militant group Hezbollah has been deriving new strands of funding.

In an extensive report by the New York Times last week, the US operation into the LCB's activities, which began shortly after Hezbollah's 2006 summer war with Israel, has revealed that the depths of the bank's connections with the powerful Lebanese militant group have been carefully buried under untainted assets for years.

After painstakingly gathering information from undercover sources and networks, the investigation, according to the NYT, has hit pay dirt in the last few months with damaging evidence emerging during the sale of the LCB, a former subsidiary of the Royal Bank of Canada Middle East, to a Beirut-based partner of the French banking giant Société Générale.

Warning bells began ringing when intelligence agencies started noticing Lebanese Shiites working for South American drug cartels. However, one of the biggest breakthroughs in the pursuit of evidence against Hezbollah and its connections with the LCB came in 2007 when Chekri Mahmoud Harb, a Lebanese middleman working with a Colombian cartel, revealed his Hezbollah connections to an undercover agent.

Harb's link failed to bear fruit but investigators were then lucky enough to get a second chance when cash from the used car racket ended up in an exchange house owned by the family of Ayman Joumaa, a former cartel member and now owner of the Caesars Park Hotel in Beirut with alleged connections to Hezbollah's 1800 Unit (elite group believed to coordinate attacks inside Israel - the ed.), and another down the street from his hotel. The exchanges then deposited the money into accounts held by the Lebanese Canadian Bank.

Criminal activities funding Hezbollah

It was only during the sale procedure, when the LCB's ledgers were opened and deeply investigated, that the extent of the bank's connection to Hezbollah became evident. The accounts have also shone light on how the militant group has managed to fund its rise to political and military prominence in Lebanon at a time when its main benefactors in Iran and Syria have suffered under the weight of international sanctions and growing public unrest.

Iran alone has been cited by US sources as providing as much as $200 million (153.5 million euros) annually, although this has been drastically reduced in recent years by the crippling restrictions placed on Tehran's own financial sector in response to its unwillingness to give up its nuclear ambitions.

With Syria's own financial crisis being exacerbated by its increasingly violent civil uprising, Hezbollah has had to look elsewhere.

"It's not much of a secret anymore that Hezbollah used illicit channels to raise funds, or **launder** money," Reinoud Leenders, Middle East expert and assistant professor International Relations at the University of Amsterdam, told Deutsche Welle. "I wouldn't be surprised if they use some Lebanese banks for their finances, which are not unknown in the world of money laundering due to ineffective controls and regulations despite what Lebanese officials may tell you."

It has long been known that Hezbollah has benefited from financial contributions from foreign loyalists and funding from elements of the large Lebanese Diaspora abroad who have successfully circumvented attempts to cut off the militant group's economic lifeblood.

What the recent revelations have shown is that this Diaspora, spread throughout Europe, Africa and South America, has provided Hezbollah with a ready made network of contacts involved in an intricate global money-laundering apparatus involving drug trafficking and other criminal activities which have in turn allowed Hezbollah to move huge sums of money into the legitimate financial system.

Drugs, cars and consumer goods

The web of criminality allegedly stretches around the world and involves South American drug cartels, goods exporters in Asia, car dealerships in the United States and Africa, and Shiite Muslim businessmen dealing in everything from conflict **diamonds** to frozen chicken.

"Among other things, there are reasons to believe that Hezbollah is involved in cigarette smuggling in the US, the trade in blood **diamonds** in West Africa, and in recent financial scams in Lebanon," said Leenders.

Intelligence from several countries, not just the United States, has also revealed the direct involvement of high-level Hezbollah officials in the cocaine trade in South America.

Through the group's connections with the cartels, cocaine is sent through the porous border where Brazil, Paraguay and Argentina meet then onto Colombia and Venezuela where it is then sent to Europe via West African countries like Benin and Gambia. The cocaine is then moved north through Portugal or Spain, or east via Syria and Lebanon.

Profits from the highly lucrative European narcotics market are then transferred back to African accounts.

Used cars are then shipped from the United States to Africa where the proceeds from their sale is mixed with the European drug profits and sent to the Lebanese Canadian Bank via exchange houses across the Middle East. Some of the money is sent back to the US to buy more used cars while some is diverted to Hezbollah.

Another portion of the money is transferred through accounts in the United States to pay Asian consumer goods suppliers in countries such as China. The consumer goods are then shipped to South America where they are sold to pay off the drug cartels.

The NYT report said that the US investigation had revealed that hundreds of millions of dollars a year have passed through nearly 200 accounts associated with companies allegedly used as fronts for Hezbollah.

Whether any subsequent US action damaged Hezbollah's financial structure is still a matter of debate.

"The Lebanese banking establishment is very aware of how this could potentially affect stability in Lebanon and Hezbollah's grip on power and this is why the affair of the Lebanese-Canadian bank was dealt with very swiftly," Nadim Shehadi, a Middle East expert at Chatham House, told Deutsche Welle. "It would now be difficult for anybody to channel illegal money through Lebanese banks."

According to Leenders it's unlikely to have any direct impact on Hezbollah.

"They have very likely diversified their financial flows to the extent that no one measure against them can stop them. The potentially precarious support by both Syria and Iran will also have prompted Hezbollah to look for revenues beyond them, including by raising funds in the Lebanese Shiite diaspora," he said.

Author: Nick AmiesEditor: Rob Mudge

15612492

Document DEUEN00020111220e7ck000b7

The Straits Times
The Sunday Times

World
Murky sources of Hizbollah's funding

735 words
15 December 2011
Straits Times
STIMES
English

Ledgers of Lebanese bank with links to militant group expose big role in drug trade

BEIRUT: In February this year, the Obama administration accused one of Lebanon's famously secretive banks of laundering money for an international cocaine ring with ties to the Shi'ite militant group Hizbollah.

The books offer evidence of an intricate global money-laundering apparatus that, with the bank as its hub, appeared to let Hizbollah move huge sums of money into the legitimate financial system, despite sanctions aimed at cutting off its economic lifeblood.

At the same time, the investigation that led the United States to the Lebanese Canadian Bank provides new insights into the murky sources of Hizbollah's money. Intelligence from several countries points to the direct involvement of high-level Hizbollah officials in the South American cocaine trade.

On Tuesday, federal prosecutors in Virginia announced the indictment of the man at the centre of the Lebanese Canadian Bank case - Ayman Joumaa, 47, a Lebanese - charging that he had trafficked drugs and laundered money for Colombian cartels and the Mexican gang Los Zetas.

The revelations about Hizbollah and the Lebanese Canadian Bank reflect the changing political and military dynamics of Lebanon and the Middle East.

American intelligence analysts believe that for years Hizbollah received as much as US$200 million (S$260 million) annually from its primary patron, Iran, along with additional aid from Syria.

But that support has diminished, the analysts say, as Iran's economy buckles under international sanctions over its nuclear programme and Syria's government battles rising popular unrest.

'The ability of terror groups like Hizbollah to tap into the worldwide criminal funding streams is the new post-9/11 challenge,' said Mr Derek Maltz, the Drug Enforcement Administration official who oversaw the agency's investigation into the Lebanese Canadian Bank, once a subsidiary of the Royal Bank of Canada Middle East.

In that inquiry, US Treasury officials said senior bank managers had assisted a handful of account holders in running a scheme to **launder** drug money by mixing it with the proceeds of used cars bought in the US and sold in Africa.

The outlines of a broader laundering network, and the degree to which Hizbollah's business had come to suffuse the bank's operations, emerged in recent months as the bank's untainted assets were being sold.

In all, hundreds of millions of dollars a year sloshed through the accounts, held mainly by Shi'ite Muslim businessmen in the drug-smuggling nations of West Africa, many of them known Hizbollah supporters, trading in everything from rough-cut **diamonds** to cosmetics to frozen chicken, according to people with knowledge of the matter in the US and Europe.

For the US, taking down the bank was part of a long-running strategy of deploying financial weapons to fight terrorism.

As the case travelled up the administration's chain of command beginning in autumn last year, the prevailing view was that it offered what one official called 'a great opportunity to dirty up Hizbollah' .

Founded three decades ago as a guerilla force aimed at the Israeli occupation of southern Lebanon, Hizbollah has never before had such a prominent place in the country's official politics.

Yet much of its power derives from elsewhere - from its status as a state within the Lebanese state. That this sliver of a country would be a crossroads for all manner of trade owes much to the flourishing of a worldwide diaspora; more Lebanese live abroad than at home.

Through criminal elements in these emigre communities, Hizbollah has gained a deepening foothold in the cocaine business, according to an assessment by the United Nations Office on Drugs and Crime described in a leaked 2009 State Department cable.

In South America and Europe, prosecutors began noticing Lebanese Shi'ite middlemen working for the cartels. But the strongest evidence of an expanding Hizbollah role in the drug trade comes from the two investigations that ultimately led to the Lebanese Canadian Bank.

From the Treasury Department's perspective, the case is a victory, albeit an incremental one, in the battle against terrorism financing.

Still, Treasury officials have no illusions that their work here is done.

NEW YORK TIMES

A Hizbollah-linked entity purchased this large parcel of land in the Chouf region of Lebanon with financing from the Lebanese Canadian Bank. -- PHOTO: NEW YORK TIMES

Document STIMES0020111214e7cf0001l

SA Role in Diamond Trade Slammed

by Alex Bell
461 words
7 July 2011
02:33
All Africa
AFNWS
English

Jul 07, 2011 (SW Radio Africa/All Africa Global Media via COMTEX) -- South Africa's role in getting Zimbabwe's **diamonds** back into international trade is being slammed as "dangerous", amid revelations that government officials there have helped export millions of dollars worth of Zim **diamonds**.

South Africa's State Diamond Trader officials admitted in parliament last week that they had helped Zimbabwe export **diamonds** from Chiadzwa, despite an international ban on the trade. During a meeting of the international trade watchdog the Kimberley Process (KP) last month the country's Mines Minister Susan Shabangu, had also publicly stated that **diamonds** from the controversial Chiadzwa diamond fields were tradeable.

That meeting ended with no consensus from KP members of Zimbabwe's future in the international diamond industry. But despite this lack of consensus the KP chair, Mathieu Yamba, announced that Zimbabwe had the green light to resume exports. It's widely understood that this unilateral declaration was prompted by South Africa's open support for Zimbabwe.

The announcement has been rejected by a number of other KP members, including the US, Canada, Australia, Israel and most recently, Switzerland. Analysts have now warned that the apparent split down the middle of the KP membership on how to proceed with Zimbabwe, threatens to collapse the monitoring body completely.

Alan Martin from Partnership Africa Canada (PAC), one of the civil society groups who are part of the KP, told SW Radio Africa on Wednesday that South Africa was playing a "very dangerous game," at a time when "the KP is on life support." Martin said that South Africa had effectively put its own **diamonds** on a par with Chiadzwa **diamonds**, if it continues to "**launder**" stones from there en route to other countries, like India or the United Arab Emirates (UAE).

"South Africa is jeopardising its own industry and is really playing the wrong kind of leadership role. I'm afraid this is going to have very serious ramifications for South Africa," Martin said.

Martin continued by saying that Africa's support for Zimbabwe has taken a suicidal turn, which threatens the entire continent's future in the diamond trade.

"Africa has shot itself in the head and is effectively wasting political capital by shoring up a bunch of crooks and thugs in Zimbabwe, and not recognising that the industry is at stake," Martin warned.

He explained that diamond traders, cutters, polishers and even consumers "are going to turn to other sources that will guarantee their **diamonds** are not sourced badly," explaining that the whole of Africa is being viewed negatively because of Zimbabwe.

"This could be the worst thing to happen to African diamond producing countries since the wars of West Africa," Martin said.

Document AFNWS00020110707e77700031

NEWS
Organized crime fuelling growing global threat: UN

By Edith M. Lederer
The Associated Press
403 words
18 June 2010
Waterloo Region Record
TKWR
Final
A10
English

NEW YORK

The UN drug and crime czar warned Thursday that international crime syndicates pose a growing threat to global security and called for a new campaign to disrupt the markets for their illicit goods and activities in the U.S. and other rich nations.

Antonio Maria Costa told a high-level General Assembly meeting that demand for illegal drugs, **diamonds** and other items is fuelling transnational organized crime and while arresting some traffickers may divert the flow of goods it will not shut them off.

"Therefore, in order to more effectively fight organized crime, we must shift focus from disrupting the mafias to disrupting their markets," he said. "We must also crack down on the accomplices of crime, like the army of white-collar criminals - lawyers, accountants, realtors and bankers - who cover them up and **launder** their proceeds."

UN Secretary-General Ban Ki-moon said the threat from transnational crime syndicates is growing and the ability of countries to deliver justice "is not evolving as quickly as the criminals' skill at evading justice."

Ban and Costa called for all countries to ratify and implement the UN Convention Against Transnational Organized Crime adopted by the General Assembly in 2000. It commits countries that ratify the treaty to adopting uniform laws to fight organized crime, strengthen money laundering investigations, and streamline extradition processes - and to co-operate with each other to combat illegal activities such as human trafficking.

"Unfortunately, over the past decade, the treaty has suffered from benign neglect," said Costa, who heads the UN Office of Drugs and Crime.

Costa's appearance coincided with the release of a report by his office titled The Globalization of Crime: A Transnational Organized Crime Threat Assessment, which said organized crime has transformed itself into one of the world's foremost economic and armed powers, leaving law enforcement to grasp for an adequate international response.

He told the General Assembly profits from illegal activities has enabled criminals "to influence elections, politicians and power - even the military."

The weakest countries face the greatest risks and some, including in Central America and West Africa, have been infiltrated from the top down while others are under attack, Costa said.

Meanwhile, about 70 per cent of profits from the $72 billion cocaine market go to mid-level dealers in consumer countries, according to the report.

Document TKWR000020100618e66i0001w

Report Exposes Mnangagwa And Mujuru Involvement in Marange

by Violet Gonda
643 words
16 June 2010
12:07
All Africa
AFNWS
English

Jun 16, 2010 (SW Radio Africa/All Africa Global Media via COMTEX) -- An international rights group, Partnership Africa Canada, issued a damning report Monday which exposes some of the players who have been at the forefront of the plunder of **diamonds** in Chiadzwa, Marange.

Titled: **Diamonds** and Clubs: The Militarized Control of **Diamonds** and Power in Zimbabwe, the report shows how the Chiadzwa **diamonds** are sustaining the ZANU PF regime and also fuelling the ongoing political conflict.

The report highlights individuals like former army general Solomon Mujuru, who is heavily involved in illegal diamond deals and also uses his diamond mine 'River Ranch' to **launder** the family's ongoing plunder of resources from the Democratic Republic of Congo.

The report goes on to say that the same personalities who orchestrated the invasion and seizure of white-owned farms and manipulated forex exchange rates have perfected their illicit behaviour and are now battling for control of Zimbabwe's **diamonds**.

Those named in the report include ZANU PF Minister of Defence Emmerson Mnangagwa, his longtime political foe and husband of one of the Vice Presidents, General Mujuru and the true 'power brokers' of Zimbabwean politics, the Joint Operations Command (JOC). "The military chiefs are the high priests of Zimbabwean politics, the final arbiters of tough decisions, and the architects of every single government sponsored act of repression from the 1985 massacres in Matabeleland, to the farm invasions, to successive episodes of election-related violence."

Defense Force Commander General Constantine Chiwenga, Air Force Commander Perence Shiri and police Commissioner Augustine Chihuri are among the elite members of the formidable JOC.

In March Finance Minister Tendai Biti was quoted as saying that almost four years after the military took control of Marange, not one cent had gone into the national treasury.

River Ranch, which General Mujuru controversially grabbed at gunpoint in 2004, is another contested diamond area that the international rights group says is inextricably linked to the pursuit of political power and defiance of Kimberley Process protocols. PAC says: "The mine goes to the very heart of Mujuru's struggle for control of ZANU"

"Mujuru has also controversially obtained technical assistance after the takeover (of the mine) from the African Management Service Company, a joint entity managed by the United Nations Development Programme and the World Bank's International Finance Corporation," said the report.

PAC noted that the story of Zimbabwe's contested diamond fields is about many things including 'smuggling', 'a scramble fuelled by raw economic desperation and unfathomable greed' and heart-wrenching cases of government-sponsored repression and human rights violations.

"These political elites are intimately tied to Zimbabwe's military establishment, the Joint Operation Command, and as such constitute a "rebel movement" opposed to the democratic governance of Zimbabwe."

The report also notes that it is often incorrectly assumed that the only fight for power in Zimbabwe is between the two parties, ZANU PF and the MDC, but in reality the main turf war is within ZANU PF. "While Mnangagwa's support base within the JOC places him closer to Marange's riches, River Ranch affords Mujuru unfettered access to his own diamond resource, one that he has protected with no less ruthlessness."

Mujuru is also said to have shares in African Consolidated Resources (ACR), the company in the middle of a legal battle with the government over mining rights in Chiadzwa. ACR CEO Andrew Cranswick is described in the report as having aligned himself with the wrong faction in ZANU PF.

"Mujuru was to provide Cranswick political coverage, as the latter comes from a family with the wrong political pedigree. (His family was known to be big supporters of Ian Smith's Rhodesian Front). Instead, Cranswick is now paying the price for backing the wrong horse in the ZANU succession race."

Document AFNWS00020100616e66g00167

EDMONTON JOURNAL

News
'Blood diamond' smuggling worries Ottawa; N.W.T. diamond boom has federal government concerned about crime

Andrew Mayeda
Canwest News Service
770 words
7 September 2008
Edmonton Journal
EDJR
Final
D10
English

OTTAWA

The diamond industry in Canada's Far North is vulnerable to smugglers looking to import "blood **diamonds**" or **launder** the proceeds of organized crime syndicates and terrorist organizations, newly released federal documents say.

A boom in diamond mining during the last decade has rapidly turned Canada into the third-biggest producer in the world and created jobs in the North, especially in the Northwest Territories where the country's biggest mines are based.

But Canadian authorities warn the fledgling industry could become a vehicle for money laundering.

"**Diamonds** have been, and continue to be, a main source of currency for both terrorist organizations and organized crime," states a briefing note prepared by Citizenship and Immigration Canada in April.

"Conflict/blood **diamonds** are used to fund rebel operations, purchase arms and other illicit activities (drugs). They are portable, high value and cannot be detected by any type of screening method," continues the note, obtained by Canwest News Service under the Access to Information Act.

Blood **diamonds**, sometimes known as "conflict" **diamonds**, are typically mined in African countries wracked by civil war and used to finance rebel or government forces.

Last week, Prime Minister Stephen Harper travelled to the Northwest Territories and Yukon to demonstrate his government's commitment to asserting Canada's Arctic sovereignty. In a speech in Inuvik, N.W.T., Harper promised to "encourage responsible development of the North's abundant economic resources."

In April, the Privy Council Office, the bureaucratic arm of the Prime Minister's Office, convened a meeting with various departments to discuss security and intelligence issues in Canada's Arctic, e-mails obtained by Canwest News Service reveal.

Among other things, PCO officials asked for briefings on illegal immigration and smuggling in the "Arctic region and northern Canada."

The briefing note suggests that temporary foreign workers hired by the diamond industry could be recruited by smugglers.

"With the rapid growth of the industry, Canada will continue to require a significant amount of foreign skill to develop and sustain the industry. These skilled workers generally earn below poverty-line wages in their country of origin. In Canada, the wages are low compared to the high cost of living in the North. This may be incentive for the workers to conduct illegal activities such as diamond smuggling on behalf of the employer," states the note, portions of which have been blanked out.

The document notes there has been a "drastic increase" in applications by employers looking to hire foreign workers, with roughly 100 new positions confirmed in the past year.

Pierre Leblanc, a retired colonel who now works as a consultant to the diamond industry, said smuggling has been an ongoing concern for the industry, especially since banks tightened money-laundering controls in the wake of the Sept. 11, 2001, terrorist attacks.

But he said Canada has one of the cleanest diamond sectors in the world, because much of the supply chain is automated and companies here used sophisticated systems to track **diamonds**.

"Very few people touch the **diamonds**, because it's all an automated system. And it's automated not only for cost efficiency, but also security," said Leblanc, former commander of the Canadian Forces' Northern Area.

Diamond miners in Canada adhere to the Kimberley Process, a system implemented by the industry in 2003 to filter out blood **diamonds**, he added.

Leblanc said there was a significant influx of workers from countries such South Africa and Belgium after the first Canadian mine opened in 1998, but most employees in the industry are now Canadian.

He noted the RCMP, which has established a Diamond Protection Services unit, has been "proactive" in monitoring for smugglers.

The diamond industry isn't the only northern business that has raised concerns among the Mounties.

According to separate documents obtained by Canwest News Service, the RCMP is worried the Mackenzie Valley pipeline project could put a strain on policing activities in the region.

"From a contract-policing perspective, the immediate and long-term social impacts of the Mackenzie Gas Project will include increased community crime, family disruption, violence and substance abuse," states an RCMP update prepared in November 2007.

"From a federal perspective, the greatly increased risk of organized criminal activity, including high-level drug trafficking, economic crime, immigration issues, Arctic sovereignty challenges and potential terrorist activity are all believed to be areas of concern."

The oft-delayed project is expected to carry natural gas from the Mackenzie River delta in the Northwest Territories to markets throughout North America.

Document EDJR000020080908e497000gp

The Gazette

News
Our Far North diamonds a target for smugglers; Money laundering. Boom in mining during last decade

ANDREW MAYEDA
Canwest News Service
748 words
5 September 2008
Montreal Gazette
MTLG
Final
A12
English

OTTAWA

The diamond industry in Canada's Far North is vulnerable to smugglers looking to import "blood **diamonds**" or **launder** the proceeds of organized crime syndicates and terrorist organizations, newly released federal documents say.

A boom in diamond mining during the last decade has rapidly turned Canada into the third-biggest producer in the world and created jobs in the North, especially in the Northwest Territories where the country's biggest mines are based.

But Canadian authorities warn the fledgling industry could become a vehicle for money laundering.

"**Diamonds** have been, and continue to be, a main source of currency for both terrorist organizations and organized crime," states a briefing note prepared by Citizenship and Immigration Canada in April.

"Conflict/blood **diamonds** are used to fund rebel operations, purchase arms, and other illicit activities (drugs). They are portable, high value and cannot be detected by any type of screening method," continues the note, obtained by Canwest News Service under the Access to Information Act.

Blood **diamonds**, sometimes known as "conflict" **diamonds**, are typically mined in African countries wracked by civil war and used to finance rebel or government forces.

Last week, Prime Minister Stephen Harper travelled to the Northwest Territories and Yukon to demonstrate his government's commitment to asserting Canada's Arctic sovereignty. In a speech in Inuvik, N.W.T., Harper promised to "encourage responsible development of the North's abundant economic resources."

In April, the Privy Council Office, the bureaucratic arm of the Prime Minister's Office, convened a meeting with various departments to discuss security and intelligence issues in Canada's Arctic, emails obtained by Canwest News Service reveal.

Among other things, PCO officials asked for briefings on illegal immigration and smuggling in the "Arctic region and northern Canada."

The briefing note suggests that temporary foreign workers hired by the diamond industry could be recruited by smugglers.

"With the rapid growth of the industry, Canada will continue to require a significant amount of foreign skill to develop and sustain the industry. These skilled workers generally earn below poverty-line wages in their country of origin. In Canada, the wages are low compared to the high cost of living in the North.

"This may be incentive for the workers to conduct illegal activities such as diamond smuggling on behalf of the employer," states the note, portions of which have been blanked out.

The document notes there has been a "drastic increase" in applications by employers looking to hire foreign workers, with roughly 100 new positions confirmed in the past year.

Pierre Leblanc, a retired colonel who now works as a consultant to the diamond industry, said smuggling has been an ongoing concern for the industry, especially since banks tightened money-laundering controls in the wake of the Sept. 11, 2001, terrorist attacks.

But he said Canada has one of the cleanest diamond sectors in the world, because much of the supply chain is automated and companies here used sophisticated systems to track **diamonds**.

"Very few people touch the **diamonds**, because it's all an automated system. And it's automated not only for cost efficiency, but also security," said Leblanc, former commander of the Canadian Forces' Northern Area.

Diamond miners in Canada adhere to the Kimberley Process, a system implemented by the industry in 2003 to filter out blood **diamonds**, he added.

Leblanc said there was a significant influx of workers from countries such South Africa and Belgium after the first Canadian mine opened in 1998, but most employees in the industry are now Canadian.

He noted the RCMP, which has established a Diamond Protection Services unit, has been "proactive" in monitoring for smugglers.

The diamond industry isn't the only northern business that has raised concerns among the Mounties. According to separate documents obtained by Canwest News Service, the RCMP is worried the Mackenzie Valley pipeline project could put a strain on policing activities in the region.

"From a contract policing perspective, the immediate and long-term social impacts of the Mackenzie Gas Project will include increased community crime, family disruption, violence and substance abuse," states an RCMP update prepared in November 2007.

"From a federal perspective, the greatly increased risk of organized criminal activity, including high-level drug trafficking, economic crime, immigration issues, Arctic sovereignty challenges and potential terrorist activity are all believed to be areas of concern," the update said.

Document MTLG000020080905e4950004c

Police allege blood diamonds found hidden in clothing of man at Edmonton airport

BY GLENN KAUTH
CP
425 words
20 February 2008
23:39
The Canadian Press
CPR
English

EDMONTON _ RCMP say a huge seizure of illegal **diamonds** unfolded recently at the Edmonton International airport after suspicious border agents pulled aside a man whose trip originated in Africa.

The man arrived Feb. 11 from central Africa via London. As he made his way through customs, a search of his clothes turned up 180 carats of rough **diamonds** as well as several hundred carats of gems _ including rubies and sapphires _ and more than 40 grams of raw gold.

The man could face charges under Canada's Export and Import of Rough **Diamonds** Act, a law intended to stop the trade in blood **diamonds** that for years financed rebel groups fighting civil wars in African countries such as Sierra Leone.

``Every time this happens, it sends a message to the crooks,'' said Ian Smillie, a research co-ordinator with Ottawa-based Partnership Africa Canada, which is involved in the fight against conflict **diamonds**.

But whether the latest seizure is related to African rebel groups is unclear. Many of the gem-fuelled conflicts in parts of Africa have wound down in recent years, with the Ivory Coast still known to produce blood **diamonds**.

``These could be just stolen **diamonds**,'' said Smillie.

Neither the RCMP nor the Canada Border Services Agency would say which African country the man was travelling from.

Police note, however, that the smuggling of **diamonds** between countries is often used to support criminal activity. When the gems get to Canada, bad guys try to **launder** them into the legitimate jewelry market, according to the RCMP.

In this case, the **diamonds** were all rough, meaning they would have little value to a retailer or a consumer until they were cut.

But while Smillie noted it would be hard to find a cutter willing to touch smuggled **diamonds**, he said whoever had them may have been planning to try to mix them up with a supply of legal Canadian **diamonds**.

As a result, they would have an easier time getting them certified under what's called the Kimberley process, an international system adopted to clamp down on the trade of blood **diamonds**.

Alternately, Smillie said, the smuggling operation may have simply been an effort to import the gems without paying taxes or duties.

Police, meanwhile, are still trying to put a value on the Edmonton seizure.

RCMP Cpl, Wayne Oakes said that while the catch was a large one, the gems themselves were mostly low quality.

(Edmonton Sun)

20080220CPCPG9615

Document CPR0000020080221e42l000dz

Search Summary

DOW JONES

NATIONAL POST

Financial Post
Ex-Madoff programmers wanted payment in diamonds; Jury told

Bloomberg News
268 words
11 December 2013
National Post
FINP
National
FP8
English

Bernard Madoff's former computer programmers asked for payment in **diamonds** to continue aiding the con man's US$17-billion Ponzi scheme in 2006 after they became uncomfortable with their role, a jury was told.

The "crazy" request from Jerome O'Hara and George Perez was turned down and the men were given salary increases and bonuses, Frank DiPascali, Madoff's former finance chief, testified Tuesday in Manhattan federal court in the trial of the men and three other ex-colleagues.

"Where the hell am I gonna get a bag of **diamonds**?" said DiPascali, who pleaded guilty in the case and is testifying in a bid for a lighter sentence. The programmers, who said they were "in a bit of a pickle," agreed on a "fairly substantial percentage increase" to their salaries, he said.

DiPascali is the highestranking former Madoff executive to testify in the first criminal trial stemming from the con man's scheme. The five former employees are accused of aiding Madoff for decades and getting rich along the way before the **fraud** collapsed at the peak of the financial crisis in 2008.

Mr. O'Hara and Mr. Perez, who have both pleaded not guilty, are accused of writing computer programs to trick regulators and customers by printing out millions of fake statements and trade confirmations. No trading took place.

The programmers' request for a payoff came about two weeks after the men arranged a meeting in Madoff 's office in which they suggested he close his investment advisory business, DiPascali said.

Document FINP000020131211e9cb0005c

THE VANCOUVER SUN

In Brief
Canada & World
Military fraud probe uncovers jewelry stash

Vancouver Sun
99 words
5 October 2013
Vancouver Sun
VNCS
Final
B4
English

Russia's Investigative Committee has confiscated 57,000 **diamonds** and 19 kilograms of jewelry from a former defence ministry official in an ongoing investigation into corruption charges. Committee spokesman Vladimir Markin said Friday that the jewelry, worth more than $3.9 million, was discovered at the home of Yevgenia Vasilyeva and "returned to the state." Vasilyeva was charged in 2012 with **fraud** related to the sale of military assets, then said to be worth about $11 million, but estimate the total damage at about $93 million.

Document VNCS000020131005e9a500012

TORONTO STAR

BX
Portus founder ordered to pay $320K; Mendelson also slapped with ban from trading

Madhavi Acharya-Tom Yew Toronto Star
302 words
1 December 2012
The Toronto Star
TOR
ONT
S17
English

The province's stock market watchdog has permanently banned Michael Mendelson from trading stocks and becoming an officer or director of a public company for his role in the collapse of hedge fund Portus Alternative Asset Management. The Ontario Securities Commission also reprimanded Mendelson and ordered him to pay back $320,000, money that he insists he doesn't have.

"I'm just glad it's over," Mendelson said Friday, after the OSC released its decision on sanctions.

According to the order, handed down by commissioner Edward Kerwin, Mendelson is permanently prohibited from holding any securities, with the exception of mutual funds in his Registered Retirement Savings Plan.

Mendelson and his partner Boaz Manor started Portus in 2003. With referrals from huge companies such as Manulife Financial Corp., the company attracted 26,000 clients and $800 million in assets.

The fund collapsed in 2005 after regulators stepped in and froze its assets amid concerns about record-keeping and investment suitability.

Portus went into receivership after Manor fled to Israel and used investor funds to buy $8.8 million worth of **diamonds**, which have never been recovered.

Manor pleaded guilty to criminal charges and is currently serving a four-year jail sentence.

Mendelson pleaded guilty to one count of **fraud** and was sentenced to two years in jail. He served six months. He started his own company, called Mikael Meir Inc., and is now a self-employed consultant who specializes in business ethics.

In January and March of 2005, just before and after the OSC began investigating Portus, Mendelson "authorized payments to himself" of $320,000, according to documents filed in the proceedings.

He told the commission that he is a changed man.

Document TOR0000020121201e8c10003u

NATIONAL POST

Financial Post
Portus's Manor must pay $8.8M; Doesn't have it

Barbara Shecter
Financial Post
641 words
28 August 2012
National Post
FINP
National
FP1 / Front
English

TORONTO . Canada's largest capitat-markets regulator attempted to send a strong message of deterrence by permanently banning Boaz Manor, the man at the centre of collapsed hedge fund Portus Alternative Asset Management Inc., from most capitalmarkets activity and ordering him to disgorge $8.8-million.

But with Mr. Manor's lawyer acknowledging after Monday's settlement with the Ontario Securities Commission that his client doesn't have the money, the impact of that message may be muted.

Mr. Manor attended but did not speak at the OSC settlement hearing Monday, where he was also formally reprimanded.

He is on day parole from a four-year jail sentence imposed last year in connection with the Portus collapse.

"This has been a very stressful time for Mr. Manor. He is absolutely relieved to put this behind him and move on with his life," his lawyer, Robin McKechney, told OSC commissioner James Turner.

The disgorgement order, part of the settlement agreement negotiated with OSC staff, relates to Mr. Manor's purchase of **diamonds** with Portus money.

But his lawyer said Monday Mr. Manor has neither the **diamonds** nor the money to pay.

Mr. McKechney said his client began proceedings in Israel against a party he believed had the **diamonds**.

That action, the lawyer said, was taken over by the receiver in the Portus case. "Mr. Manor is not in possession of the **diamonds** nor does he know their whereabouts at this time," the lawyer said.

Asked if his client has the money to pay the millions of dollars in the disgorgement order, Mr. McKechney replied, "He does not at this time."

The OSC settlement with Mr. Manor, along with two others reached with players in the Portus saga Monday, is the culmination of an investigation launched in 2004. The following year, regulators froze the fund manager's operations amid a flurry of allegations about offshore accounts, **diamonds** and missing investor money.

As part of the OSC settlement, Mr. Manor, 38, has been banned permanently from trading securities and can purchase them only in mutual funds or exchange-traded funds for his retirement savings plan through a registered dealer.

He is also permanently banned from becoming a director or officer of any company, investment firm or fund manager in Ontario.

At its height, Portus had $730-million under management and 26,000 clients, most of them in Ontario.

Portus investors got back most of their money, but Mr. Manor left for Israel as the company fell apart. He returned in 2007, the same year he and Portus co-founder Michael Mendelson were charged criminally by the RCMP.

Mr. Mendelson pleaded guilty to a single count of **fraud** and served the mandated portion of a two-year sentence before his release in 2008.

Mr. Manor went to jail in May last year to serve the mandated portion of a four-year sentence after pleading guilty to breach of trust and disobeying a court order.

On Monday, his lawyer said the "most important" thing to Mr. Manor is that, despite the scandal, most of the money was returned to investors who did not suffer fallout from the market turbulence of 2008.

The OSC has not resolved its issues with Mr. Mendelson, who, upon his release from jail, launched a consulting business under a new name, Mikael Meir. In March, he spoke at an event at the Centre of Excellence in Responsible Business at the Schulich School of Business.

The OSC's administrative hearings into the Portus affair were put on hold in 2006 to deal with the criminal court proceedings and resumed last year.

bshecter@nationalpost.com

Darren Calabrese, National Post / Portus co-founder Boaz Manor arrives for a hearing at the Ontario Securities Commission in Toronto Monday.;

Document FINP000020120828e88s0002f

THE GLOBE AND MAIL*

Report on Business Magazine

CHASING MANOR'S MILLIONS; Seven years after the spectacular collapse of his firm Portus, the mystery persists: What became of the diamonds that Boaz Manor bought with investors' money?

BRUCE LIVESEY
5,093 words
26 October 2012
The Globe and Mail
GLOB
50
English

John Finnigan's first question for Boaz Manor was a formality. Pen poised, Finnigan asked for Manor's address.

Manor stared at the ceiling.

A silence hung in the air of the law firm's boardroom. Finally, in exasperation, Finnigan demanded: “When you left the house this morning, what was the number on the door?”

The lawyer had good reason to be frustrated. He had fought a long, draining battle in Israel's courts to force Manor to answer his questions. It was February, 2006, and Finnigan, a commercial litigator with the Toronto law firm Thornton Grout Finnigan LLP, was in Tel Aviv attempting to extract information from the 33-year-old Manor.

Finnigan wanted to know about the whereabouts of tens of millions of dollars that had gone missing after the collapse of Portus Alternative Asset Management Inc., a Bay Street firm that had operated one of Canada's largest hedge funds. Manor was the investment brains behind Portus, which had been shut down by the Ontario Securities Commission (OSC) in 2005 amid allegations of **fraud**. Finnigan had been retained by KPMG Inc., the court-appointed receiver, to help it find the money that couldn't be accounted for.

But the young financier was proving to be an elusive quarry – not only because he had bolted Canada for Israel but also because his answers were unhelpful and elliptical. At one point, Finnigan asked Manor about the identity of a man in Milan, Italy, to whom Manor had given $3 million of Portus funds. Manor didn't seem to know a thing about him.

“How old was he?” Finnigan asked.

“I'm hazy on that part,” replied Manor.

“You can't describe him?”

“I'm hazy on it. I don't want to guess.”

At another point, after Finnigan told Manor that his version of events “sounds made up,” Manor conceded: “I know that a lot of things that I'm saying are fantastic in nature. Going to Italy, going to Zurich – there's **diamonds**, there's hundreds of millions of dollars. If you lump it all together, it's sort of a fantastic story.”

By early 2005, when the OSC discovered irregularities at Portus and shut it down, the hedge fund had raised $800 million from some 26,000 retail investors. Despite the OSC's imposition of a cease-trading order, Manor went rogue, attempting to move tens of millions of dollars in investor savings to Europe.

The upshot of his efforts was that $17.6 million (U.S.) of investors' cash was never recovered, of which as much as $12 million (U.S.) could still be under Manor's control. In total, as much as $130 million was fraudulently diverted by the Portus brain trust, although investors managed to get their original investment back because most of the money had been invested in principal-protected notes held by a French bank, Société Générale SA. By the time they'd matured, the notes' appreciation covered the losses.

This June, Manor was released from prison after serving a little over a year of a four-year sentence, mostly in a residential-style minimum-security facility. Soon after his release, the OSC slapped Manor with a lifetime ban on

trading securities and sitting on the board of a public company, and with an order to disgorge $8.8 million. But the OSC is effectively accepting Manor's claim that he can't pay.

Manor may be a free man, but numerous questions hang over his head, especially about where all of that money ended up and whether his punishment fit the crime. “His sentence is a reinforcement that crime pays in Canada. It's totally inadequate. I'd do 16 months in a provincial or federal penitentiary if I could pocket millions of dollars,” says Bill Majcher, a former RCMP investigator who specialized in financial **fraud**. “I know the investors were very disappointed with the length of the sentence,” says Finnigan. Were he one of them, he says, “It would give me some heartburn that Manor was walking away with a smirk on his face feeling, ‘They came after me with everything they got and I'm now going to live a very luxurious and happy life from this point on.' That would gall me.”

Manor is not inclined to chat about the missing cash. But his lawyer is. Brian Greenspan is among Canada's top defence lawyers, famous for a bravura style of angry exhortation mixed with avuncular charm that he has wielded effectively for clients such as hockey agent Alan Eagleson, Livent co-founder Myron Gottlieb and investment banker Andrew Rankin. Although Manor pleaded guilty to breach of trust and disobeying a court order, that's as far as he'll go: He claims he doesn't have access to the $8.8 million worth of **diamonds** that he acknowledged in an affidavit he bought with investors' money. And although his sole partner was convicted of **fraud**, Greenspan insists Manor is not a master fraudster with a fortune squirrelled away somewhere. “Bo is adamant that he would defend any allegation that he intentionally diverted money to the detriment of investors and defrauded anyone,” says Greenspan. “He's a strong-willed, stubborn, smart guy who still believes, had he been given the opportunity, he would have vindicated his plan and would've provided investors with significant return on their money.”

The author of the Portus debacle was born in Israel, where his father, Daniel, developed defence systems for the Israeli military before moving his family to Canada in 1988. In Toronto, Daniel founded EIS Electronic Integrated Systems Inc., which manufactures traffic-monitoring equipment. The younger Manor had a classic Toronto Jewish upbringing, growing up in Forest Hill and attending Forest Hill Collegiate Institute. His yearbook photo for 1992, his graduating year, sported this oddly prescient and creatively spelled caption: “Into the future I see an array of precious jems, dimonds, and rubies glowing with effervesent light…and a guy named Louie yelling ‘Put the jems in the yellow bag, the **diamonds** in the green bag, and get a move on it before we get busted.'”

Manor went on to attend the University of Toronto and completed a degree in applied science, graduating in 1996. But business was his calling. After working briefly for his father's firm, Manor met entrepreneur Michael Mendelson, who was running a small merchant bank, KBL Capital. Mendelson gave Manor some work, and soon they were fast friends, united by a desire to become spectacularly rich.

After KBL Capital took a hit when the dot-com bubble burst in 2001-'02, Manor and Mendelson looked around for a new line of business and settled on hedge funds. They devised an investment plan that was brilliantly simple: They told investors that all of their money was going to be plowed into principal-protected notes issued by a large bank – in this case, the French giant Société Générale. The bank then promised the notes would be linked to returns of a basket of hedge funds.

Normally, retail investors are not allowed to invest in hedge funds; they're too risky. But this structure provided a workaround. The upshot was that, after five years, investors would be guaranteed to get at least their principal back, plus whatever was made by being linked to the hedge funds. “You're selling zero downside,” explains Mendelson. “And your upside is, you're tied to a sexy asset class.” The duo's dream was to build an investment management firm that would grow to $5 billion in assets, sell it off and pocket $250 million apiece.

They opened Portus in January, 2003, with Mendelson acting as the operations guy and Manor the investment guru. Things took off when they managed to land a referral arrangement with a group of securities dealers, including a branch of Manulife Financial Corp., one of the most solid names in the financial industry. This meant hundreds of brokers across the country were steering their retail clients to Portus. It was like striking oil, with hundreds of millions coming through the door every quarter at one point. Eventually employing 120 people, Portus leased offices on the 24th floor of BCE Place at the foot of Bay Street, with a stunning view of Lake Ontario. It was a cocky, young workplace that “reeked of arrogance,” recalls one former Portus salesman. “People wanted to work for us because we were the shit.” Hours were long, expectations high. Vacations were frowned on.

In the office, Manor was introverted and private. “Boaz was often in his office with the door closed,” says the former employee. “He was the strong, silent type. He was paranoid.” Nevertheless, Manor was the face of Portus in marketing material and on a ghostwritten book, A Guide to Alternative Investing.

Despite appearances of success, Portus had a design flaw. Its managed account agreement said Portus would be entitled to an annual management fee ranging from 1.9% to 2.25% of the market value of assets in an investor's account. But Mendelson and Manor felt this was not enough money to grow the business as fast as they wanted. In particular, they needed a lot of cash to persuade financial planners to steer clients to Portus.

Their solution, as it turned out, was illegal. Although the firm's managed account agreement explicitly said Portus was required “to invest all assets which the investor contributes,” in reality only 86 cents of every dollar was invested in the principal-protected notes. The remaining 14 cents went to meeting Portus's payroll and expanding the business by paying fees to brokers. “That was the **fraud**,” says Joel Vale, a Toronto lawyer involved in a lawsuit against Portus's auditors, PricewaterhouseCoopers LLP, after the hedge fund crashed.

Mendelson claims it was not this straightforward: He says Portus received a huge discount from Société Générale, which Portus then used, through a complex manoeuvre, to pay for operating expenses. And Portus received a thumbs-up from its lawyers that it was perfectly legal. What no one disputes is that none of this was disclosed to investors, as it should have been.

In the spring of 2004, Manor and Mendelson went to one of Bay Street's top securities lawyers, Joe Groia, and asked him to conduct due diligence on Portus. Groia was singularly unimpressed with Manor and his investment theories. “He just gives us gobbledygook,” he remembers. Groia quickly discovered that Portus was using investors' money without proper disclosure and told Manor and Mendelson that unless they ceased this practice, they could be facing dire consequences. “And they basically said, ‘Thank you very much but you're fired,’” says Groia. After receiving Groia's warnings, Portus would go on to raise another $400 million from investors.

“They disagreed with [Groia],” says Greenspan with a shrug. “[Manor] thought he was doing things in accordance with other advice he received. It's about accepting the opinion you like to hear. They had another opinion they chose to follow.”

Mendelson claims that after receiving Groia's advice, he told Manor to fix this fundamental problem. “And he didn't do it,” he says.

The end for Portus came when another provincial securities regulator triggered an OSC compliance review in January, 2005. The following month, the commission issued a cease-trading order. At that juncture, Mendelson thought they could iron out their differences with the regulators and be back in business. He was convinced Portus wasn't engaged in **fraud**. “I felt we could get out of it,” he maintains. “I thought this was a disclosure issue. That it was civil, it was not a career killer, it's not an ‘I am going to prison' thing.”

Manor's subsequent actions made any simple resolutions all but impossible. According to court documents, two weeks after Portus was shut down, on the evening of Feb. 16, 2005, and into the following day, Manor oversaw the deletion of the fund's electronic files and e-mail accounts, and the reformatting of servers and hard drives of 60 desktops and 30 laptops. He collected all backup tapes and duplicate electronic copies of records. Voluminous paper files were also removed or destroyed, and a laptop containing vital data disappeared. “I came in the next morning and people were freaking out,” says Mendelson. “It was a disaster zone.” KPMG says Manor even hired temporary employees to forge backdated documents that showed investors' money had been invested, when it had not.

Two weeks later, after KPMG was appointed as the receiver, it sent accountants to Portus's offices to examine the books. “It looked like a whirlwind had gone through the offices,” says one KPMG accountant. “We soon find out records have been deleted and the computer system had been trashed.” KPMG had to bring in forensic IT experts, who attempted to reconstitute files.

Today, Greenspan vehemently denies that Manor destroyed records, although he concedes “I am not saying [Manor] made it easy for anybody or made them accessible to them.” He insists records were later returned. But KPMG says many of the records Manor removed were never recovered.

Court documents indicate that just prior to the OSC opening its investigation into Portus, Manor and Mendelson spent millions of investor dollars on themselves, friends and family. Mendelson authorized payments to himself over and above his salary totalling $320,000 prior to and after the start of the OSC investigation. Manor paid himself, friends and family nearly $2.4 million. The two claim they were repaying people who'd loaned them start-up funds for Portus.

Up to this time, Manor and Mendelson had paid themselves relatively modestly. Over all, they were each making about $100,000 a year. “They were not spending the money on the usual toys, like big houses or cars,” says Finnigan, who was hired by KPMG soon after the receiver was appointed.

KPMG's most stunning discovery was that during its two years in operation, Portus had spent $110 million of investors' money just to keep the fund running – money investors were led to believe was being invested. Of this sum, $41 million had gone to financial planners; some of this money was then used to pay redemptions to clients, but the larger part went to the advisers themselves for recommending Portus to their clients. In an agreed statement of fact, the Ontario Crown, which alleged that **fraud** had been committed, says Portus "misappropriated" this money. But neither of the Portus founders were truly held to account by the Crown on this allegation.

When KPMG approached Mendelson to help sort out Portus's complex financial structure, he co-operated. Manor, on the other hand, refused. In March, 2005, the receiver obtained court approval to interview him. A few days later, Manor's lawyer told KPMG his client had left the country. "It was either the day of or day after the Canadian court makes the order that his lawyer says, 'Uh oh, he's not here,'" recalls Finnigan.

Greenspan says he doesn't know why Manor chose that moment to leave Canada. And initially, neither did KPMG. Manor flew to France and Switzerland before heading on to Israel. A few weeks later, KPMG received a phone call from a Swiss banker that shed light on Manor's sudden departure.

He said his name was Jean-Pierre Regli, and he was an investment adviser based in Lugano, Switzerland. His trade involved managing the assets of wealthy people and navigating the murky waters of private and offshore banking. Regli told KPMG he had been working for Manor since the previous year, setting up a bank account for him at the Banca di Roma in Italy and helping him move funds around. For instance, in the summer of 2004, $2.5 million (U.S.) of Portus investors' money was deposited into that Italian account. "[Manor] said the funds belonged to him," says Regli. "He claimed it was commission he took from investors up front." (None of this money was ever recovered.)

But what Regli said next really made Finnigan sit up and take notice. He said Manor had contacted him since he had left Canada, asking whether Regli could help him transfer between $34 million and $40 million (U.S.) from offshore bank accounts to Europe, apparently with the intention of investing the money. This, too, was Portus cash that KPMG and Finnigan had never heard about.

Regli contacted KPMG because he'd heard about the OSC investigation. Initially, Manor told Regli he wanted to use the money to buy a house in Italy and invest the rest in a Swiss bank. "And then after a few weeks, there was a new story popping up," recalls Regli. "He wanted all of the money in cash and no real estate and no Swiss bank account."

Thanks to Regli's tip, KPMG and Finnigan learned that in 2003, of the $800 million Manor and Mendelson had raised, about $53 million (U.S.) of it – derived from 900 investors – was supposed to be invested offshore. To that end, Manor had hired veteran Montreal lawyer Anthony Malcolm to set up a series of offshore trusts and companies. Malcolm later admitted he spent more than $1 million of Portus funds to make secret and unrecorded payments to bankers and board nominees in the Cayman Islands and Turks and Caicos to get the Portus companies and accounts off the ground. (Despite famously loose regulation in those jurisdictions, such payments are illegal.) Yet KPMG discovered that none of the $53 million (U.S.) had been invested; the money was languishing in the offshore accounts. Says Finnigan: "It's pretty clear there was no legitimate purpose to sending money offshore, and someone was trying to hide it and keep it from investors' reach."

Today Greenspan says that after Portus was shut down, Manor received legal advice confirming his opinion that the $53 million (U.S.) was not affected by the OSC's cease-trading order because the cash was offshore and therefore outside the commission's jurisdiction. "Bo thought the OSC had been precipitous," explains Greenspan. "I think Bo's position is that when he goes [abroad], he's trying to salvage things and make sure that the offshore money is invested." Whatever his intentions, once KPMG was appointed receiver, no Portus money was to be touched without its permission – no matter where it was.

Having learned about the offshore holdings, KPMG and Finnigan were soon unearthing a crazy quilt of offshore entities that Manor had set up over the previous two years – a total of 130 Portus accounts in 10 different countries.

They also learned that Regli was not the only proxy Manor had used to move money around. There was also Nigel Freeman, a debonair Cambridge-educated Brit who lives in Bermuda and acts as a private banker. KPMG concluded that Manor dictated instructions to Freeman through Anthony Malcolm, the lawyer in Montreal.

In 2004, Freeman had opened an account in his own name at the Credit Suisse bank in Zurich – which, to KPMG, became known as the Freeman Account. He opened a safety deposit box in Zurich as well. Freeman later testified that this account and box were used to transfer money on behalf of Manor. The only other person who

had access to the box was John Dallas Campbell, a high school buddy of Manor's who acted as a "runner" – moving money in and out of the box.

In the end, KPMG and Finnigan succeeded in finding most – about $35 million (U.S.) – of the offshore money before Manor could move it. "We traced it through these various jurisdictions before we ended up at this account in the Turks and Caicos," recalls Finnigan. But of the original $53 million (U.S.), $17.6 million (U.S.) was still missing. Where had it all gone?

Malcolm, for one, had been paid $2.7 million (U.S.) for his services, it later became clear. Another $2.5 million (U.S.) had ended up in the Italian bank account Regli had helped set up; it also disappeared. (When finally confronted by Finnigan, Manor claimed he gave that money to the mysterious man in Milan whom he could not describe or name.) Then there was the money going in and out of the Freeman Account and safety deposit box – about $1 million vanished this way.

In July, 2005, Manor provided KPMG with a list of payments made with investors' funds. One line indicated he'd spent $11.6 million (U.S.) on "Precious Metals – Precious Stones." KPMG figured out what had happened to this money when its accountants examined the Freeman Account at Credit Suisse and found that nearly $9 million (U.S.) had passed through it to banks in Hong Kong.

The "precious stones" turned out to be **diamonds** Manor had purchased. The celebrated gem is an ideal commodity for those who want to transfer wealth across borders without being traced: **Diamonds** are small, easily concealed and liquid – on the black market.

After Manor arrived in Israel, he had gone to a diamond broker and selected 100 **diamonds**, including a 22-carat stone worth $4.5 million (U.S.). The stones were then flown to Hong Kong, where they were paid for and picked up.

Why wouldn't Manor simply have paid and taken possession in Israel? Finnigan theorizes that Manor made the transaction in Hong Kong to make it more difficult for the receiver to track down the assets.

Indeed, the **diamonds** remain shrouded in mystery, although the identity of the players is known. Manor's sister-in-law, Jieying Yu, is the founder of a Hong Kong company, Bringood Investments. According to court documents, Manor had Yu pick up the stones from the Israeli diamond broker's Hong Kong office in the summer of 2005. They then were given to a man named Yitzchak Toib.

Manor had met Toib in Israel through family connections. Manor paid Toib as much as $900,000 in Portus money to fly to Hong Kong and collect the gems. Toib stored them in a safety deposit box in the city. Toib later claimed he returned to China and gave the **diamonds** back to Yu, on Manor's orders. She denies receiving them this second time.

The **diamonds** have never been found. Manor insists Toib has the stones; he launched a lawsuit against Toib, but has allowed it to go dormant. Others believe Manor has the stones himself. "I think Manor did it and he knows where they are and is keeping them for a new day," says Israeli lawyer David Tadmor, who worked for KPMG on the Manor case.

The lawyers involved say it's irrelevant where the **diamonds** are: Manor used investor money to make the purchase. "He basically embezzled the funds and took millions of dollars and bought other things for himself," says Tadmor. "Whether Toib can produce the **diamonds** or not doesn't really matter. It's Manor who stole the money and bought the **diamonds**."

Soon after Manor arrived in Israel in the summer of 2005, KPMG obtained a court order preventing him from leaving that country. Manor responded by taking $700,000 (U.S.) of investors' funds and giving it to Yehuda Weinstein, one of Israel's top criminal lawyers and today its attorney-general (most of this money was eventually frozen after Weinstein was informed of its origins). For months, Weinstein told Finnigan that Manor was too ill to be interviewed. At one point, Weinstein arranged to have a psychiatrist interview Manor; the psychiatrist said the young man, suffering from depression and suicidal thoughts, "cried like a little boy." Manor's medical issues aside, his lawyer, Brian Greenspan, blames KPMG and Finnigan's "very aggressive position" as the reason why Manor was unwilling to co-operate.

After months of delay, Manor was finally forced by an Israeli judge to answer Finnigan's questions. In February, 2006, the lawyer and a pair of KPMG accountants examined Manor in Tel Aviv. Manor's answers were a surprise: He claimed that Anthony Malcolm, the elderly Montreal lawyer he'd hired to set up Portus's offshore companies, not only controlled Portus but that he, Manor, was a mere employee of Malcolm's.

KPMG couldn't find one shred of evidence substantiating this claim. When Finnigan presented Manor with OSC documents showing his signature on the corporate filings that established Portus, Manor shrugged them off. Mendelson agrees that Malcolm did not control Portus, while Nick Mancini, who was briefly CEO of Portus in 2004, said he'd never heard of Malcolm. “The ownership was around Boaz and Michael,” Mancini says. Malcolm himself denies he controlled Portus or instructed Manor to do anything. “I don't even want to talk about it, the son of a bitch,…” he said when contacted.

In the end, the examination provided no useful information on the whereabouts of the missing **diamonds** and other funds. Manor did, however, produce a recording he'd secretly made in the fall of 2005 of a conversation between himself and Yitzchak Toib. At one point, Manor accuses Toib of taking his money, and demands that his “assets” be returned. Toib's answers are rambling and often incoherent, although he does say, “If you are willing to be patient and get out of the mess and so you can get your money, okay, you can get it. You have no patience – do what you want. Be my guest, I'm not cross…we're through.” The word “**diamonds**” is never uttered in the conversation, but Greenspan holds up this tape as evidence that Toib has the gems. “Toib is a liar,” he says.

In 2007, the RCMP laid 18 charges against Manor. That fall, after his lawyers had negotiated the terms of his return, Manor flew back to Canada, where he was arrested, released on $250,000 bail and ordered to live with his parents.

That same year, Mendelson, who'd co-operated with the RCMP and prosecutors, pleaded guilty to one charge of **fraud** and accepted a two-year sentence. While he could have fought the charges, he wanted to move on with his life and put the whole Portus episode behind him. He ended up spending six months behind bars. “I went through this spiritual transformation,” says Mendelson. “I'm raising three daughters. I can't teach them the importance of being truthful if I'm scheming and trying to figure out how to get out of this. I'm clearly implicated in all this stuff that [Manor's] doing, even though I didn't have a hand in it. I just wanted to make a new life.”

Manor, in contrast, refused to accept any blame for the Portus **fraud** or admit he'd stolen any money. After four years of negotiations and delays, Manor finally pleaded guilty to one count of breach of trust and another for disobeying a court order. Today, the Ontario Attorney-General's office refuses to discuss why the Crown prosecutor, John Pearson, cut this deal. Scott Hutchison, a well-regarded former Crown lawyer and now a Toronto criminal lawyer, observes that “four years is a pretty modest sentence for a breach of trust in the millions.”

What softened the blow was that investors got all of their original money back because most of it had been invested in principal-protected notes. Although an estimated $110 million of investors' cash had been fraudulently siphoned off, by the time the notes matured a few years later, the interest earned made up for the lost money.

But a full accounting of the mess that Manor and Mendelson made puts many more millions on the loss side of the ledger. KPMG's work cost $13.7 million – which investors ended up paying, since their assets had been recovered. Lawsuits were launched against Société Générale and Portus's auditors, PricewaterhouseCoopers; thus the case not only damaged the companies' reputations but racked up hundreds of thousands in legal bills. And more costs were accrued to deal with the OSC charges that were settled this past August.

Then there are the losses that investors suffered because their cash was never fully invested in the first place. “It's a misleading story to say there's no loss,” says one of the KPMG accountants who worked on the case. “If investors got back 100 cents on the dollar, they would've been just as well off to put that money under a mattress for three years.” Nor does it take into consideration the hardship borne by investors wondering for up to four years if they would ever see their money again. “Nobody knows how many people had strokes, heart attacks, sleepless nights waiting for years to see if they would get their money back,” says attorney Joel Vale, who was involved in a post-Portus lawsuit.

Mendelson now views his Portus experience with a mixture of regret and defiance, believing he never set out to defraud anyone. Working out of a small office in a holistic-health business complex in east-end Toronto, Mendelson operates a leadership development training agency under a new name. On a recent sunny morning, the 46-year-old sat Buddha-style in his chair, and reluctantly revisited how the two partners ended up in prison – an ordeal that almost cost Mendelson his marriage, and deep-sixed his high-flying career in finance.

“There was major greed there,” Mendelson says. “We wanted to be considered successful in the eyes of other people. It's what young ambitious guys do on Bay Street.” Since leaving prison, Mendelson has revised his life goals. “My values were misplaced,” he says. “What was important to me back then was money, prestige and success on society's terms…I have now shifted from being ego-based and self-grasping, to practising living a life of service, using my skills and talents to help others achieve their goals.”

How does he feel about Manor? “So much of my work today is around forgiveness. If you hold on to that kind of stuff, it just eats away at you….He's got his karma. Whatever he has done and whatever he's doing, I feel he will pay for in his life.”

Document GLOB000020121026e8aq0000g

Portus' Manor Bought 22-Carat Diamond With Fund Investments

By Joe Schneider - October 14, 2005 13:22 EDT

Oct. 14 (Bloomberg) -- Boaz Manor, co-founder of a Canadian hedge fund that collapsed in February, spent $7.5 million of investors' money on diamonds, including a $4.5 mil ion, 22-carat stone that investigators are trying to find in China, according to the accounting firm that's probing the fund.

Manor's sister-in-law Yu Jieying acquired about 100 diamonds, including the 22-carat gem, in three separate transactions in Hong Kong at the end of June and beginning of July, Robert Rusko, a vice president of KPMG LLP, told reporters after a court hearing in Toronto today.

The 22-carat diamond is ``extremely portable and extremely valuable,'' Rusko said. ``Whoever arranged this transaction didn't want to take delivery in Israel.''

Portus, founded by Manor and Michael Mendelson three years ago, became one of the fastest-growing hedge funds in Canada. The fund's customers had invested more than C$750 million ($632 million), with companies including Manulife Financial Corp., referring their clients to the fund. Manulife refunded its clients their investments and is the fund's biggest creditor now.

Manor left Canada for Israel after the Ontario Securities Commission began investigating transactions at Portus in February.

KPMG LLP, an accounting firm appointed by an Ontario court to trace money invested in Portus, has recovered all but $17.6 million, which was moved to banks in the Caribbean.

Manor has refused to speak with KPMG's investigators. His Israeli lawyer, Yehuda Weinstein, has said in letters to KPMG that Manor is too sick to be interviewed. He could not be reached for comment today.

Tracking Down Yu

KPMG will ask an Israeli judge at a hearing scheduled for Nov. 7 to order Manor to submit to questioning in the country.

As KPMG investigators traced money movements from the Caribbean to Europe, Manor arranged further transfers including sending more than $10 million to MID (HK), a Hong Kong company

specializing in gems.

It was through MID (HK) that Manor arranged the purchase of the diamonds, KPMG's lawyer John Finnigan said.

KPMG is also working with Chinese police in trying to track down Manor's sister-in-law, Yu, Finnigan said. She failed to show up for an interview after a Hong Kong court ordered her to, he said.

``We're hopeful she will be found," Finnigan told an Ontario judge overseeing the investigation.

The case is Ontario Securities Commission v. Portus Alternative Asset Management, 05-CL-5792, Ontario Superior Court (Toronto).

NATIONAL POST

Financial Post
UBS Snitch gets US$104M payoff; U.S. tax-scam reward contrasts with Canada

John Greenwood
Financial Post With Files From Barbara Shecter
927 words
12 September 2012
National Post
FINP
National
FP1 / Front
English

Brad Birkenfeld, the man who blew the whistle on a massive tax-evasion scam that cost the U.S. government billions in lost revenue, has been awarded US$104-million by the U.S. Internal Revenue Service.

The massive payout is understood to be the largest such reward to an individual ever made. It highlights the stark difference between the United States, where even criminal whistleblowers can become fantastically wealthy for selling out their company's shady tax practices, and Canada, where critics complain there is zero incentive to point out wrongdoing.

As an executive at Swiss banking giant UBS AG in Zurich in 2007, Birkenfeld approached the IRS and the information he provided served as the basis for a landmark court case that saw UBS pay a US$780-million settlement and turn over details on thousands of U.S. holders of offshore accounts.

Birkenfeld, now 47, also revealed details of the bank's operations in Canada.

Evidence presented before a U.S. Senate subcommittee that was looking into the matter included information about a major offshore business in this country run out of UBS's offices in Switzerland, managing more than $5-billion of Canadian assets at one point.

Officials in Ottawa vowed to crack down when the information was reported but so far no Canadian holders of UBS offshore accounts have been successfully prosecuted.

"People realized that it's a question of time before we get them," Jean-Pierre Blackburn, then the minister of revenue, told the Financial Post in 2009. "I tell them, we'll get you, we'll find you."

Despite his efforts to secure immunity in the United States, Birkenfeld was himself caught up in the legal wrangling around UBS and was sentenced to 40 months in prison for conspiracy to defraud the U.S. government. (He was released on Aug 1.)

According to court documents, UBS bankers in the U.S. trolled art shows, yacht races and other high-end events in search of potential clients who were looking for ways to avoid paying income tax. As a senior member of the bank's wealth management team, Birkenfeld had a ring-side seat and also took part, at one point helping a client to stuff **diamonds** into a toothpaste tube to avoid airport security.

Under U.S. law, such practices are illegal and Birkenfeld reportedly became uncomfortable with what UBS was doing and complained to senior officials at the bank. Birkenfeld claims that it was only when his concerns were ignored that he went to the IRS.

In a statement on Tuesday the U.S. tax authority praised Birkenfeld's evidence, calling it "comprehensive" and "exceptional in both its breadth and depth. While the IRS was aware of tax compliance issues related to secret bank accounts in Switzerland and elsewhere, the information provided by the whistleblower formed the basis for unprecedented actions against UBS."

Offshore banks in Switzerland and other tax haven jurisdictions had largely avoided the gaze of tax authorities in countries such as the United States and Canada, but that changed in the wake of a series of scandals involving former employees going public with incriminating information and computerized client files.

One of the first tipsters was Heinrich Kieber, a former computer technician at LGT Bank in Liechtenstein, who sold details about account holders to Britain, France and Germany among others. Thanks to Mr. Kieber, the CRA came into possession of details of more than 100 Canadian clients of LGT bank.

The CRA subsequently obtained similar lists of offshore account holders UBS and HSBC.

Because of its efforts to chase after Canadian tax evaders and the publicity around the matter, the CRA says it has collected tens of millions of income tax that it would otherwise not have received.

But critics say it would collect a lot more if took a more aggressive approach, perhaps prosecuting tax evaders in court. Another strategy employed in the United States but not in this country is encouraging whistleblowers to come forward by offering financial rewards - as much as 30% of the tax collected as a result of the information provided.

Indeed, critics frequently complain that far from being rewarded, whistleblowers are more likely to be punished in Canada.

Howard Wetston, chair of the Ontario Securities Com-mission, raised the possibility of creating a whistleblower program in the securities industry shortly after taking top job at Canada's largest capital markets regulator in November of 2010. But nearly two years later no such program exists.

Al Rosen, founder of forensic accounting firm Al Rosen & Associates, said the failure of the CRA to aggressively pursue tax dodgers is part of a much larger problem.

"There is no investigation, no prosecution to speak of in Canada," he said.

Whether it's the tax authority, financial or securities regulators, there is no will to ensure that players follow the rules.

Mr. Rosen said he recently reported a case of tax **fraud** to the CRA "but quite likely they won't even pursue it... [far from giving out rewards for information] they don't even follow up when you give it to them for free."

jgreenwood@nationalpost.com

Bradley C. Bower, Bloomberg News Files / Former UBS AG banker Bradley Birkenfeld speaks during a 2009 interview at Schuylkill County Federal Correctional Institution in Minersville, Pa. Birkenfeld, who was released Aug. 1, was praised by the U.S. Internal Revenue Service.;

Document FINP000020120912e89c0002q

THE VANCOUVER SUN

David Baines
BusinessBC
Lax securities rules at root of $50-million Freedom Investment Club calamity

David Baines
Vancouver Sun
1,022 words
7 March 2012
Vancouver Sun
VNCS
Final
C2
English

Honestly, I don't know how B.C. Finance Minister Kevin Falcon can continue to ignore the carnage that the B.C. Securities Com-mission enables promoters to wreak on investors. Talk about fiddling while Rome burns.

The problem, as I have pointed out so many times before, is centred on provisions in the B.C. Securities Act that permit unlicensed, uneducated and often unethical people to sell risky and illiquid securities to B.C. residents. It is a recipe for disaster.

These disasters occur with mind-numbing regularity - causing immense financial damage, destroying retirement plans, ruining marriages, and infusing their victims with bitterness and distrust.

The B.C. government is ultimately responsible for what's in the Securities Act, but in most cases it acts on the advice and recommendations of the commission. To date, the commission has not recommended any substantive changes to the rules and the government has not intervened. In my view, they are equally culpable.

The latest exempt-market fiasco to hit the news is the Freedom Investment Club. On Monday, BCSC enforcement staff issued a notice of hearing alleging that the two key promoters, Michael Lathigee and Earle Pasquill, committed **fraud** by raising $21.7 million from 698 investors with-out telling them that the club was on the verge of insolvency.

This is a familiar pattern: BCSC officials, with government acquiescence, open the door for promoters to flog dodgy securities to mom-and-pop investors, then call on their enforcement people to clean up the inevitable mess.

FIC is a classic example. In December 2002, I reported that Lathigee and Pasquill were promoting the club at financial motivational speaker T. Harv Eker's so-called Millionaire School.

At that point, the club had about 200 members who had invested just over $600,000. Lathigee and Pasquill - who are not licensed to sell or advise in securities - invested the money in sketchy deals such as payroll loans, coloured **diamonds** and junior stocks. The business grew rapidly through marketing seminars and word-of-mouth referrals. By mid-2007, it had grown to 2,500 members and $10 mil-lion in assets.

BCSC enforcement staff were clearly worried about this gathering storm. They intervened on several occasions and at one point ordered FIC to offer investor refunds.

"If I was an investor, I would take my money and run," I wrote in July 2007. But very few investors did so. Most were incapable of properly analyzing financial risk and reward. And by that time, the club had become a kind of cult, with many people investing on faith rather than reason.

By March 2008, the club had grown to 5,000 members and $100 million in assets, mostly Alberta development properties. I noted that the properties were highly levered and the market was softening. "A drop in value could be devastating for shareholders," I reported, which was simply stating the obvious.

In August 2008, I reiterated the structural problem: "FIC looks and acts like a conventional mutual fund, but it has none of the usual consumer safeguards. Neither the fund nor its principals are registered with the securities commission, and they operate outside the purview of the Mutual Fund Dealers Association."

THE WINDSOR STAR

News
Ponzi loot on auction; Millions in Rotschild scam

Mcclatchy Newspapers
316 words
14 July 2011
Windsor Star
WINSTR
Final
D7
English

The Rothstein collection of ill-gotten bling - world-class watches, diamond-encrusted jewelry - was auctioned off, piece by glittering piece, at a brisk pace Wednesday.

It was the second large-scale selloff of Ponzi schemer Scott Rothstein's material possessions. It got under way at 9: 30 a.m. at the Broward County Convention Center, where several hundred people came to bid, or just observe, and lasted till 3 p.m., with just a five-minute bathroom break.

An auction last year of Rothstein's yachts and exotic supercars brought in $5.8 million for victims of his $1.4 billion investment **fraud**, the largest ever in Florida. Some of the more exquisite jewelry pieces on sale Wednesday brought in tens of thousands of dollars. A white gold Piaget sold for $77,500. A men's diamond ring quickly went for $64,000. A yellow gold Patek Philippe watch sold for $61,000.

Also going under the auctioneer's gavel: a collection of stylish lighters used by Rothstein to fire up his premium cigars, two late-model Corvettes and a 2009 Mercedes SL550 sports coupe.

As Rothstein was grabbing tens of millions of dollars from his investor-victims, he spent their money lavishly on jewelry.

For his wife Kim, the now disbarred Fort Lauderdale lawyer bought **diamonds**, rubies, sapphires and pearls by the multi-carat-load, with mounts in platinum, gold and silver.

For himself, he stockpiled diamond rings, flashy cufflinks and more than 200 of the world's most prized watches - crafted by the likes of Rolex, Franck Muller, Gerald Genta, Richard Mille, Patek Philippe and Piaget.

Rothstein, 48, is serving a 50year sentence in federal prison, but prosecutors recently filed notice that they intend to ask a judge to reduce his punishment because he is co-operating in the investigation.

Document WINSTR0020110714e77e0003i

THE GLOBE AND MAIL*

ON THE COAST
British Columbia News: Column

Persian rugs, biker bling, other loot for sale; Police recovered property auction displays what people have lost, not including their sense of security

STEPHEN QUINN
930 words
30 April 2011
The Globe and Mail
GLOB
S3
English

I've always approached the Vancouver Police Recovered Goods and Bicycle Auction with some degree of amusement. Among the bikes, electronics and jewellery, there are always a few odd items. Last year there were seven mascot costumes, including one adult-sized white rabbit get-up.

This year was different for me. I wasn't just there as a journalist.

The auction preview held earlier this week is always a draw for the TV cameras. It's an easy story with good pictures.

Show me the most expensive item, the weirdest item, the one with the best story. The thing someone might miss the most but never went to police to ask about. Or the item that couldn't be reported stolen for one reason or another.

This time around there are 40 machine-woven Persian rugs. Now before you go admiring the work ethic of the particular thief who hauled away hundreds of pounds of bulky woven wool, Ian Wightman, who manages the police department's stolen property room, says they are the leftovers of a police **fraud** investigation.

What's big this year? The hottest of hot items? Well, gold. With the precious metal up over $1,500 per ounce, it has been a favourite of thieves. Gold chains with jewelled crosses, and **diamonds** set around an open-mouthed Ghost Rider skull. Bulky stuff. Some of the chains so thick they look like strings of nuggets. Biker bling to be sure. There are also watches, diamond solitaire rings, cocktail rings, rubies and other gems, some with price tags as high as $10,000. All of it once belonged to someone. All of it remains unclaimed. It will be sold off to the highest bidder.

There's even a kitchen sink. A stainless steel double sink, likely lifted from a construction site, Mr. Wightman suggests. (I wonder if it wasn't just put there so auction organizers could say with authenticity: "… everything and the kitchen sink.")

This year, though, was different for me because I was looking for my own stuff. Specifically the three laptop computers, two iPods, a professional audio recorder, video camera, digital still camera, equipment bag, two purses with their contents and my wife's wallet that were all taken when our house was broken into just over a year ago.

Here's what I learned from our robbery, and from Mr. Wightman this week:

Lesson No. 1: Don't hang car-key fobs or purses near the front door.

The thieves not only got all that loot, but drove away with it in our car – along with our child seats, a stroller and various other kid-related paraphernalia (blankets, beach toys) – thanks to how easy it was to find our keys. It also meant we had to call in an emergency locksmith on a Sunday to change our locks. The car we got back a few weeks after it was stolen. It had been parked a few minutes drive from our house.

Lesson No. 2: If you have an alarm system, set it, even when you are home.

We were home. Two adults and three small children sleeping upstairs.

They came in through a kitchen window, tiptoed over the plush toys and a carpet mined with Lego, and grabbed what could be easily fenced. They left the front door open.

Lesson No. 3: Engrave your driver's licence number on everything.

Ian Wightman says it's the easiest way for police to contact you if they've recovered something that is yours. And save your proof of purchase. If you see something at the auction that once belonged to you, it will be pulled from the lot and returned if you can prove it is yours.

Walking through the tables piled with bagged and tagged property this year, I thought less about the dollar value of the merchandise and more about what it might have meant to people.

The bags of jewellery and coin collections dumped out of dresser drawers.

The tools that represented someone's livelihood, including a new set of chef knives wrapped in a case marked with the logo of the cooking school the owner was attending. “Most likely stolen from a car,” Ian Wightman guesses aloud. The cameras and iPods that once contained photos or carefully curated music collections. The electric guitars, and a student's clarinet. A walker. A wheelchair.

Then there are the bicycles. Ask anyone who has ever had his bike stolen how he felt about it and you'll know the racks containing more than 400 stolen bicycles represent a lot of misery, disappointment and anger. Not to mention bus rides.

I look past all the expensive mountain bikes and all I can see are the children's bikes, some with baskets and bells.

My stuff wasn't there. Police no longer resell laptop computers because they can't be certain the hard drives have been wiped completely clean. The physical items we lost were replaced but their contents are gone: the photos and videos that were never downloaded, the skeletal writing projects and wedding speeches held on the personal laptop. We'll never get those back.

Our sense of feeling completely secure in our house? That's gone too.

Stephen Quinn is the host of On the Coast on CBC Radio One, 690 AM and 88.1 FM in Vancouver.
stephen.quinn@cbc.ca

Document GLOB000020110430e74u0001f

THE GLOBE AND MAIL*

Business

Lacroix sentenced to 13 years; Former Norbourg head given time for his role in a $130-million fraud that claimed 9,200 victims

287 words
9 October 2009
The Globe and Mail (Breaking News)
GMBN
English

Montreal --

Financier Vincent Lacroix has been sentenced to 13 years in prison for his role in a $130-million **fraud** that claimed 9,200 victims.

Mr. Lacroix - the former head of Norbourg Asset Management Inc. - was handed the sentence in Quebec Superior Court Friday morning. Last month, he pleaded guilty to 200 charges after years of protesting his innocence.

The Crown had asked for a sentence of up to 14 years, while Mr. Lacroix's defence had suggested between 10 and 12 years.

Mr. Lacroix has already served part of a prison term on a 2007 penal conviction for securities violations.

He and several Norbourg associates masterminded one of the biggest **fraud** and embezzlement schemes in Canadian history.

The associates also face criminal charges.

After Montreal-based Norbourg was shut down in 2005, the evidence that came to light included allegations that investors' money was diverted into money-laundering schemes such as real estate investments, the purchase of small financial firms as well as **diamonds** and sapphires.

There were false bookkeeping entries and falsified documents, according to the charges.

Norbourg's main line of business was selling mutual funds.

Many of the victims were modest investors who lost their life savings as a result of the financial scandal.

The lengthy criminal investigation included members of the RCMP's white-collar crime unit, the Integrated Market Enforcement Team.

Mr. Lacroix's 13-year sentence is believed to be the most severe yet in Canada for financial crimes. He will not be eligible for early release until the end of 2011.

Globe and Mail Update

Document GMBN000020120625e5a9004d8

Sentencing hearing delayed for Man., addictions centre head who defrauded Ottawa

BY MIKE MCINTYRE
CP
556 words
12 December 2008
19:08
The Canadian Press
CPR
English

WINNIPEG _ The former head of a Manitoba addictions treatment centre has delayed his sentencing hearing by requesting a review of whether his aboriginal background should earn him leniency from the justice system.

Perry Fontaine has admitted to being the architect of an elaborate **fraud** scheme that robbed the federal government of several million dollars.

The Crown is seeking a three-year prison sentence, while Fontaine has asked for two years behind bars.

He will also be forced to pay a restitution order of $2.36 million, which is the amount he personally received through the scam.

His case was halted Friday when Justice Perry Schulman agreed to order a report on a Supreme Court of Canada mandate that some aboriginal offenders be given lesser sentences based on their troubled upbringing and an overrepresentation of aboriginals in custody.

The report won't be completed until the new year.

Fontaine's case has been adjourned until at least February. He remains free on bail.

Fontaine, 55, helped set up two phoney consulting firms that skimmed millions of dollars in program payments from Health Canada to the Virginia Fontaine Addictions Foundation, court was told.

Fontaine pleaded guilty in September to charges of **fraud** and bribing a public official.

He engineered the **fraud** with two senior federal government employees: Paul Cochrane, an assistant deputy minister of health; and Patrick Nottingham, the former regional director of Health Canada in Manitoba. They pleaded guilty in the fall of 2005.

In exchange for testifying against Fontaine, Cochrane was given a one-year sentence and ordered to make $211,000 in restitution. Nottingham, who also agreed to testify against Fontaine, was given a conditional sentence of two years less a day and ordered to pay $1.14 million in restitution.

Charges against the men's wives were dropped as part of the plea.

Crown attorney Dale Harvey said Fontaine had convinced Cochrane and Nottingham to increase funding to the treatment centre over the course of several years.

In exchange, Fontaine diverted centre funds to two consulting firms _ one controlled by Nottingham and his wife, and another controlled by Fontaine.

The centre paid the consulting firms on the pretext of providing services to the centre. But in reality, the firms provided work of no value, Harvey said.

Harvey said that between 1991 and 2000, the centre received $97.5 million in funding from Ottawa and part of those funds were diverted to pay for luxury vehicles, homes, NHL hockey tickets and vacations for the three men and their families.

The scheme began to unravel with a 2000 newspaper report of a Caribbean cruise taken by Fontaine and 70 centre staff, along with Cochrane. That resulted in Health Canada ordering a forensic audit, which took three years to complete.

In addition to the criminal charges, the federal government is suing Fontaine to recover more than $800,000 he paid himself in vacation and retirement settlements after he quit the facility.

Luxury jewelry items seized from Fontaine's former condominium following his arrest in 2003 are to be auctioned off next month.

The items include rings, bracelets, earrings and necklaces made of gold and **diamonds**. One 14-karat gold diamond ring had an appraised value of $14,000.

(Winnipeg Free Press)

20081212CPCPG2390

Document CPR0000020081213e4cd00091

CALGARY HERALD

News
Ill-gotten jewelry goes to auction

Winnipeg Free Press
159 words
14 November 2008
Calgary Herald
CALH
Early
A11
English

WINNIPEG

The federal government will auction off tens of thousands of dollars in jewelry seized from the home of Perry Fontaine, former head of the scandal-ridden Virginia Fontaine Addictions Foundation, which delivered services to the Sagkeeng First Nation east of Lake Winnipeg.

Fontaine, the linchpin in an elaborate **fraud** and bribery scheme that brought down two senior Health Canada officials and saw six others also charged, pleaded guilty in September to defrauding taxpayers. He is to be sentenced in December, with the Crown seeking a three-year prison term.

The jewelry to be auctioned off in Winnipeg in January was seized by RCMP when they executed a search warrant at Fontaine's condominium in 2003. The items, valued at more than $148,000, include rings, bracelets, earrings and necklaces made of gold and **diamonds**. One 14-karat gold diamond ring alone has an appraised value of $14,000.

Document CALH000020081114e4be0000v

Search Summary

Text	diamonds and fraud
Date	01/01/2008 to 18/03/2014
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	All Languages

Diamond Exports Face New Threat

by Hebert Zharare
611 words
16 June 2010
03:02
All Africa
AFNWS
English

Harare, Jun 16, 2010 (The Herald/All Africa Global Media via COMTEX) -- THE plot to criminalise Zimbabwe's diamond sector thickened this week with a Canadian-based organisation, Partnership Africa Canada, imploring the Kimberley Process Certification Scheme to redefine the term "blood **diamonds**" so that it covers gems mined in Chiadzwa.

The lobby comes ahead of a key intercessory meeting of the KP in Tel Aviv, Israel, next week where Zimbabwe will present its case and how it has been unfairly treated.

The Government will also outline how the continued denial of KP certification is slowing down economic transformation.

Mines and Mining Development Minister Obert Mpofu yesterday dismissed the PAC report, pointing out that Zimbabwe had complied with all KP requirements.

The KPCS regulates international trade in **diamonds**.

Minister Mpofu said: "We are a principled country. These people (PAC) have employed some locals to demonise their country. They are working against the people of Zimbabwe.

"We are going to deal with those peddling falsehoods to international organisations legally. These people are very lucky that they are in Zimbabwe.

"In some of these Western countries you cannot peddle State secrets to hostile organisations and get away with it," he said.

In its June report titled "**Diamonds** and Clubs: The Militarised Control of **Diamonds** and Power in Zimbabwe", PAC claims Government-sponsored smuggling of **diamonds** and human rights violations in Chiadzwa.

"Blood **diamonds** are **diamonds** involved in murder, mutilation, rape or forced servitude. PAC endorses this definition and calls on the KP to adopt it at the earliest possible opportunity," part of the report reads.

The Canadian organisation said the KP's definition of conflict **diamonds** failed to encapsulate Zimbabwe.

"(The) definition is outdated and needs changing. It erroneously assumes all governments are legitimate and does not recognise that such governments in whole or part could engage in acts of **terror** or criminality as egregious as any rebel movement."

PAC said the KP had lost direction and credibility.

Irish Aid, Foreign Affairs and International Trade Canada, the International Research Centre among others funded the compilation of the 32-page report.

KP monitor for Zimbabwe Mr Abbey Chikane of South Africa recently adjudged the country to be in compliance with their minimum requirements.

Government in May banned the export of all **diamonds** until Chiadzwa **diamonds** got KP certification.

Apart from Mbada Holdings and Canadile Miners, who are exploiting the Chiadzwa resource, Murowa **Diamonds** and River Ranch are also into mining of the gemstones elsewhere in Zimbabwe.

Minister Mpofu yesterday said: "When Mr Chikane came here for the first time, he produced a report against us and we never complained.

"This time we have complied with the requirements and we are going by that. We will not listen to anyone."

PAC said Mr Chikane "sold out" Farai Maguwu - an NGO worker facing criminal charges in the courts for peddling confidential State information -- by alerting police to what he was up to.

However, Minister Mpofu responded: "Let the law take its course. If we interfere and order his release, they are the same people who will also complain."

PAC, in its report, recommended that the KP suspend Zimbabwe immediately and that mining licences given to Mbada and Canadile be revoked.

"The United Nations Security Council should place an immediate embargo on Zimbabwean **diamonds** until such a time as there is legitimate and competent governance of the country's diamond resources."

The attempt to use the UN Security Council to push Western agendas in Zimbabwe is not new and last year one such effort was thwarted by Russia, China, South Africa and other progressive members of the international community.

Document AFNWS00020100616e66g0008h

TORONTO STAR

Greater Toronto

Crime syndicate exposed: Police 'They themselves believe they're untouchable' Unsolved killings; A dozen alleged members of deadly Shower Posse among 78 people nabbed in 1000-officer sweep

Rosie DiManno Columnist

With files from Jesse McLean, Jennifer Yang and Henry Stancu
1,610 words
5 May 2010
The Toronto Star
TOR
ONT
GT1
English

"I ran it like a CEO of a Fortune 500 company. The only difference is that instead of litigating in a court of law, we held court in the streets."

Vivian Blake, the late co-founder of the Jamaican Shower Posse

Legions of cops turning over the rocks of two gun and drug street gangs in Toronto found slime traces of a notoriously lethal international crime syndicate underneath.

Project Corral - unleashed in the early-morning hours Tuesday as more than 1,000 officers fanned out across the GTA, Ottawa, Sault Ste. Marie and Windsor - nailed a dozen alleged members of the deadly Shower Posse among the nearly 80 people arrested by late afternoon.

The suspected Shower Posse contingent is being portrayed as the cream of the criminal crew crop, an über institution of importers and wholesalers criminally superior to the street-level clot represented by the two gangs that had been specifically targeted: the well-known-to-police Falstaff Crips and Five Point Generalz.

Project Corral has emerged as a rare infiltration of a sophisticated criminal operation that has long managed to keep its fingerprints off narcotic trafficking and gun violence on Toronto's streets, in large part by staying above the bloody neighbourhood level fray contested by their client gangs, police say. They'll supply everybody, police say, and let the bullets fall where they may.

"Over the past several months, this investigation has focused not only on the gunmen and the drug traffickers, but the source of those drugs and those firearms," Toronto Police Chief Bill Blair told a news conference where the arrests and seizures were revealed.

"We always believed there was a criminal organization, even a criminal intelligence, that was operating behind many of the activities of the street gangs. This investigation has given us an opportunity to identify some of those individuals, to apprehend them and to compromise their ability to continue to supply drugs and firearms into these communities."

The alleged Shower Posse members have evolved from their roots in the "garrisons" of the poorest ghettoes in Kingston, Jamaica, where they spent decades fighting for turf with archrivals, most especially the Spanglers Posse. Both groups had deep ties to Jamaica's two main political parties; were indeed born out of allegiances to politicians who provided them with protection from prosecution in return for turning out the vote.

While it was speculated as far back as 15 years ago that the Shower Posse had secured a foothold in Toronto, they're barely mentioned in the annals of local crime as reflected in arrests and prosecutions. Internationally, however, they have a massive profile and feared reputation, believed responsible for more than 1,400 murders in the United States.

American law enforcement officials have been trying without success for the past year to extradite Christopher Coke, believed to be the current Shower Posse boss in the Jamaican capital. Vivian Blake, co-found of the posse

with Coke's father (who died in a prison cell fire on the day he was to be extradited to the U.S.), passed away in Jamaica in March from kidney failure and diabetes. He warranted a lengthy obituary in the New York Times.

Investigators in the joint-forces operation launched their nine-month project last August following a spike of violent incidents in Toronto's northwest region, apparently a spree of internecine bang-bang between the Cripps and the Generalz over drugs and territorial control. That conflict is blamed for two unsolved homicides.

"Over the course of this investigation, a more significant crime involvement was identified," said Blair. "We've identified an international organization which has tentacles into these street-level organizations and is supplying them with both drugs and guns, organizing and profiting from their criminal activities."

As part of the probe, and working with the Canada Border Services Agency, three Toronto residents were recently arrested in the Dominican Republic over 72 kilograms of seized cocaine. The drugs were allegedly bound for Toronto.

Staff Insp. Mike Earl, head of the guns and gangs task force that led Project Corral, said the Shower Posse was at the hierarchical apex, supplying drugs and weapons to local gangs for street-level purchases.

Shower Posse members don't necessarily look or behave like their client gangs, said Earl. "They're older members. They're not young kids. They're a well-organized Jamaican criminal organization" that's largely functioned off the police radar. "They're very sophisticated. They're very smart. But I can't tell you much more about them. It's not like they're going to be wearing colours or you're going to run into them on a day-to-day basis. They don't wear do-rags."

They also appear to be unafraid of law enforcement.

"I don't think they've been touched before. They themselves believe they're untouchable. We've finally made a step in the right direction," Earl said.

Project Corral, which was put into raid mode around 5 a.m. Tuesday, simultaneously executed 105 search warrants by officers from 19 organizations and 35 tactical squads. Three Toronto police stations were designated to process the arrests as many of the accused started routing through bail hearings at a Finch Ave. courthouse.

In Toronto neighbourhoods, some residents awoke to police banging on the door though others slept through the whole shebang.

"I was half asleep when I heard a loud bang and wondered what the heck it was," said Cindy Wood, who lives in an apartment above stores on John St., north of Lawrence Ave. W., in the Weston neighbourhood.

Tactical officers used a pry bar to break open the street-level door to the staircase leading to the second floor units, where police had a suspect named in a search warrant.

"They came and knocked down two doors - one on the second floor and one on a higher floor," said Mike, property manager of a highrise on Martha Eaton Way, near Trethewey and Black Creek Drs.

As of 3 p.m. Tuesday, police had made 78 arrests, including females discovered as found-ins.

Blair admitted that communities might feel traumatized by the raids but argued that police have an obligation to "disrupt and dismantle" gang operations that cause ordinary people to live in **terror**.

Police claim their seizure of guns, drugs and cash will cripple the activities of the Cripps and Generalz. Among the material seized: 10 firearms, $30,000 in cash, $10,500 in casino cheques, **diamonds**, cocaine, crack cocaine, marijuana, hashish oil, more than 10,000 ecstasy pills, body armour and vehicles.

Charges laid run the gamut from trafficking in firearms and drugs, possession of prohibited firearms with ammunition, robbery, committing a criminal offence in association with a criminal group and living on the avails of prostitution.

One of the Canadians charged in the Dominican had allegedly been a major player in the Jamestown Cripps a few years ago. The three Toronto residents were identified by Dominican authorities as Oliver A. Willis, David George Daniel Parker and Mauro Giuseppe. The 69 packages of cocaine had been hidden in the bed of a pickup truck.

But at least equal in significance to the drugs and guns seized in Toronto was the small inroad police have made into the mysteries of the Shower Posse - so named, allegedly, because of the tendency of their gunmen to spray victims (often innocent bystanders as well) in a "shower" of bullets.

The posse hadn't been heard from hereabouts since the early '90s. It's unclear if they went away and came back or just dug down deeper.

"Unfortunately, I don't think any of the more traditional crime groups do go away," said Toronto police Supt. Greg Getty. "Sometime they may be crippled, sometime they may change and morph into a different entity."

The Shower Posse, said Getty, was known to have offshore resource links. "In our experience, the higher level organized crime groups all across the country or across the GTA are not out on the street committing random acts of violence, so the insulation factor around them makes them much difficult for law enforcement to focus on.

"There was a crack in the armour and investigators were able to exploit that successfully."

Project Corral has unearthed information on two unsolved homicides.

In December 2009, 19-year-old Aeon Grant and three friends were shot in the 15th-floor stairwell of 30 Falstaff Ave. Grant was hit in the head and died.

Elaine Sawyers, Grant's grandmother, said she was relieved to hear the police may have new leads to find her grandson's killer.

The other case is eerily similar: On Feb. 8, 2010, Tyrell Duffus was gunned down in a stairwell of 20 Falstaff Ave., just minutes away from where Grant was killed.

Duffus had been returning home to his apartment around 6:30 p.m. The 22-year-old lay there for four hours before a neighbour found his body.

His family said he had spent time in and out of jail but wasn't involved in anything gang-related.

With files from Jesse McLean, Jennifer Yang and Henry Stancu

A member of the police emergency task force on Parkway Forest Dr. Canadians David Parker, left, Mauro Giuseppe and Oliver Willis sit in a Dominican court in March after police seized 72 kilograms of cocaine.

Manny Rodrigues photo Eduardo Munoz/Reuters

Document TOR0000020100505e65500021

Former official with US consulate in Toronto sentenced to 1 year in visa bribery scheme

BY NEDRA PICKLER
CP
744 words
29 July 2009
19:20
The Canadian Press
CPR
English

WASHINGTON _ A former official at the U.S. consulate in Toronto was sentenced to a year in prison Wednesday for expediting visas in exchange for gifts of jewelry and trips with exotic dancers.

Mike O'Keefe admitted he expedited 21 visas for employees of STS Jewels between 2004-2006 and in return got the presents from the chief executive officer, Sunil Agrawal. The pair, who still call each other friends, were sentenced together in Washington by U.S. District Judge Paul L. Friedman.

Agrawal, a 50-year-old native of India who lives in New York City, got probation and a $100,000 fine, which prosecutors said was one of the largest ever imposed by the Washington court for the misdemeanour charge of illegal supplementation of salary. Agrawal told the judge he wasn't aware that giving the gifts to O'Keefe created a conflict of interest.

O'Keefe, a 62-year-old who now lives in Portsmouth, New Hampshire, was sentenced to the felony charge of accepting an illegal gratuity. He must return four rings and a necklace made of gold, rubies, **diamonds** and tanzanite he received for himself and his wife. He also must pay $5,000 to compensate for trips to New York with two exotic dancers and Las Vegas with three strippers from Toronto's Brass Rail Tavern, where he was a regular customer.

``I took gifts of jewelry and essentially cashed in my career," O'Keefe told the judge, explaining he was unhappy at work and being treated for depression at the time of the crime. ``I knew these were inappropriate gifts and I never should have accepted them. To this day, I don't know why."

O'Keefe did not mention his relationship with the dancers. But O'Keefe's attorney, Bernard Grimm, said his client is medically unable to have sex.

O'Keefe's wife Ann tearfully asked the judge to be lenient on her husband, saying he's a good man and the crime was small compared to his 40 years of public service. Besides more than 20 years as foreign service officer, he served in the U.S. Air Force, six years as a Democratic member of the New Hampshire State House in the 1970s and most recently as a professor at Southern New Hampshire University. Grimm said O'Keefe was fired by the school the day he pleaded guilty in the case in February.

Friedman told O'Keefe he recognized his public service and did not think he would commit another crime. But the judge said he was sentencing him to prison to send a message that bribery will not be tolerated among government workers.

At the time of the crime, O'Keefe was deputy non-immigrant visa chief at the U.S. consulate in Toronto, the last stop in a long State Department career that took him to posts across Latin America and Africa.

He met Agrawal in 2002 when he went to a gem fair in Tuscon, Ariz., and delivered speech about a government investigation that found tanzanite, a gem mined in Tanzania that represented a large part of STS Jewels' business, was not being sold to finance terrorist operations.

The next year O'Keefe was posted in Toronto and began to personally handle STS's application for Indian national employees to enter the United States on a fast track. Since the **terror** attacks of 2001, the United States has tightened controls over non-immigrant visas like those granted to students, tourists and workers.

According to email cited in court documents, O'Keefe wrote to Agrawal that he was growing tired of the visa arguments and frustrated with younger subordinates who were ``determined to find problems" and reject STS

applications. He overturned their rejections, even when a subordinate noted that terrorists use jewelry to raise money.

He also hinted about gifts he would like to receive, asking whether Agrawal could help him find a necklace to give his wife for Christmas in one email and in another recalling a conversation they had about making a trip to Las Vegas.

``For some reason I really love Las Vegas," O'Keefe wrote. ``I guess it is because it is a place where I can lose my stiff diplomatic persona and just act like everyone else. Let me know if we can work anything out."

20090729CPCPW5271

Document CPR0000020090730e57t000an

NATIONAL POST

Canada
Guilty plea in crime ring stung by lost luggage; Bank robbery proceeds used to finance terror

Mike McIntyre
Winnipeg Free Press
542 words
8 March 2008
National Post
FINP
National
A6
English

WINNIPEG - They duped banks out of millions of dollars, held police at bay for years and used their electronic wizardry on victims around the globe.

Yet the Canadian-based Blanchard Criminal Organization nearly came unglued, thanks to the most unlikely of foes: the airline industry.

A piece of luggage containing a King's ransom--$50,000 cash, some **diamonds** and a few hundred stolen credit cards -- somehow got lost when one of the accused was attempting to fly from Egypt to Africa.

The missing suitcase has never been found, a Winnipeg court heard yesterday.

The owner, Balume Kashongwe, pleaded guilty to fraud and participating in a criminal organization in one of the most sophisticated operations uncovered by Canadian police.

Kashongwe, 35, was sentenced to two years of time already spent in custody. He was set to be released from jail yesterday and plans to resume living in British Columbia, where a job in the forestry sector apparently awaits.

Kashongwe admitted he helped the leader of the criminal network, Gerald Blanchard, steal an estimated $250,000 from several banks in Cairo in late 2006.

The money was then funnelled to a mysterious Lon-don-based man called "The Boss" and used to finance terrorism in the Middle East, court heard.

Blanchard, Kashongwe and four others spent 10 days in Egypt and used data from 633 stolen credit cards to access various bank accounts. The group wore burkas to avoid detection from surveillance cameras.

Kashongwe was supposed to leave Cairo and go to Africa to continue the thefts, but stunned Blanchard when he called to report his suitcase had gone missing.

The money and **diamonds** inside were destined for the British boss, forcing Blanchard to pay the man out of his own pocket, court heard.

Provincial court Judge Kelly Moar told Kashongwe the fact his criminal actions indirectly helped terrorist activities is a major concern.

"When these attacks occur, innocent people die. That money being obtained by yourself and others was used to do that," Judge Moar said.

Blanchard, 35, pleaded guilty last November to 16 charges and was given an eight-year prison term.

He admitted he was the brains behind several sophisticated attacks on banks in Winnipeg, Edmonton and British Columbia, which netted his group millions of dollars.

Six co-accused remain before the courts. Blanchard, Kashongwe and other co-accused were not charged with any terrorism-related crimes.

Winnipeg police began investigating in 2004 after the theft of $510,000 from seven automatic banking machines inside a new CIBC branch.

They would later learn Blanchard and associates had secretly installed a pinhole camera and two listening devices -- including a baby monitor -- inside the walls and roof of the bank while it was still under construction.

The true "gem" of the investigation involved recovering the Koechert Pearl Diamond from Blanchard's grandmother's house in Winnipeg last year.

The historic jewel-encrusted brooch once belonged to Elisabeth, the Empress of Austria, during the 19th century. It was stolen from a castle in Vienna in 1998.

No one has been charged with the theft. Blanchard admitted to possession of stolen goods.

Document FINP000020080308e4380004f

Search Summary

Text	diamonds and terror
Date	01/01/2008 to 18/03/2014
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	All Languages
News Filters	Subject: Crime/Courts

Dubai refinery Kaloti, DMCC caught up in $5bn global gold scandal

ARTICLE VIDEOS

By Staff Writer Wednesday, 26 February 2014 11:52 AM

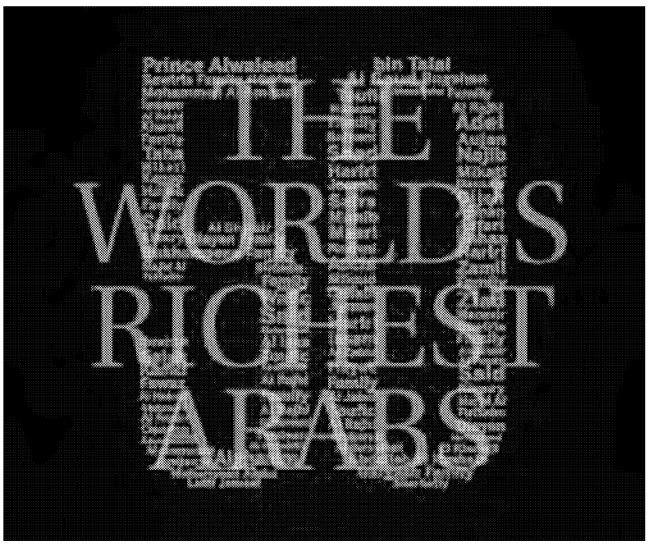
Ahmed Bin Sulayem, executive chairman of Dubai Multi-Commodities Centre (DMCC)

A Dubai-based gold refinery has been accused of flouting new international rules aimed at stopping trade in so-called conflict gold, amid claims it paid more than $5bn in cash for the precious metal and accepted gold from more than 1,000 customers without paperwork, London's *The Guardian* newspaper has reported.

Citing a confidential 2012 inspection report by Ernst & Young, the Kaloti Group, a $12bn refining and trading business which owns the largest refinery in the Middle East, is also accused of also taking millions of dollars of gold plated in another metal and seemingly smuggled out of Morocco.

It comes as it also reported that the Dubai Multi-Commodities Centre (DMCC), which was set up by Dubai ruler Sheikh Mohammed in 2002 to promote and regulate the gold industry and is headed by executive chairman Ahmed Bin Sulayem, changed its rules in a way which resulted in the the full details of the inspection reports being kept confidential.

The newspaper said the leaked E&Y report showed Kaloti paid out $5.2bn in cash-for-gold deals – equivalent to almost 45 percent of its business in 2012.



It also accepted 2.4 tonnes of gold in more than 1,000 transactions with customers who provided no paperwork and paid cash to Sudanese suppliers who had hand-carried gold to Dubai that was sourced from small-scale, artisan mining operations without checking for mining licences.

The Guardian said while there was no evidence that Kaloti accepted conflict gold, a term which refers to underground trade linked to African warlords and human rights abuses, major breaches in new gold trading guidelines were uncovered.

The new international rules, being championed by US President Barack Obama, the UN, EU and campaign groups, aim to stamp out illicit trade in conflict gold, with the UN pointing to growing evidence linking extortion at hundreds of mines in the Democratic Republic of Congo to armed groups involved in war crimes.

Quoting former E&Y partner-turned whistleblower Amjad Rihan, who was in charge of the inspection division, *The Guardian* report said DMCC had altered its reporting rules, with pressure put on E&Y over the report.

The report findings, published in December, are mentioned only briefly in a DMCC press release, which hailed the inspection outcome, saying Kaloti was compliant, certified and offered conflict-free gold.

"I am not a lawyer, but in my opinion, what is 'ethical' and what is

'legal' should not conflict," Rihan was quoted as saying.

"The DMCC, Ernst & Young and Kaloti were all aware that the risk of conflict gold entering Dubai had been very high. In my opinion the way they acted is appalling, amoral and extremely unethical."

Kaloti said in a statement to *The Guardian* that it "had shortcomings in the initial stages of the long, multi-staged audit process" but its "fully compliant final result was confirmed by Ernst & Young".

The DMCC rejected that it had sought to influence or interfere in the review process "or that it altered or softened the review process to favour any member refinery".

"All our findings have been made public and the review and reporting processes are robust," it was quoted as saying.

E&Y Dubai managing partner Joe Murphy reportedly said that it took the views of Rihan "very seriously" and undertook its own review of the report before it was issued.

The firm rejected it was under pressure to soften the findings.

At the time of going to press, Ernst & Young, the Kaloti Group and DMCC has not responded when contacted by *Arabian Business* to comment on the allegations made by *The Guardian* report

Dubai Refiner Kaloti Group Linked to Conflict Gold Scandal by E&Y Whistleblower

By M Rochan , Published: February 26, 2014 14:59 PM | Updated: February 28, 2014 09:47 AM

E&Y findings reveal Dubai gold refiner Kaloti Group bought conflict gold. Reuters

Dubai's Kaloti Group, one of the world's leading gold refineries, has ignored international rules about so-called "conflict gold" and is alleged to have purchased billions of dollars worth of the precious metal from unethical sources with no provenance, a whistleblower from Ernst & Young (E&Y) has stated.

Confidential papers shown to the Guardian, by Amjad Rihan, who was charged with inspecting Kaloti for E&Y, detail how, in 2012 the refinery group disregarded guidelines issued to halt the trade in suspect gold, which can be linked to African warlords and comes at a cost of atrocious human rights abuses.

Kaloti paid more than $5bn (£3bn, €3.6bn) in cash for the metal - equivalent to almost 45% of its business in 2012 - and accepted gold from over 1,000 customers who walked in off the street without any paperwork, according to

E&Y documents.

The Guardian report states that while there is no evidence that the refinery accepted conflict gold, major breaches in new guidelines were uncovered, raising concern about the history of huge volumes of shipments.

Details of the damning findings have not been spelled out in full in public documents, but have been uncovered in the Guardian's investigation. The leaked papers are also being reported by BBC2's Newsnight, al-Jazeera and the campaign group Global Witness.

A spokesman for Kaloti said: "We reject all allegations that we did not comply with the audit process or new regulations, and any suggestion that we have sourced gold from conflict zones is totally false. While we accept that we had some shortcomings in our initial report, these were quickly rectified to the full satisfaction of our external auditors and the regulators."

Kaloti is a $12bn refining and trading business based in Dubai. It owns the largest refinery in the Middle East and is at the centre of Dubai's gold industry, estimated to be worth $70bn in 2012.

Both Dubai rules and international standards set by the OECD maintain that the purpose of publishing reports, on the outcome of independent inspections, is to display transparency in relation to refineries' performance on responsible sourcing measures in order to "generate public confidence".

However, before the inspectors' work was finished and their reports filed, the Dubai authorities learned of E&Y's findings and changed their own rules to prevent the verdict from being publicised.

The Dubai Multi-Commodities Centre (DMCC) said rules were changed to keep them in line with similar international standards.

Covert Pressure

Emails showed how some at E&Y felt a regulator, "keen to promote the Dubai gold industry," had pressurised them, reported the Guardian.

“The DMCC, Ernst & Young and Kaloti were all aware that the risk of conflict gold entering Dubai had been very high.”

- Amjad Rihan of E&Y Dubai

That pressure compelled Amjad

Rihan, the man in charge of the inspection division, to break ranks and come forward as a whistleblower.

Rihan said he was horrified that Dubai authorities had changed their rules and that E&Y had signed off as "fair" public reports blocking out full details of Kaloti's failings.

"DMCC strongly refutes any allegation that it sought to influence or interfere with the review process, or that it altered or softened the review process to favour any member refinery," it said, adding: "All findings have been made public and the review and reporting processes are robust."

Rihan said: "I am not a lawyer, but in my opinion, what is 'ethical' and what is 'legal' should not conflict. The DMCC, Ernst & Young and Kaloti were all aware that the risk of conflict gold entering Dubai had been very high. In my opinion, the way they acted is appalling, amoral and extremely unethical."

International rules are in place to tackle the underground trade in blood gold, much of which is linked to African warlords and human rights abuses.

Earlier in the year, both Apple and Intel announced that all gold used in the circuitry of their phones, computers and other devices was conflict free.

Confidential papers raise fears over conflict gold

Papers show firm accepted gold from customers walking in off the street with no paperwork

Simon Bowers and **Juliette Garside**
The Guardian, Wednesday 26 February 2014

Hundreds of millions of dollars worth of suspect gold has poured into the global markets as major breaches occurred in new international rules designed to tackle an underground trade linked to African warlords and human rights abuses.

Confidential papers shown to the Guardian by a whistleblower detail how, in 2012, one of the world's biggest gold refineries ignored guidelines designed to stop the trade in so-called conflict gold.

It paid more than $5bn (£3bn) in cash for the metal and accepted gold from more than 1,000 customers who walked in off the street with no paperwork.

While there is no evidence that the refinery accepted conflict gold, major breaches in new guidelines were uncovered, raising concern about the history of huge volumes of shipments. Details of the damning findings have not been spelled out in full in public documents, but have been uncovered in a Guardian investigation. The leaked papers are also being reported by BBC2's Newsnight, al-Jazeera and the campaign group Global Witness.

Allegations that the full scandal has not been laid bare are a huge setback to international efforts – championed by Barack Obama, the UN, the EU and campaign groups – to stamp out the illicit trade in conflict gold by requiring the world's largest refineries to be independently audited to check that they are sourcing gold responsibly

and publishing the findings.

Full details of the findings are set out in confidential inspection reports from Ernst & Young, which was brought in to review the practices of the Kaloti Group, a $12bn refining and trading business based in Dubai. Kaloti owns the largest refinery in the Middle East and is at the centre of Dubai's booming gold industry, estimated to be worth $70bn in 2012. Documents show the group systematically flouted new rules on conflict gold.

The UN has been pushing for tough international guidelines covering the trade in gold and other "conflict minerals" because of mounting evidence linking extortion at hundreds of mines in the Democratic Republic of Congo to armed groups involved in war crimes.

The UN's largest peacekeeping force is deployed in the country, with more than 20,000 uniformed personnel. More than 5 million people are estimated to have died in the DRC or its neighbours in the last two decades, making it the most deadly conflict since the second world war.

All refiners around the world must be able to show they meet the new international standards, and have been independently inspected, if they want to continue trading with US multinationals from May this year. Guidelines recommend companies "make and receive payments for gold through official banking channels where they are reasonably available, avoid cash purchases where possible, and ensure that all unavoidable cash purchases are supported by verifiable documentation".

The rules of the Dubai Multi-Commodities Centre, set up by Dubai's ruler Sheikh Mohammed in 2002 to promote and regulate the gold industry, require refiners to make extra checks on suspicious, cash-in-hand deals above 40,000 dirhams (£6,540). Kaloti had no system in place to do this in 2012.

In fact Kaloti paid out $5.2bn in cash-for-gold deals – equivalent to almost 45% of its business in 2012. E&Y Dubai's inspectors also found the refinery group had:

• Taken millions of dollars of gold knowing it was plated in another metal and seemed to have been smuggled out of Morocco.

• Accepted 2.4 tonnes of gold in more than 1,000 transactions with customers who provided no paperwork.

• Paid cash to Sudanese suppliers who had hand-carried gold to Dubai – sourced from small-scale, artisan mining operations – but did not check whether they had approved

mining licences.

These details from E&Y inspections have never been disclosed before. In Kaloti's much-delayed compliance report, published last December, the failings are mentioned only briefly and in terms that do not leave the reader with a clear picture of the inspectors' findings. Kaloti maintains all failures in its procedures were rectified by November last year, with all but one of its remedial measures having been independently verified by E&Y. In a statement to the Guardian, it said: "Kaloti had shortcomings in the initial stages of the long multi-staged audit process ... Our fully compliant final result was confirmed by Ernst & Young."

Both Kaloti and E&Y stressed all shortcomings were properly reported and acknowledged in published reports. Other comparable reports from major refineries in Dubai and elsewhere also offer only very scant descriptions where inspectors have discovered failings, suggesting this may be emerging as common industry practice for these new reports.

The Guardian has seen no evidence that published reporting of Kaloti failings was out of line with regulatory rules or industry practice. But leaked emails show their proper presentation in published filings was hotly contested.

Both Dubai rules and international standards set by the OECD say that the purpose of publishing reports on the outcome of independent inspections is to demonstrate transparency in relation to refineries' performance on responsible sourcing measures in order to "generate public confidence". But before the inspectors' work was finished and their reports filed, the Dubai authorities learned of E&Y's findings and changed their own rule book in a way that meant that the overall verdict of inspectors would stay confidential.

The Dubia Multi-Commodities Centre insists these changes were made simply to keep rules in line with similar international standards. "DMCC strongly refutes any allegation that it sought to influence or interfere with the review process, or that it altered or softened the review process to favour any member refinery," it said, adding: "All findings have been made public and the review and reporting processes are robust."

Emails show how some at E&Y felt pressure had been put on them by a regulator "keen to promote the Dubai gold industry", pressure that led Amjad Rihan, the partner in charge of the inspection division, to break ranks and come forward as a whistleblower. Rihan said he was horrified that the Dubai authorities had altered the rules and that E&Y had signed off as "fair" public reports obscuring full details of Kaloti's failings.

So brief were eventual descriptions of the failings reports published last December that in press releases the DMCC and Kaloti made no mention of them, celebrating the inspection outcome and stressing Dubai's leading refinery had ended the audit fully compliant, certified as offering conflict-free, responsibly sourced gold.

Rihan said: "I am not a lawyer, but in my opinion, what is 'ethical' and what is 'legal' should not conflict. The DMCC, Ernst & Young and Kaloti were all aware that the risk of conflict gold entering Dubai had been very high. In my opinion, the way they acted is appalling, amoral and extremely unethical."

At one stage, so serious had E&Y's concerns about how to treat the Kaloti findings become that the case was referred to some of the firm's top global executives and legal experts in London. At one stage, Mark Otty, E&Y's managing partner for Europe, Middle East, India and Africa (EMEIA) based in London, said in an email: "Rest assured that we are taking this issue very seriously ... I have taken the lead in relation to our investigation of it." Otty said later that he was satisfied with the outcome because "both client and regulator will report deficiencies".

A spokesman for both E&Y divisions declined to answer questions from the Guardian. "This matter ... concerns work done by EY Dubai, in Dubai, for a Dubai-based client under guidelines promulgated by the DMCC, a Dubai regulatory body."

Joe Murphy, managing partner at E&Y Dubai, said: "EY Dubai took the views of our former partner [Rihan] very seriously and prior to issuing our ... report undertook a comprehensive review, including consulting with internal and external experts, who supported the actions we took. We firmly believe that by identifying elements of non-compliance we have played an important role in achieving improvements in the client's supply chain controls."

E&Y's global code of conduct says: We are robust and courageous in our challenge to clients and are not afraid to deliver unwelcome information to them ... We support people and will withdraw from working for any clients that put our people under undue pressure". Rihan does not feel that is what happened in Dubai "I went to senior figures at EY asking them to back me up in my professional opinion but instead I think they went to great lengths to please the client and they pushed me out."

EY deny this. "EY Dubai took the views of our former partner very seriously and prior to issuing our ... report undertook a comprehensive review; including consulting with internal and external experts, who supported the actions we took".

New international guidelines have emerged to tackle conflict gold, after similar to curb

the trade in blood diamonds.

According to a UN report at the end of 2011: "A significant proportion of gold financing armed groups and criminal networks [within the DRC military] continues to end up in the United Arab Emirates, making the due diligence of refiners, smelters and jewellers based in that country of particular importance."central Africa, unless from long-standing industrial suppliers or well-known global traders. Kaloti, the UN report said, insisted it "had not purchased artisanal gold from the region for three years."

Dubai is one of the world's global hubs and attracts business from all quarters. Last October the Responsible Jewellery Council, whose members include Cartier, Tiffany & Co, H Samuel, Ernest Jones and Argos, signed a deal recognising Dubai's conflict gold refinery inspection programme and permitting RJC jewellers to market gold bought from the emirate as conflict free.

In recent weeks both Apple and Intel have also announced that all gold used in the circuitry of their phones, computers and other devices is now conflict free.

Gold rush hits Calgary precious metals dealers

Wednesday, August 10, 2011

Hundreds of people stood outside the Bank of Nova Scotia to bet their savings on the precious metals market.

Among them were a 13-year-old Calgary Herald paper boy, an art gallery operator from Cochrane and Elaine Abercrombie, who was trading her retirement fund for silver bars.

"The dollar isn't going to be worth much," Abercrombie told the Herald after buying 150 ounces of silver.

The value, she said, "is going to go up again. It's an investment. Paper money isn't any good."

It was Jan. 4, 1980.

Within weeks, the precious metals market crashed.

Gold dropped hundreds of dollars, prompting lines of dejected buyers to return to the bank, sell their investment and eat their losses. By March, monopolies on the silver market had been broken. Within a few short years, the price of silver dropped to $5 an ounce from a high of about $50.

With hindsight, it was easy to see that gold and silver had been in a bubble - like Nortel stock and American homes, their value was artificially inflated by feverish demand.

In 1980, gold reached a peak of $850 per ounce. More than 30 years later, gold and silver are again breaking price ceilings.

Gold reached a record $1,800 per ounce on Wednesday. Likewise, silver is commanding rates of about $40 per ounce.

As they did in the '80s, those prices are prompting long lines at bullion exchanges.

Calgarians are sorting through buckets of old coins looking for pre-1967 silver quarters. They are wrapping their broken chains and orphan earrings in Ziploc bags and crumpled paper, hoping to cash in on the scrap hiding in the back of their jewelry boxes.

Even highbrow jewelry seller Birks has jumped in. For the past year, it has bought its customers' gold. The jeweller is holding several consultations in Calgary this week.

There's a tidy profit in store for those who would sell otherwise unworn or unloved gold and silver.

Buying such metals, on the other hand, is a riskier strategy.

Experts and skeptics of silver and gold's new price run are already warning that the commodity is wildly overvalued. In short, they say, this is just another bubble.

But those warnings were not heeded at Albern Coin & Foreign Exchange on 16th Avenue earlier this week. Amid displays of collector's coins framed in velvet boxes, the phone is ringing off the hook.

Behind thick glass and locked doors, the line of customers continues unabated all day.

"It's stupid panic is what it is," says Don Carlson, the general manager. "This is more like Y2K, when people were afraid every computer would shut down."

In a store staffed with white-haired men, Carlson now sits behind a series of living graphs and Microsoft Excel spreadsheets listing the latest values. Prices change by the minute.

Every time a seller steps up to the glass window, he prints out the latest price sheet, which is stapled to a baggie filled with coins or jewels.

Cufflinks, clasps, commemorative medallions and tarnished rings (sans stones) are then whisked to the back of the office to be tested. The gold buyers also take dental fillings, as long as all tooth material is removed.

Nothing to declare': Russian busted smuggling 26,000 diamonds (VIDEO)

Published time: March 11, 2013 15:29
Edited time: March 11, 2013 16:58

Get short URL

Download video (4.92 MB)

A Russian passenger trying to smuggle in 26,000 diamonds was detained at Moscow's Sheremetyevo Airport on his way back from Dubai.

Tags
Crime, Russia

"Various gemstones were found during the customs inspection. There were diamonds of different colors and cuts packed in plastic bags," said the press service of the Federal Customs Service of Russia on Monday.

The diamonds are worth about 5 million rubles (about US$163,000) according to preliminary estimates in the media.

The baggage also contained 249 boxes with iPhone5s and five other devices that were not packed.

The man, who appears to be an unemployed 37-year-old Russian citizen, walked down *"nothing to declare"* customs lane. This is in spite of the fact that Russia requires that gems and precious metals whose value exceed $10,000 should be divulged and are subject to taxes.

The man further claimed that the gems and other goods do not belong to him as he was just asked by a friend to transport them, RIA Novosti says.

The valuable parcels were sent to the Customs Service for examination. The man could face a huge fine in addition to the customs duties on the smuggled gems.

Rush to cash in gold attracts tarnish of possible scams

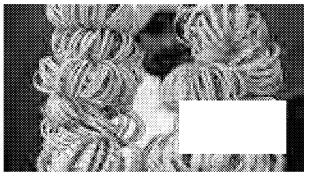
SHIRLEY WON, PAUL WALDIE
The Globe and Mail
Published Thursday, Nov. 11 2010, 7:03 PM EST
Last updated Thursday, Aug. 23 2012, 4:10 PM EDT

The gold frenzy has sparked a rush to sell everything from tooth fillings to old rings from ex-beaus, but it has also spawned a new type of gold digger.

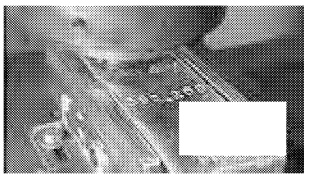
As people rush to profit from a booming gold price – heading to gold parties, cash-for-gold stores and pawn shops – authorities are issuing warnings about seamier outfits luring consumers, through the Internet, to mail in jewellery.

MORE RELATED TO THIS STORY

- Is gold really a safe haven?
- How far to go for gold?
- Here come the gold-is-a-bubble comments



MARKET VIEW
Gold: It's really not a superstar



VIDEO
How to play gold

"It's like the Wild West," said Jo-Ann Sperano, a mediator specialist at New York-based Jewelers Vigilance Committee (JVC), a watchdog for the jewellery industry.

"There are too many of these people ready to take advantage of consumers for a quick buck."

On Thursday, gold reached $1,403.30 (U.S.) an ounce.

The cash-for-gold phenomenon is gaining momentum in Canada, but the darker side of this unregulated industry is the mail-order business, companies offering cash to consumers who send them jewellery.

In the United States and Great Britain, government agencies have launched several investigations. U.S. consumer groups say they have discovered companies making low-ball offers – as much as 80 per cent below the gold's real value.

Ms. Sperano said she has been trying to stop some virtual gold buyers from "stealing" her organization's logo to put on their home pages.

"It [the logo]ensures consumer confidence," she said, adding that her organization fielded many calls from consumers about one website that solicited gold and diamonds and disappeared earlier this week. It was the subject of 57 complaints filed to the Ottawa Better Business Bureau.

The site gave an Ottawa address, which turned out to be a mailbox service, where the jewellery that was mailed in was redirected, said Diane Iadeluca, president of the Ottawa BBB.

"All the complaints were unanswered," she said. "All these customers have sent in different types of jewellery and never saw a return [of money]or a very small cheque. It's very sad."

Chantal Croteau says she got caught in this.

As a way to help pay legal costs for her divorce, she shipped her gold-and-diamond engagement ring and wedding band in September to a man named "Andrew," who had agreed to pay about $2,500 for her jewellery.

"I never heard from them again," she said. "I felt kind of silly. Then, I got a cheque for $4.36. It was a joke."

These kinds of complaints spurred high-end Montreal-based jewellery retailer Birks & Mayors to start an online division a year ago to offer a mail-in jewellery service branded the Birks Gold Exchange.

"A lot of our customers were asking for it" because they didn't feel comfortable sending their jewellery to faceless virtual gold buyers, said Jeanne Gilbert, Internet director at Birks & Mayors. "They trust us. We are a company that is recognized."

Complaints are more common in the United States, where the U.S. Postal Service received more than 1,300 loss claims between 2008 and 2009 from consumers who sent jewellery to Florida-based Cash4Gold, one of the largest U.S.-based mail order businesses.

The company, which advertises heavily on television, has said that packages in the mail get lost or are stolen, according to documents submitted to a U.S. congressional subcommittee. It says it receives as many as 20,000 packages a week.

Jeff Aronson, the chief executive officer of Cash4Gold, stands by the company's practices and says the vast majority of its customers accept the appraisals and the company's offers for their jewellery. Mr. Aronson helped launch the business three years ago and says it has recorded more than 900,000 transactions.

Gold buyers sell the scrap metal to refiners, who melt it into bars. Gold

from rings or necklaces make its way back to jewellers or to the investment industry where it's made into bullion bars bought by exchange-traded funds and the like.

It's all part of the frenzy surrounding gold's spectacular runup.

Gold parties, which are legitimate, started in the United States three years ago amid the recession. Payouts to consumers vary after the company, hostess, and refiners get their cut. Toronto-based Gold Party Princess, one of the pioneers in this country, is also in the midst of selling franchises.

Sherry Wilson, who went to a gold party last Saturday that was hosted by a colleague at her suburban Toronto home, dumped six 10-karat gold rings, two pairs of earrings, a chain and four tiny pendants onto a table in front of gold buyers with GoldSmart Network.

Once the jewellery was tested and weighed, she was given $238 in bills.

"This is a nice treat," said the 37-year-old mother of twin boys. "Some of the rings are from ex-boyfriends. One would be horrified if he knew I just made money from them. … But I wouldn't ever wear them again – they would have sat in my jewellery box for years."

Gold parties, which also grow by referrals, have a "built-in mechanism that forces people to treat others better," but consumers still need to be on their toes, warned Keith Perrin, co-owner of Toronto-based GoldSmart Network and a former president of Jewellers Vigilance Canada, an industry watchdog.

"There are a lot of people who are in this business, and all they did was buy a gold-testing machine and some business cards ...

"A common trick is to confuse people with units of measure," said Mr. Perrin, a former general manager of a metals refinery.

Editor's Note: Some information contained in the original newspaper version and an earlier online version of this article has been deleted from this online version.

Bling losing its lustre

A discreet sign outside the Birks store in the Eaton Centre advises couples they can get up to $1,000 off their wedding bands if they buy a diamond engagement ring at least 0.70 carats in size.

COLIN MCCONNELL / TORONTO STAR Order this photo

Mark Mani, owner of Mani Jewellers in Toronto, says he has been forced to adapt to the economic downturn by carrying more affordably priced pieces (July 15, 2009).

By: Dana Flavelle Business reporter, Published on Thu Jul 16 2009

A discreet sign outside the Birks store in the Eaton Centre advises couples they can get up to $1,000 off their wedding bands if they buy a diamond engagement ring at least 0.70 carats in size.

In the worst economic downturn in decades, even emotion-laden purchases such as wedding rings are being discounted. Stores of all kinds are feeling the impact of rising unemployment and sagging stock portfolios. An unseasonably cool, wet spring hasn't helped.

On the floors below Birks, there are signs of deep price discounting by major retailers: Sears, Esprit, The Children's Place, Pottery Barn.

Sales of clothing, furniture, appliances and electronics are all down. But purveyors of luxury goods are really feeling the pinch. It is a tough time to be in the jewellery business, especially in the United States where a string of chains have filed for bankruptcy as sales plummeted.

"Jewellery is probably one of the most discretionary, delayable purchases there is except for your Sweet 16th or your 25th anniversary where you've got to cough up something," said John Williams of the Toronto-

based retail-consulting firm J.C. Williams Group.

"Also, there's an attitude out there that being frugal is cool," he added. "In the '80s, it was all about `if you've got it, flaunt it.' That's over."

Mark Mani, owner of Mani Jewellers, sees it in his independent store in Toronto's financial district.

Jewellery is still a popular gift but some people are spending less, said Mani, who is stocking fewer "high-ticket" items of $3,000 and up.

"We've had to adapt by stocking more lower-priced items," he said. "I'm carrying lines that are 14-carat gold, instead of 18-carat. Or they're of medium quality finishes versus high-end finishes. Or the diamond quality is one notch down."

He's also still carrying the higher quality merchandise, he said. And in an apparent contradiction, the store's decision to move its bridal collection upmarket is paying off by attracting people who are willing to spend $15,000 or more on an engagement ring.

The decline and fall of the retail sales is particularly challenging for luxury goods firms, that are loath to tarnish their brand by deeply discounting their goods.

Some manufacturers have chosen instead to introduce new lines at lower price points, sometimes under different names.

Gucci has launched a line of watches under its own name that start at $600 instead of $1,000. Simon G has launched lower-priced diamond rings, pendants and necklaces under the Zeghani brand.

Others, such as Tiffany & Co., say they are "staying the course."

"We are not engaging in discounting or changing our marketing or merchandise strategy. We remain confident that the future is bright," Andrea Hopson, vice-president of Tiffany Canada, said.

The big publicly traded jewellery firms, Tiffany, Birks & Mayors, and Zale Corp., which owns Peoples, have all reported dramatic declines in sales, especially in the U.S., where last fall's credit crisis sparked the global downturn.

Sales at the very high-end stores owned by Canadian diamond miner, Harry Winston Inc., fell a dramatic 30 per cent in the spring quarter. Still, that was an improvement over the 60 per cent plunge it felt over Christmas, traditionally the jewellery industry's best season. The stores are outside Canada.

At Tiffany, sales at U.S. stores open more than a year were down 34 per cent in the latest quarter although it is still making money. Other U.S. chains have filed for bankruptcy, including Fortunoff, Whitehall, Friedman's, Christian Bernard and Ultra Stores, the start of what could be an industry shakeout.

The Canadian market, buoyed by a relatively strong banking sector and global demand for oil, has proved to be relatively robust. Still, consumer demand for discretionary big-ticket items, such as jewellery, is at best flat.

Birks & Mayors, whose business is divided between the southern U.S. and Canada, reported sales fell 23.3 per cent in the quarter ending March 28. Same-store sales fell 16 per cent at Mayors chain in the U.S. but were

flat at its Birks stores in Canada. The two chains carry similar merchandise but most of Mayors stores are Florida.

"The economic downturn continues to have a significant impact on the retail industry and luxury goods products in particular," Birks & Mayors' president and chief executive Tom Andruskevich told analysts on a conference call July 6.

The Montreal-based company, which operates 69 stores, has cut 160 jobs, or 15 per cent of its workforce, since the start of the year and frozen management bonuses. It also plans to close its store in St. Catharines at the end of July.

But some observers said what they're seeing is partly a return to more rational industry behaviour.

"Gone are the days of ridiculous mark-ups to pay for the jeweller's Porsche," said Paul Aguirre, editor of *Canadian Jeweller* magazine. "Now, it's more about getting a 10 per cent profit margin and creating a relationship with the client."

He sees jewellery designers moving to address the new "trading down" mentality.

Economic uncertainty has delivered a double whammy, driving the price of gold bullion above $1,000 (U.S.) an ounce as investors flock to hard assets in the face of a fluctuating U.S. dollar.

At the annual JCK trade show in Las Vegas last month, Aguirre said he saw a lot more platinum in place of gold, and a lot more exotic woods in place of gemstones. Pandora, a popular maker of charm bracelets, recently added a line of "eco-chic" wooden beads to its collection of gold, silver and gemstones, he said.

"We also saw a lot of silver. Well-mined, well-produced silver is making a comeback in everything from necklaces, to earrings, rings, and cufflinks," Aguirre said. "I wouldn't be surprised to see silver engagement rings next, if things don't improve."

Looking ahead to the Christmas season, some jewellery retailers are being even more cautious, ordering fewer and less expensive pieces.

"We believe that we have to reduce inventory," Andruskevich of Birks said. "We've given our merchants the responsibility to bring some fresh new products into the business, even though they may have a smaller purchasing budget than a year ago."

OP-ED

Stop Buying and Selling Blood Diamonds

The Kimberley Process and World Diamond Council are a sham.

By Martin Rapaport

Severe human rights violations, including murder, rape and forced labor, have taken place in the diamond fields of Marange, Zimbabwe. Recent reports from Human Rights Watch (HRW) indicate that these horrific conditions continue to take place.

Blood diamonds from Marange, Zimbabwe, have been issued Kimberley Process (KP) certificates and imported into the cutting centers, where they were cut and polished and then sold to dealers, jewelry manufacturers and retailers. Tens of thousands of carats of blood diamonds are now in dealers' inventories and jewelers' showcases — and are being actively sold to consumers.

The jewelry trade's purchase and distribution of blood diamonds is funding a continuing cycle of horrific human rights violations. Our industry is providing money and distribution to those who murder, rape and enslave. Every time we buy or sell a blood diamond, we are sending a message of encouragement to the perpetrators of these inhuman crimes. We are legitimizing their dirty business. We become their partners in crime.

We must face the fact that the KP has been issuing certificates for Marange blood diamonds. The KP has made these "certified blood diamonds" perfectly legal. Customs officials did not — and do not — have the right to stop Marange diamonds with KP certificates. Instead of eliminating blood diamonds, the KP has become a process for the systematic legalization and legitimization of blood diamonds. When you get right down to it, the KP has become a blood diamond laundering system. The KP is not just a sham; it's a scam.

To understand how this could happen, we must define "blood diamonds" and compare our definition to the KP definition of "conflict diamonds."

Rapaport definition: *"Blood diamonds are diamonds involved in murder, mutilation, rape or forced servitude."*

KP definition: *"Conflict diamonds means rough diamonds used by rebel movements or their allies to finance conflict aimed at undermining legitimate governments, as described in relevant United Nations Security Council (UNSC) resolutions insofar as they remain in effect, or in other similar UNSC resolutions which may be adopted in the future, and as understood and recognised in United Nations General Assembly (UNGA) Resolution 55/56, or in other similar UNGA resolutions which may be adopted in future…"*

The KP definition of conflict diamonds does not address human rights violations and does not include blood diamonds. It is a legal definition established by governments to limit the scope and authority of the KP. The KP is a highly politicized process controlled by governments for governments. Its primary function is to protect governments and their revenue — legitimate or not — from rebel forces and consumer boycotts. The KP is

essentially agnostic when it comes to human rights. As HRW concluded in its November 6, 2009, report: "This diamond monitoring body has utterly lost credibility."

In spite of the above, there is a common misconception in the jewelry trade that diamonds with KP certificates are free of human rights abuses. Trade organizations, under the misguided leadership of the World Diamond Council (WDC), have promoted and continue to promote the KP as an acceptable standard for ensuring human rights compliance, even though they know that the KP has been issuing certificates for blood diamonds that have penetrated the diamond and jewelry supply chain. The WDC refuses to inform the trade that the KP cannot be relied upon to ensure human rights compliance and that polished blood diamonds are in the supply chain. The WDC has lost its moral compass. Its primary loyalty is now to the KP and not to the diamond industry or even the basic principles of human decency.

What To Do?

• **Raise Consciousness.** We need to raise consciousness within the jewelry industry about the problem of blood diamonds so that people will stop trading them. Industry organizations that should play a role need to be awakened. I suggest sending emails to Terry Burman, chairman of Jewelers of America (JA), director of the Responsible Jewellery Council (RJC) and the WDC, at tburman@jewels.com; Matt Runci, president and chief executive officer (CEO) of JA, chairman of the RJC, director of the WDC, atmatt@jewelofam.org; Cecilia Gardner, president and CEO of the Jewelers Vigilance Committee (JVC), director of the WDC and CIBJO, at clgjvc@aol.com. You might want to cc the email to other leaders and send a copy to us.

Ask these leaders to confirm that polished blood diamonds are in the distribution system and ask what you or they can do about it. Ask them to use their organizations to inform the trade about the problem. If you know anyone on the board of these organizations, give them a call and ask them to have their organization let people know about blood diamonds.

Email us at fairtrade@rapaport.com if you would like to help us raise consciousness. We will be holding conferences to discuss the issue at BaselWorld on Friday, March 19, 2010, at the Basel Congress Center from 2:00 p.m. to 4:00 p.m., and the JCK Vegas Show, Monday, June 7, 2010, at the Sands Convention Center from 2:00 p.m. to 4:00 p.m. We need new ideas and solutions. We need your help to get organized.

• **Stay informed.** Visit diamonds.net/zimbabwe for background information and google Marange diamonds to stay up to date. Help us stay informed. If you know about people or companies that are selling Marange diamonds, email us. While we don't have the resources to investigate all claims, if a name comes up enough or the case is compelling, we will quietly notify relevant investigative authorities.

• **Return diamonds that you suspect may be blood diamonds.** Pay careful attention to diamonds that have a green hue. Unless you are absolutely sure of where the diamond came from, it is probably a good idea to return all diamonds with a green or green/gray hue in the D to Z and light green color range, not fancy green colors. While there are green diamonds from other places, about 60 percent of Marange's cuttable diamonds are green and tens of thousands of carats have come onto the market over the past year. Furthermore, we are getting reports that the color of some green Marange diamonds is unstable and may worsen.

While many in the industry are opposed to the idea of returns, the hard fact is that you are going to have to make a personal decision about what to do. Thanks to the KP, blood diamonds are perfectly legal and you have no right to return them. On the other hand, do you really want to be selling what may be blood diamonds? It's a financial and ethical issue with a high dose of uncertainty. There may be no clear answers. You might want to talk to a spiritual or ethical adviser.

• **Ask Before You Buy.** As noted in the HRW campaign*, "Zimbabwe's Blood Diamonds, Ask Before You Buy," asking is probably the most important thing you can and should do. Recognize that you are responsible for what you buy and that someone's life may be at stake. Make sure you know who your suppliers are and ask them serious questions to ensure that the diamonds you buy are not from Marange nor involved in other serious human rights abuses. Err on the side of caution. Tell your supplier you really care about where your diamonds come from. If they know you care, they also will care. Make it a point to personally talk to every diamond supplier about human rights issues and how important they are to you.

You will also want your supplier to sign a document promising to refund payment for any diamonds that turn out to be associated with human rights violations. But don't rely solely on the paper; remember to have the talk.

Conclusion

It's time to transcend Kimberley and the WDC. One wonders how many lives will have to be destroyed before the demonstrations begin — before victims come marching down Fifth Avenue, as they did a decade ago. What will it take to get our trade to stop buying and selling blood diamonds?

I know that there are many good and decent people in the diamond and jewelry trade. And I know that many of you care but are frustrated and feel the situation is hopeless. I urge you to reconsider. I urge you not to give up.

We can and will beat this problem. It will take time and unprecedented levels of cooperation. But I do believe that there are enough people in our industry who really care about human rights and that we can make a difference by working together. There is so much good that we can do. I am confident that when the right people come together, we can and will build a more fair and ethical diamond market. We can and will create solutions that will make the world proud of us and our diamonds.

Article from the Rapaport Magazine - February 2010. To subscribe click here.

THE GLOBE AND MAIL

GEMS

Canada to unveil diamond market

Brenda Bouw
VANCOUVER — From Thursday's Globe and Mail
Published Thursday, Jan. 28 2010, 12:00 AM EST
Last updated Thursday, Aug. 23 2012, 1:43 PM EDT

Canada is set to open its first official diamond trading marketplace in downtown Toronto, a move spurred by the rush in recent years to mine and market the homegrown stones both nationally and worldwide.

The Diamond Bourse of Canada opens Monday and will be the first forum of its kind in the country where both polished and rough stones will be bought and sold.

There are 28 diamond bourses in places such as Belgium, Israel and South Africa. The Canadian bourse will become the 29th on the international circuit, which is overseen by the World Federation of Diamond Bourses. Canada produces about 15 per cent of the world's annual rough diamonds.

"It's only logical for Canada to establish a full-fledged bourse," federation president Avi Paz stated yesterday. "While Canada's population is small compared to its huge southern neighbour, the country's jewellery industry and trade, as well as its consumer market, have been growing steadily."

Diamonds were first discovered in Canada in the Northwest Territories in 1991. Since then, Canada has grown to become the third-largest producer of gem-quality stones valuing about $2.4-billion in 2008. (Botswana and Russia are number one and two, respectively.)

The Canadian bourse will begin by trading polished diamonds, and expects to later move into the trade of rough diamonds. Currently, a small portion of Canadian rough production has been available for sale in the NWT, which hasn't been considered a top buying destination for diamond dealers. It's considered more cost effective to travel to places such as South Africa, where there's also a wider selection.

Colleen Peyer, general manager at the Diamond Bourse of Canada, said the bourse is expected to change that, and will provide a secure space for people to trade the stones. "We'd like to see all Canadian diamonds traded on Canadian soil, rough and polished," she said.

To trade, you have to be a member of the bourse; there are now about 35 members. Only Canadian members can sell at the Canadian-based bourse, although any international members can buy there.

Bourse chairman Bhushan Vora, of diamond wholesaler Gemstar Inc., said the Canadian marketplace was a long-time coming. "This was one element in the industry was missing."

He said the Ontario government took the lead on the bourse project and matched the $140,000 in funds raised to help create the bourse.

Mr. Vora said the bourse will be self-financed through its $1,500 annual membership fees, as well as commissions on activities such as tenders, which are basically auctions for diamonds, and services such as storage and supplies.

THE GLOBE AND MAIL

DIAMONDS

Skilled immigrants staff Sudbury gem plant

Andy Hoffman
Globe and Mail Update
Published Wednesday, Oct. 14 2009, 8:00 PM EDT
Last updated Friday, Jan. 14 2011, 9:10 PM EST

On the eighth floor of a nondescript office building in downtown Sudbury, a group of highly skilled workers slice, score and sever millions of dollars worth of merchandise each day.

Most have been practising their trade for years and their work is destined for sale at some of the world's most exclusive retailers. But the exact location of the facility, the first of its kind in Ontario, is a secret, because of the nature of the goods - diamonds.

"We've been warned by the local police in Sudbury that there is a certain amount of biker activity. It's something we have to be aware of," said Dylan Dix, marketing director for Crossworks Manufacturing Ltd., which operates the factory.

The operation was envisaged as a job creation initiative by the Ontario government, part of its effort to spur new business and employment by positioning the province as a key link in the global diamond trade.

For now, though, all 27 workers at Ontario's only diamond polishing and cutting facility have had to be flown in from Vietnam.

In a city where the unemployment rate is 10 per cent, it's not that there's a shortage of available workers. But diamond polishing and cutting is a highly specialized skill that isn't learned overnight.

The Sudbury factory's production will all be labelled as Ontario diamonds, but staffing the new Sudbury facility with local workers is likely to take years, concedes Ron Gashinski, chief gemmologist of the diamond sector unit at Ontario's Ministry of Northern Development, Mining and Forestry.

"It's extremely difficult. You're not working on a $2 bolt here," he said. "Some diamonds will be worth thousands of dollars or tens and hundreds of thousands of dollars. The expertise required to do that takes quite a while to get."

The Vietnamese diamond cutters arrived in the Northern Ontario city in August. They are being housed at an apartment building leased by Crossworks, a privately held Vancouver company that specializes in processing rough diamonds for sale to the jewellery industry.

The workers have been quietly cutting and polishing diamonds sourced from De Beers Canada's Victor Mine near James Bay for about a month now.

About $25-million worth of diamonds sourced from the Victor mine are to be processed each year at the Sudbury diamond factory. As part of an agreement with the government of Ontario, the South African diamond giant agreed to make 10 per cent of Victor's annual production available to diamond cutting and polishing operations in the province.

Diamonds have been mined in Canada for more than a decade - first in the Northwest Territories and more recently in Ontario - but the vast majority of the production ends up being shipped to traditional diamond polishing and cutting centres such as India, Africa or Vietnam, where workers are paid far less than they would be in Canada. Ontario wants to be part of the "international diamond pipeline," processing and trading the stones as well as unearthing them.

Mr. Dix said Crossworks is able to cut and polish diamonds in a high-cost environment and still be profitable by working with more valuable stones.

"If your [polishing]cost is $100 on a $1,000 stone, it's 10 per cent. If it is $100 on a $10,000 stone, it's 1 per cent. In general, what we are polishing is a more expensive product, so we are willing to absorb the costs," he said.

In addition to operations in Namibia, Ho Chi Minh City and Vancouver, Crossworks operates a polishing facility in Yellowknife that processes diamonds from the Diavik and Snap Lake Mines. Currently, none of the 11 polishers at the Yellowknife factory are locals, and the staff have been drawn from Vietnam and Vancouver.

Crossworks expects to reach an agreement with a local college in Sudbury to develop and host a training course that will be used to eventually staff the new factory.

Despite the high unemployment rate, Sudbury Mayor John Rodriguez said his city has welcomed the new diamond factory and its Vietnamese workers.

"I know it will take time to train them properly. I do have the commitment that these folks that are here cutting and polishing are here to get the operation started. When our workers are trained, they will take up those jobs," Mr. Rodriguez said.

http://www.financialpost.com/related/topics/RCMP+issues+warning+diamonds/5231287/story.html

RCMP issues warning on diamonds

Stanley Tromp, Financial Post · Aug. 10, 2011

The RCMP has warned that Canada's fast-growing diamond industry is at serious risk for money laundering by organized crime and terrorists, according to a document released to the Financial Post under the Access to Information Act.

"The Canadian diamond industry remains largely unregulated," the partially censored report says, and leaves dealers vulnerable to money laundering and a law enforcement system ill-equipped to handle the problem.

"The RCMP can only enforce existing legislation," said RCMP Sergeant Julie Gagnon. "The trade in precious metals and stones is a self-regulated industry where instances of money laundering do occur."

She said an update to the 2009 Project SHYNE report by the RCMP's criminal intelligence branch is expected to be publicly released this fall.

Canada is the world's third largest producer of rough diamonds, and in the next decade its share will likely rise.

But in the global context, Canada is a reasonably new diamond net exporter, the report says, "with no tradition in policymaking or industry regulation."

The diamond exploration boom that began in the early 1990s in the far north is well known, but the secondary diamond industry is also expected to grow in Canada, leading to more cutting and polishing centres.

It is the immense profit potential in these secondary industries that could be lucrative for organized crime groups in Canada, the report adds.

There are 6,500 dealers of precious metals and stones in Canada's highly fragmented market. Unlike other industries with easy entrances, the jewellery business is often a family affair and fuelled by personal contacts, and as a result it is so much harder for police to access.

Diamond smuggling could be used to import or export criminal profits through airports because the items are so small, odourless, non-metallic and easily hidden (even within a person's body), and they are not considered "monetary instruments" in law.

A major problem is the "value manipulation" of diamonds. Dealers can alter the jewellery's price by falsifying documents, or by not declaring the nature of diamonds at the point of sale. As well, retailers now often buy more diamonds from underground markets than from legitimate

wholesale dealers, perhaps partly due to more jewellery store robberies across Canada, which has helped lead to "the growth of a parallel, illicit market among dealers."

Auction houses are at special risk from money launderers for three reasons, the report noted. First, auction houses are not covered under the rules of Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). In law, they are not considered to "purchase or sell" jewellery in the auction process, but are "mere intermediaries or agents" between buyers and sellers.

Second, at the largest auction houses, bidders can be sophisticated in knowing the true value of the jewellery, and they can be agents for the real buyer who wants anonymity. Third, jewellery pieces are often sold as a part of an entire lot, and the lot numbers are compiled in a catalogue that is distributed only to industry insiders.

Information on dealers' sales and clientele is "guarded with the utmost secrecy," the report stated.

Pierre Leblanc, president of Canadian Diamond Consultants Inc., said in an interview that the jewellery industry is so competitive, it is fair that such commercially sensitive information be guarded closely.

-30-

NATIONAL POST

Financial Post

Peoples gets new parent

Armina Ligaya

Financial Post, Bloomberg News
962 words
20 February 2014
National Post
FINP
All_but_Toronto
FP1 / Front
English

Two of the U.S.'s biggest diamond sellers - including the owner of Canada's Peoples Jewellery and Mappins - have agreed to a multi-million dollar marriage of convenience.

Signet Jewelers Ltd.'s acquisition of Zale Corp., a deal valued at US$1.4-billion including debt, is the latest sign of industry consolidation as chains and mom-and-pop shops increasingly battle online upstarts for customers.

The top two U.S. mid-priced jewellers announced Wednesday they have entered into an agreement in which Signet will acquire all of its smaller rival's issued and outstanding stock at US$21 in cash per share, a 41% premium over the closing price on the NYSE a day earlier.

With this acquisition Signet, the largest specialty retailer in the U.S. and the U.K., boosts its store locations from 1,900 to 3,600 and becomes the leading trinket retailer in Canada, said Mike Barnes, the chief executive and director of Signet Jewelers.

"We are not only number one in the U.S. and the U.K.; this acquisition will also make our newly combined company number one in Canada as well and it will allow us to continue building a platform for potential future geographic expansion," he said during a conference call Wednesday.

Investors seemed to like the pairing as Zale stock rose more than 40% to close at $20.92 on the New York Stock Exchange - impressive given that it hovered as low as $3.80 last March. Signet's stock rose 18% Wednesday.

The combined company will generate approximately US$6-billion in sales and more than US$700-million in EBITDA, and will have nearly 30,000 associates, Mr. Barnes said.

With Signet's jewellery brands Kay and Jared, which are leaders in the mid-priced and the upper-midpriced segments, the addition of Zale's equally mall-friendly brands "will help us maximize our midmarket success," he said.

The new company is also expected to see US$100-million in synergies by the third year of operation, in large part due to stronger buying power and cost improvements, Signet executives said on the conference call. The Zale brand will operate as a separate standalone division within Signet, led by Zale's chief executive Theo Killion.

This acquisition, subject to shareholder approval, would cap what has been a tumultuous run over the years for Zale, and Peoples Jewellery.

Peoples was founded in Toronto 1919 by the Gerstein family, which grew the business over the following decades into a chain of jewellery stores with as many as 280 locations by the 1980s.

In 1986, Peoples teamed up with Switzerland's Swarovski International to swing the junk-bond financed US$650-million purchase of Zale, which at the time was a firm more than five times its size. In 1989, the company later bought Gordon Jewelry Corp for US$311-million.

But after recession hit in the early 1990s, combined with high interest payments, Zale was pushed to the brink, filing for bankruptcy in 1992. In 1993, Peoples followed it down. In an odd twist, by 1999, a stronger, financially-healthier Zale bought Peoples Jewellery for US$115-million.

Many years later, consolidation in the jewellery industry at all price points continues, said David Wu, luxury goods analyst at Telsey Advisory Group in New York.

Hamilton, Bermuda-based Signet had previously discussed buying Zale but those talks ended in 2006 after Zale's board decided to stay independent, according to Bloomberg. After Zale saw slumping sales in recent years, it embarked on a multiyear restructuring which is "starting to bear fruit," said Mr. Wu, drawing a suitor.

Zale Corp.'s holiday sales results showed overall comparable store sales up 2%, with Zales' branded stores up 4.4% and Peoples performing strongly at 2%. Mappins, however, saw sales drop more than 6%.

In both Canada and the U.S., this sector of retail remains fragmented with independent retailers and momand-pop stores competing with the jewellery giants, but consolidation is increasing as chains look to benefit from economies of scale.

"Consolidation has been happening, but at a very slow pace," Mr. Wu. said. "This acquisition does speed up the pace."

The U.S. jewellery industry is also consolidating as stores face online challengers such as Blue Nile Inc., Ken Gassman, president of the Jewelry Industry Research Institute, told Bloomberg.

Mr. Wu said the deal potentially allows to roll out its brands north of the border and providing Zale with access to "best in class" management.

"It really gives Signet an entry way into the Canadian market," he said. "I wouldn't be surprised if Signet uses some of the real estate it currently has in Canada and potentially convert some of the underperforming Mappins stores into potentially a Kay store or a Jared store ... which I think would be very well-received."

aligaya@nationalpost.com

Scott Eells, Bloomberg News / Traffic passes in front of a Zale Corp. retail store in New York. Signet Jewelers Ltd., operator of the Kay and Jared brands, agreed to buy Zale Corp. for about US$1.4 billion, expanding its leadership as the largest jeweller in North America. The deal also affects the Peoples chain in Canada which is owned by Zales.; Scott Eells, Bloomberg News / Traffic passes in front of a Zale Corp. retail store in New York. Signet Jewelers Ltd., operator of the Kay and Jared brands, agreed to buy Zale Corp. for about US$1.4 billion, expanding its leadership as the largest jeweller in North America. The deal also affects the Peoples chain in Canada which is owned by Zales. [NTNP_20140220_All_but_Toronto_FP1_02_I001.jpg];

National Post

Document FINP000020140220ea2k0002r

Search Summary

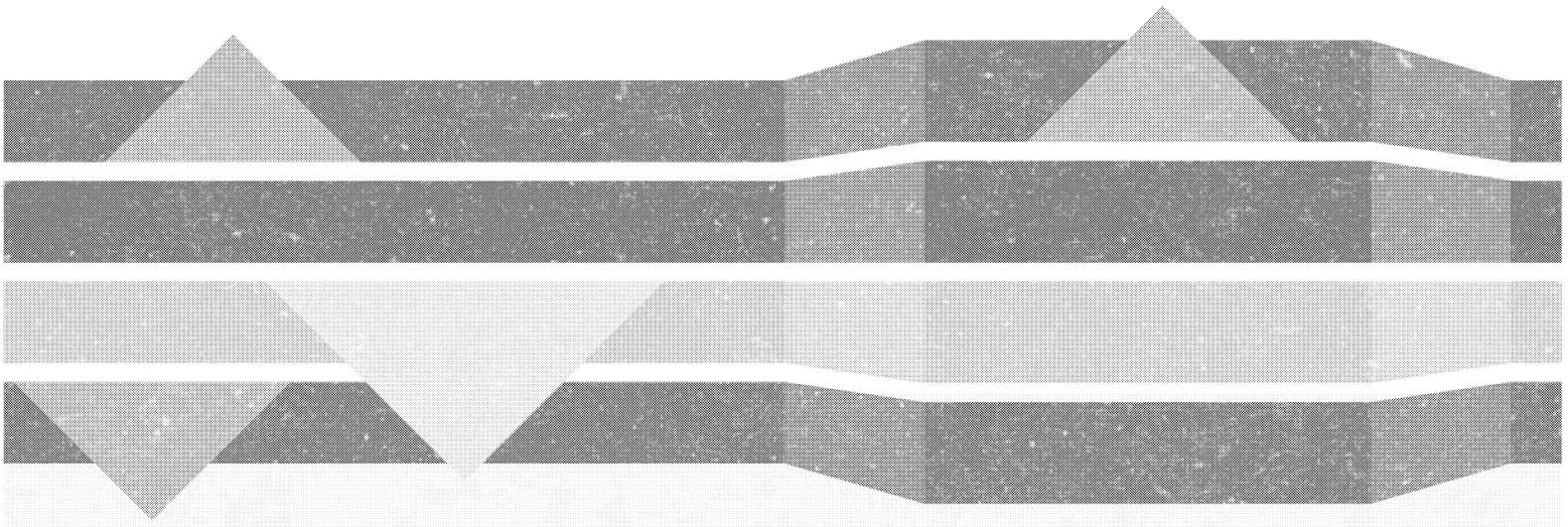
Text	peoples gets new parent
Date	All Dates

Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	All Regions
Language	English

Grant Thornton

Reporting Entity Sector Profiles: Securities Dealers Appendices

Prepared for FINTRAC | March 31, 2014



Appendix A: Industry statistics and reporting entity data

Securities Dealers Industry NAICS Codes

Code	Description
5231	Securities and commodity contracts intermediation and brokerage
52311	Investment banking and securities dealing US
523110	Investment banking and securities dealing US
52312	Securities brokerage US
523120	Securities brokerage US
52313	Commodity contracts dealing US
523130	Commodity contracts dealing US
52314	Commodity contracts brokerage US
523140	Commodity contracts brokerage US
5232	Securities and commodity exchanges
52321	Securities and commodity exchanges
523210	Securities and commodity exchanges
5239	Other financial investment activities
52391	Miscellaneous intermediation US
523910	Miscellaneous intermediation US
52392	Portfolio management US
523920	Portfolio management US
52393	Investment advice US
523930	Investment advice US
52399	All other financial investment activities US
523990	All other financial investment activities
6211	Security Brokers, Dealers, and Flotation Companies
6221	Commodity Contracts Brokers and Dealers
6282	Investment Advice

Securities Sealers SIC Codes

Code	Description
6211	Security Brokers, Dealers, and Flotation Companies
6221	Commodity Contracts Brokers and Dealers
6282	Investment Advice

Using NAICs codes, searches for statistical data on the Real Estate Industry sectors were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Banking and Securities Dealing (NAICS 52311)

This industry comprises establishments primarily engaged in acting as principals (investors who buy or sell on their own account), generally on a spread basis, in originating, underwriting and/or distributing issues of securities of businesses, governments and institutions. Establishments primarily engaged in making markets (dealing or trading) in securities are included.

Number of establishments in Canada by type and region: December 2012
Inverstment Banking and Securities Dealing (NAICS 52311)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	134	263	397	15.7%
British Columbia	180	294	474	18.7%
Manitoba	18	45	63	2.5%
New Brunswick	20	16	36	1.4%
Newfoundland and Labrador	9	11	20	0.8%
Northwest Territories	1	1	2	0.1%
Nova Scotia	21	38	59	2.3%
Nunavut	0	1	1	0.0%
Ontario	407	681	1,088	43.0%
Prince Edward Island	6	6	12	0.5%
Quebec	131	175	306	12.1%
Saskatchewan	38	31	69	2.7%
Yukon Territory	1	1	2	0.1%
CANADA	966	1,563	2,529	100%
Percent Distribution	38.2%	61.8%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Inverstment Banking and Securities Dealing (NAICS52311)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	69	63	2	0
British Columbia	60	117	2	1
Manitoba	6	12	0	0
New Brunswick	8	12	0	0
Newfoundland and Labrador	2	7	0	0
Northwest Territories	0	1	0	0
Nova Scotia	5	16	0	0
Nunavut	0	0	0	0
Ontario	162	224	15	6
Prince Edward Island	1	4	1	0
Quebec	48	77	6	0
Saskatchewan	10	28	0	0
Yukon Territory	0	1	0	0
CANADA	371	562	26	7
Percent Distribution	38.4%	58.2%	2.7%	0.7%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Securities Brokerage (NAICS 52312)

This Canadian industry comprises establishments primarily engaged in buying or selling securities for others on a commission basis

Number of establishments in Canada by type and region: December 2012 Securities Brokerage (NAICS 52312)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	107	64	171	10.6%
British Columbia	170	110	280	17.3%
Manitoba	43	17	60	3.7%
New Brunswick	15	8	23	1.4%
Newfoundland and Labrador	4	2	6	0.4%
Northwest Territories	1	0	1	0.1%
Nova Scotia	31	13	44	2.7%
Nunavut	0	0	0	0.0%
Ontario	430	268	698	43.1%
Prince Edward Island	6	2	8	0.5%
Quebec	131	144	275	17.0%
Saskatchewan	41	10	51	3.2%
Yukon Territory	2	0	2	0.1%
CANADA	981	638	1,619	100%
Percent Distribution	60.6%	39.4%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Securities Brokerage (NAICS52312)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	67	35	4	1
British Columbia	105	57	7	1
Manitoba	23	20	0	0
New Brunswick	9	6	0	0
Newfoundland and Labrador	3	1	0	0
Northwest Territories	1	0	0	0
Nova Scotia	19	12	0	0
Nunavut	0	0	0	0
Ontario	252	151	24	3
Prince Edward Island	3	3	0	0
Quebec	59	66	5	1
Saskatchewan	26	15	0	0
Yukon Territory	2	0	0	0
CANADA	569	366	40	6
Percent Distribution	58.0%	37.3%	4.1%	0.6%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Securities and Commodity Exchanges (NAICS 52321)

This industry comprises establishments primarily engaged in providing marketplaces and mechanisms for the purpose of facilitating the buying and selling of stocks, stock options, bonds or commodity contracts. The establishments in this industry do not buy, sell, own or set the prices of the traded securities and/or commoditie

Number of establishments in Canada by type and region: December 2012 Securities and Commodity Exchanges (NAICS 52321)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	12	26	38	14.4%
British Columbia	15	43	58	22.1%
Manitoba	2	8	10	3.8%
New Brunswick	2	2	4	1.5%
Newfoundland and Labrador	2	0	2	0.8%
Northwest Territories	0	0	0	0.0%
Nova Scotia	2	4	6	2.3%
Nunavut	0	0	0	0.0%
Ontario	26	77	103	39.2%
Prince Edward Island	0	0	0	0.0%
Quebec	6	28	34	12.9%
Saskatchewan	1	7	8	3.0%
Yukon Territory	0	0	0	0.0%
CANADA	68	195	263	100%
Percent Distribution	25.9%	74.1%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Securities and Commodity Exchanges (NAICS52321)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	8	4	0	0
British Columbia	13	1	1	0
Manitoba	1	1	0	0
New Brunswick	2	0	0	0
Newfoundland and Labrador	0	2	0	0
Northwest Territories	0	0	0	0
Nova Scotia	1	1	0	0
Nunavut	0	0	0	0
Ontario	10	11	3	2
Prince Edward Island	0	0	0	0
Quebec	2	3	1	0
Saskatchewan	0	1	0	0
Yukon Territory	0	0	0	0
CANADA	37	24	5	2
Percent Distribution	54.4%	35.3%	7.4%	2.9%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Portfolio Management (NAICS 52392)

This Canadian industry comprises establishments primarily engaged in managing the portfolio assets of others on a fee or commission basis. These establishments have the authority to make investment decisions, with fees usually based on the size and/or overall performance of the portfolio. Examples of establishments in this industry are pension fund managers and mutual fund managers.

Number of establishments in Canada by type and region: December 2012 Portfolio Management (NAICS 52392)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	362	1,585	1,947	10.3%
British Columbia	495	1,919	2,414	12.8%
Manitoba	113	436	549	2.9%
New Brunswick	33	186	219	1.2%
Newfoundland and Labrador	12	59	71	0.4%
Northwest Territories	11	12	23	0.1%
Nova Scotia	46	253	299	1.6%
Nunavut	1	2	3	0.0%
Ontario	1,168	6,059	7,227	38.4%
Prince Edward Island	6	31	37	0.2%
Quebec	627	5,044	5,671	30.1%
Saskatchewan	79	275	354	1.9%
Yukon Territory	1	15	16	0.1%
CANADA	2,954	15,876	18,830	100%
Percent Distribution	15.7%	84.3%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Portfolio Management (NAICS 52392)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	237	115	9	1
British Columbia	342	142	11	0
Manitoba	70	37	4	2
New Brunswick	21	10	2	0
Newfoundland and Labrador	9	3	0	0
Northwest Territories	2	8	1	0
Nova Scotia	30	15	1	0
Nunavut	1	0	0	0
Ontario	708	387	57	16
Prince Edward Island	4	2	0	0
Quebec	376	228	20	3
Saskatchewan	42	33	4	0
Yukon Territory	1	0	0	0
CANADA	1,843	980	109	22
Percent Distribution	62.4%	33.2%	3.7%	0.7%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Investment Advice (NAICS 52393)

This Canadian industry comprises establishments primarily engaged in providing investment advice to others on a fee basis, provided that they do not also have the authority to execute trades. Establishments in this industry may communicate their advice both directly to their clients and via printed or electronic media as part of a subscription service. Establishments providing financial planning advice, investment counseling and investment research are included. (e.g. financial investment advice services, customized, fees paid by clients, investment advice counselling services, customized, fees paid by clients.

Number of establishments in Canada by type and region: December 2012 Investment Advice (NAICS 52393)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	297	1,057	1,354	16.7%
British Columbia	391	841	1,232	15.2%
Manitoba	92	127	219	2.7%
New Brunswick	47	46	93	1.1%
Newfoundland and Labrador	20	49	69	0.8%
Northwest Territories	0	5	5	0.1%
Nova Scotia	45	111	156	1.9%
Nunavut	0	0	0	0.0%
Ontario	1,190	2,503	3,693	45.5%
Prince Edward Island	2	18	20	0.2%
Quebec	342	697	1,039	12.8%
Saskatchewan	87	151	238	2.9%
Yukon Territory	3	3	6	0.1%
CANADA	2,516	5,608	8,124	100%
Percent Distribution	31.0%	69.0%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Investment Advice (NAICS52393)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	258	39	0	0
British Columbia	327	63	1	0
Manitoba	69	22	1	0
New Brunswick	39	8	0	0
Newfoundland and Labrador	14	6	0	0
Northwest Territories	0	0	0	0
Nova Scotia	36	9	0	0
Nunavut	0	0	0	0
Ontario	898	282	8	2
Prince Edward Island	2	0	0	0
Quebec	266	74	2	0
Saskatchewan	69	18	0	0
Yukon Territory	2	1	0	0
CANADA	1,980	522	12	2
Percent Distribution	78.7%	20.7%	0.5%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Sic Code 6282 - Services Allied with the Exchange of Securities - Investment Advice

Province	Number of Establishments
Alberta	
British Columbia	1223
Manitoba	260
New Brunswick	104
Newfoundland and Labrador	62
Northwest Territories	5
Nova Scotia	176
Nunavut	1
Ontario	3485
Prince Edward Island	29
Quebec	1176
Saskatchewan	189
Yukon	4
Grand Total	7689

NAICS 52311 - Investment Banking and Securities Dealing

Province	Number of Establishments
Alberta	34
British Columbia	50
Manitoba	2
New Brunswick	3
Newfoundland and Labrador	1
Northwest Territories	1
Nova Scotia	2
Ontario	212
Quebec	40
Saskatchewan	7
Grand Total	352

NAICS 523130 - Commodity Contracts Dealing

Province	Number of Establishments
Alberta	26
British Columbia	90
Manitoba	9
New Brunswick	1
Nova Scotia	2
Ontario	147
Quebec	28
Saskatchewan	3
Grand Total	306

NAICS 523120 - Securities Brokerage

Province	Number of Establishments
Alberta	1
British Columbia	4
Ontario	11
Quebec	5
Saskatchewan	1
Grand Total	22

523140 – Commodity Contracts Brokerage

• Province	• Number of Establishments
Alberta	4
British Columbia	4
Manitoba	4
Ontario	10
Grand Total	22

523920 - Portfolio Management

• Province	• Number of Establishments
Alberta	2
British Columbia	11
Manitoba	1
Nova Scotia	2
Ontario	28
Quebec	6
Grand Total	50

NAICS - 52393 - Investment Advice

Province	Number of Establishments
Alberta	977
British Columbia	1,213
Manitoba	259
New Brunswick	105
Newfoundland and Labrador	62
Northwest Territories	5
Nova Scotia	174
Nunavut	1
Ontario	3,467
Prince Edward Island	29
Quebec	1,179
Saskatchewan	189
Yukon	4
Grand Total	7,664

SIC 6211 - Security Brokers, Dealers, and Flotation Companies

Province	Number of Establishments
Alberta	672
British Columbia	907
Manitoba	103
New Brunswick	64
Newfoundland and Labrador	34
Northwest Territories	2
Nova Scotia	146
Nunavut	1
Ontario	1,854
Prince Edward Island	14
Quebec	565
Saskatchewan	128
Yukon	6
Grand Total	4,496

SIC 6282 - Investment Advice

Province	Number of Establishments
Alberta	975
British Columbia	1,222
Manitoba	260
New Brunswick	104
Newfoundland and Labrador	62
Northwest Territories	5
Nova Scotia	176
Nunavut	1
Ontario	3,486
Prince Edward Island	29
Quebec	1,176
Saskatchewan	189
Yukon	4
(blank)	
Grand Total	7,689

SIC 6221 - Commodity Contracts Brokers and Dealers

Province	Number of Establishments
Alberta	4
British Columbia	5
Manitoba	5
Ontario	14
(blank)	
Grand Total	28

Gross domestic product (GDP) at basic prices, by North American Industry Classification System (NAICS) - (dollars x 1,000,000)

	Canada Annual GDP	Financial investment services, funds and other financial vehicles
2000	14,841,865	118,128
2001	15,050,832	128,749
2002	15,446,975	134,700
2003	15,774,145	140,616
2004	16,262,665	154,572
2005	16,751,040	167,604
2006	17,219,219	192,156
2007	17,600,292	204,528
2008	17,784,972	197,868
2009	17,259,612	180,444
2010	17,870,712	190,272
2011	18,360,060	194,544
2012	18,696,924	196,068
2013	19,065,087	211,074

Appendix B: Case examples and typologies

The enclosed articles have been sourced from; news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. IIROC News Release - Personal Financial dealings and Outside Business Activities: IIROC Rule Changes Improve Transparency and Reduce Potential Conflicts, June 13, 2013.

2. IIROC News Release - In the Matter of Frederic Lavoie – Discipline Decision – Liability and Penalty – October 15, 2013.

3. IIROC News Release – In the Matter of James Charles Dennis – Penalty – June 29, 2011.

4. IIROC News Release – IIROC announces settlement agreement for Todd William Stefiuk, March 22, 2011.

5. IIROC News Release – In the Matter of Malcolm McKimm – Discipline, August 16, 2010.

6. IIROC News Release – In the Matter of Konstantine Dariotis and Alfonso Fiumidinisi – Settlement Accepted, February 13, 2012.

7. IIROC News Release – In the Matter of Malcolm Joseph McKimm – Settlement, September 8, 2010.

8. IIROC News Release – In the Matter of Acadian Securities Inc. – Settlement, January 29, 2009.

9. IIROC News Release – In the Matter of Stephane Rail – Discipline, July 22, 2008.

10. IIROC News Release – In the Matter of Sandy Joseph Bortolin – Discipline decision – Liability and Penalty, April 13, 2012.

11. OSC – In the Matter of Mrs Sciences Inc. (Formerly Morningside Capital Corp), Americo Derosa, Ronald Sherman, Edward Emmons, Ivan Cavric and Primequest Capital Corporation, February 2, 2011.

12. OSC – In the Matter of Firestar Capital Management Corp., Kamposse Financial Corp., Firestar Investment Management Group, Michael Civarella and Michael Mitton.

13. Reorganized crime; Our Mafia and Hells Angels have grown in a nice, co-operative Canadian way. Now, big-time crime is run so much like a business that the boundary between legit and crooked is beginning to blur. The Globe and Mail, September 26, 2008.

14. Vancouver promoter implicated in international bribery scandal; Naeem Tyab arranged $2-million payment to wife of Chadian ambassador, according to court document. Vancouver Sun, February 2, 2013.

15. Surry man banned for bogus gold scheme; Securities commission also issues cease-trade order against Bahamian firm. Vancouver Sun, May 24, 2012.

16. The Wild West of investing: The biggest financial market you've never heard of. Golden Girl Finance, April 2, 2012.

17. Welcome to Canada's exempt market: Exclusive, anything goes investments – but play at your own risk. Financial Post, June 15, 2013.

18. UANI condemns AGF for maintaining investments in fraudulent bonds that support illicit Hizballah and Iranian activities, Business Wire, September 11, 2012

19. Disgraced investment firm ordered to forfeit $15M, pay $750K penalty, Belleville Intelligencer, September 12, 2012.

20. Hearing underway in $400-milliion Ponzi scheme case. Calgary Herald, September 6, 2012.

21. Regulator for mutual fund dealers tries to stay relevant. The Globe and Mail, December 29, 2013.

22. Tougher advisors' standards up for debate. The Bottom Line, March 2014.

23. More consolidation as boutique investment dealers struggle to survive. Financial Post, January 27, 2014.

24. St. Albert man charged with fraud; Concrete Equities raised millions for Mexico condominium project. Edmonton Journal, January 23, 2014.

25. 'The wolf? He's still big and bad,' says one of 1,500 real-life fraud victims. Postmedia Breaking News, January 19, 2014.

26. TD Bank fined $5.2 million by Federal regulators. Dow Jones News Service, September 23, 2013.

27. Accused money launderer and admitted stock offender cross paths in Naramata; Erwin Speckert's B.C. company is listed as the owner of lakefront property, but Ingo Mueller and his wife live there and call it their own. Vancouver Sun, April 17, 2013.

28. FROG Genmed's Harris pleads not guilty in L.A. Canada Stockwatch, March 7, 2013.

29. Woman accused in $135-million scheme; Payday-loan operator had hundreds of investors in alleged Ponzi scam. Victoria Times Colonist, January 22, 2013.

30. Calgary men, companies face $54-million in sanctions for 'massive fraud'; ASC issues penalties in fraud case for Brost, Morice and Sorenson. The Globe and Mail, September 28, 2012.

31. Victoria 'wealth creation' firm closes doors after string of bad investment recommendations; President and owner of Wealth by Design, Denise Andison, now promoting fledgling recycling company. The Vancouver Sun, September 8, 2012.

32. Investment advisor found guilty of obstruction; Was fined for a similar crime in 2009. Montreal Gazette, August 14, 2012.

33. Canadian man charged in U.S. Ponzi scheme. Calgary Herald, April 18, 2012.

34. Four charged in $16m investment scheme; Hamilton and Halton residents invested in what police say were bogus companies; restitution ordered. The Hamilton Spectator, April 12, 2012.

35. Fraud isn't likely to disappear even with convictions. Victoria Times Colonist, March 29, 2012.

36. West Vancouver stock promoter languishes in Austrian jail; Aly Mawji has been in prison for 10 months awaiting outcome of multimillion-dollar manipulation charges. Vancouver Sun, March 29, 2012.

37. Securities fraud still largely undetected in Canada and the U.K. – CFA Institute study. Business Vancouver, September 3, 2013.

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

NEWS RELEASE

For immediate release

For further information, please contact:

Lucy Becker
Vice President, Public Affairs
416 943-5870
lbecker@iiroc.ca

Karen Archer
Senior Media & Public Affairs Specialist
416 865-3046
karcher@iiroc.ca

Personal Financial Dealings and Outside Business Activities

IIROC Rule Changes Improve Transparency and Reduce Potential Conflicts

June 13, 2013 (Toronto, Ontario) – The Investment Industry Regulatory Organization of Canada (IIROC) today announced that firms will have six months to implement rule amendments relating to prohibited personal financial dealings and permissible outside business activities (Attachment A). IIROC's rule amendments take effect December 13, 2013, with the exception of trustee or executor type arrangements which must be compliant by June 13, 2014.

The amendments, approved by its recognizing regulators, codify IIROC's prior position by specifically prohibiting employees and Approved Persons of IIROC-regulated dealer firms from directly or indirectly engaging in personal financial dealings with clients. To achieve this, IIROC Dealer Member Rule 43 includes a general prohibition on engaging in personal financial dealings with clients and provides a non-exhaustive list of prohibited dealings.

The amendments to Dealer Member Rule 18.14 expand the scope of the current rules that apply to "other gainful occupations" to include all "outside business activities". Further, the rules clarify that a Registered Representative/Investment Representative must inform their IIROC-regulated firm of any outside business activity and obtain their firm's advance approval to engage in any such outside business activity.

The rule amendments follow extensive consultations with stakeholders over the past three years and are consistent with other IIROC initiatives designed to improve relationship disclosure, enhance transparency and reduce potential conflicts.

***

IIROC is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Created in 2008 through the consolidation of the Investment Dealers Association of Canada and Market Regulation Services Inc., IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets.

IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees and through setting and enforcing market integrity rules regarding trading activity on Canadian equity marketplaces.

-30-

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

NOTICE/NEWS RELEASE

For immediate release

Enforcement Notice
Decision
13-0258

For further information, please contact:

Enforcement Contact:

Carmen Crépin
Vice President, Québec
514 878-2854
ccrepin@iiroc.ca

Media Contact:

Karen Archer
Senior Media and Public Affairs Specialist
416 865-3046
karcher@iiroc.ca

IN THE MATTER OF Frédéric Lavoie – Discipline Decision – Liability and Penalty

October 15, 2013 (Montréal, Québec) – Following a disciplinary hearing held on May 22, 2013, in Montréal, Québec, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) found Frédéric Lavoie liable for the following violations: failing to use due diligence to ensure that he had the necessary knowledge of the features and risks inherent in leveraged Exchange-Traded Funds before recommending such an investment to his clients, and failing to inform his employer that he was engaging in an outside business activity.

The Hearing Panel's decision, dated September 3, 2013, is available at http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=D89F615BAB214379AB9086C912205031&Language=en.

Specifically, the Hearing Panel ruled that Mr. Lavoie did commit the following violations:

(a) Between March 8, 2008 and March 2, 2009, Mr. Lavoie failed to use due diligence by neglecting to ensure that he had the necessary knowledge of the features and risks inherent in leveraged Exchange-Traded Funds before recommending such an investment to two of his clients, contrary to IIROC (formerly the IDA) Dealer Member Rule (By-Law) 1300.1(a);

(b) Between March 8, 2008 and March 2, 2009, Mr. Lavoie failed to use due diligence by neglecting to ensure that his investment recommendations in leveraged Exchange-Traded Funds constituted a suitable investment for two of his clients, given their

financial and personal circumstances and their investment objectives, contrary to IIROC (formerly the IDA) Dealer Member Rules (By-Law) 1300.1(a), (p) and (q); and

(c) Between January 20, 2006 and April 30, 2009, Mr. Lavoie engaged in an outside business activity without the knowledge of the IIROC Dealer Member with whom he was employed and without the latter's consent, contrary to IIROC (formerly the IDA) Dealer Member Rule (By-Law) 29.1.

The Hearing Panel imposed the following penalties on Mr. Lavoie:

(a) A fine in the amount of $45,000;

(b) A two-year suspension of approval in any capacity with an IIROC-regulated firm;

(c) Strict supervision for 12 months, with monthly reports from his employer, in the event of his re-approval with an IIROC-regulated firm; and

(d) Repeat and pass the Conduct and Practices Handbook Course within six months following his re-approval with an IIROC-regulated firm.

The Hearing Panel also ordered Mr. Lavoie to pay IIROC costs in the amount of $40,000.

Documents related to ongoing IIROC enforcement proceedings - including Reasons and Decisions of Hearing Panels - are posted on the IIROC website as they become available. Click here to search and access all IIROC enforcement documents.

IIROC formally initiated the investigation into Frédéric Lavoie's conduct in May 2011. The violations occurred when Mr. Lavoie was a Registered Representative with the Sainte-Foy branch of Laurentian Bank Securities Inc., an IIROC-regulated firm. Mr. Lavoie is no longer a registrant with an IIROC-regulated firm.

* * *

IIROC is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Created in 2008 through the consolidation of the Investment Dealers Association of Canada and Market Regulation Services Inc., IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets.

IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees

and through setting and enforcing market integrity rules regarding trading activity on Canadian equity marketplaces.

IIROC investigates possible misconduct by its member firms and/or individual registrants. It can bring disciplinary proceedings which may result in penalties including fines, suspensions and permanent bans or terminations for individuals and firms.

All information about disciplinary proceedings relating to current and former member firms is available in the Enforcement section of the IIROC website. Background information regarding the qualifications and disciplinary history, if any, of advisors currently employed by IIROC-regulated firms is available free of charge through the IIROC *AdvisorReport* service. Information on how to make investment dealer, advisor or marketplace-related complaints is available by calling 1 877 442-4322.

– 30 –

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Enforcement Notice
Decision

Please distribute internally to:
Legal and Compliance

Contact:
Jeff Kehoe
Vice President, Enforcement
416 943-6996
jkehoe@iiroc.ca

Elsa Renzella
Director, Enforcement Litigation
416 943-5877
erenzella@iiroc.ca

11-0197
June 29, 2011

IN THE MATTER OF James Charles Dennis – Penalty

Following a disciplinary hearing held on November 23 and 24, 2010, in Toronto, Ontario, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) found that James Charles Dennis was liable of engaging in conduct unbecoming a registered representative for failing to disclose certain outside business activities to his employer and its compliance staff.

The Hearing Panel's Decision and Reasons on Liability, dated January 21, 2011 are available at:
http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=90A402BBDA9E45B1A9958618F38880E6&Language=en

Specifically, the Hearing Panel found that the Respondent failed to disclose to his employer, IPC Securities Corp. certain outside business activities, contrary to IIROC Dealer Member Rule 29.1.

The penalty hearing was held on April 28, 2011. In its written decision, the Hearing Panel imposed the following penalties on Mr. Dennis:

1) The Respondent shall pay a fine in the amount of $321,855.14, which includes an amount of $291,855.14 representing a disgorgement of the net profit earned by the Respondent as a result of engaging in the outside business activity which was

not reported to his employer, as specified in the charges and a further amount of $30,000.00 to reinforce the importance of deterring conduct of this nature.

2) The Respondent shall be required to re-write and pass the examination based on IIROC Conduct and Practices Handbook Course as a condition of being re-engaged as a registered representative/approved person in a business regulated by IIROC.

3) The Respondent shall be subject to strict supervision by his employer for a period of one year from the date of being re-engaged as a registered representative/approved person in a business subject to the regulatory authority of IIROC.

4) The Respondent shall pay part of the costs incurred by IIROC in connection with this proceeding in the amount of $15,000.00.

The Hearing Panel's Decision and Reasons on Penalty, dated June 21, 2011 are available at:
http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=EA4A1C8B602145D6B78A24641F8A5195&Language=en

IIROC formally initiated the investigation into the Respondent's conduct in October 2008. The violations occurred when he was a Registered Representative with the Toronto branch of IPC Securities Corp., an IIROC regulated firm. The Respondent is no longer a registrant with an IIROC regulated firm.

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

NEWS RELEASE

For immediate release

For further information, please contact:
Warren Funt
Vice President, Western Canada
604.331.4750
wfunt@iiroc.ca

Jeff Kehoe
Vice-President, Enforcement
416.943.6996
jkehoe@iiroc.ca

IIROC announces settlement agreement for Todd William Stefiuk

March 22, 2011 (Calgary, AB) – A Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) has accepted a Settlement Agreement, with sanctions, between IIROC staff and Todd William Stefiuk.

In the agreement, Mr. Stefiuk admits his failure to disclose certain outside business activities to his firm and his involvement with clients in what is called an off-book investment violated IIROC rules.

Mr. Stefiuk agrees to a $35,000 fine and to pay $5,000 in costs. Furthermore, as a condition of re-approval in any category, Mr. Stefiuk must successfully complete the Conduct and Practices Handbook examination, and be subject to strict supervision for one year.

Specifically, Mr. Stefiuk admits to conduct unbecoming or detrimental to the public interest, contrary to IIROC Rule 29.1, by:

- Failing to disclose to his firm his outside business activities in approximately eight corporations; and
- Facilitating and participating in the purchase and sale of securities on behalf of 42 investors, 37 of whom were his clients, in a private placement that was not done through his firm.

The violations occurred approximately between March 2006 and October 2008, when he was a Registered Representative with the Calgary branch of MGI Securities Inc., an IIROC-regulated firm. IIROC began its formal investigation into Mr. Stefiuk's conduct on February 19, 2009. He is no longer registered with an IIROC-regulated firm.

* * *

IIROC investigates possible misconduct by its member firms and/or individual registrants. It can bring disciplinary proceedings which may result in penalties including fines, suspensions and permanent bans or terminations for individuals and firms.

All information about disciplinary proceedings relating to current and former member firms is available in the Enforcement section of the IIROC website. Background information regarding the qualifications and disciplinary history, if any, of advisors currently employed by IIROC-regulated firms is available free of charge through the IIROC *AdvisorReport* service. Information on how to make investment dealer, advisor or marketplace-related complaints is available by calling 1.877.442.4322.

IIROC is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Created in 2008 through the consolidation of the Investment Dealers Association of Canada and Market Regulation Services Inc., IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets.

IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees and through setting and enforcing market integrity rules regarding trading activity on Canadian equity marketplaces.

-30-

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Enforcement Notice
Hearing

Please distribute internally to:
Legal and Compliance

Contact:
Warren Funt
Vice President, Western Canada
604-331-4750
wfunt@iiroc.ca

Jeff Kehoe
Vice President, Enforcement
416.943.6996
jkehoe@iiroc.ca

10-0221
August 16, 2010

IN THE MATTER OF Malcolm McKimm – Discipline

SUMMARY

NOTICE is hereby given that a hearing, which was scheduled to commence on August 17, 2010 has been postponed and will be held before a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC), on August 19, 2010 at the Calgary TELUS Convention Centre, located at 120-9 Ave SE, Calgary, Alberta, at 10 a.m. or as soon thereafter as possible.

The hearing concerns matters for which the Respondent may be disciplined as a Regulated Person of IIROC pursuant to Part 10 of IIROC Dealer Member Rule 20. The substantive allegations against the Respondent are that from 2002 to 2007, he engaged in outside business activities without the prior knowledge or consent of his Member firm, contrary to IDA By-law 29.1 and Dealer Member Rule 29.1.

IIROC formally initiated the investigation into the Respondent's conduct on January 29, 2008. The violations occurred when the Respondent was a Registered Representative with the Red Deer, Alberta sub-branch of Wolverton Securities Ltd. The Respondent is not currently registered with an IIROC regulated firm.

The Hearing Panel's decision and reasons will be made available to the public.

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

NOTICE/NEWS RELEASE

For immediate release

Enforcement Notice
Decision
12-0053

For further information, please contact:

Enforcement Contact:

Carmen Crépin
Vice President, Québec
514 878-2854
ccrepin@iiroc.ca

Media Contact:

David Thomas
Director, Public Affairs
416 943-6921
dthomas@iiroc.ca

IN THE MATTER OF Konstantine Dariotis and Alfonso Fiumidinisi – Settlement Accepted

February 13, 2012 (Montreal, Quebec) - On January 25th, 2012, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) accepted a Settlement Agreement between IIROC staff and Mr. Konstantine Dariotis and Mr. Alfonso Fiumidinisi.

Mr. Dariotis and Mr. Fiumidinisi admitted that they engaged in outside business activities without proper disclosure and authorization from their employer.

Specifically, Mr. Dariotis and Mr. Fiumidinisi admitted to the following violation:

(a) During the approximate period between 1991 and 2005, Mr. Dariotis and Mr. Fiumidinisi engaged in outside business activities without proper disclosure and authorization from their Dealer Member employer by:

   a) referring individuals including clients of its Dealer Member employer to offshore banks;

   b) obtaining and acting upon trading authority over most of these offshore accounts; and

   c) facilitating these individuals to invest in offshore funds for which Mr. Dariotis and Mr. Fiumidinisi had an interest to earn fees and commissions.

   all of which is business conduct that is unbecoming or detrimental to the public interest, contrary to IDA By-law 29.1 (now Dealer Member Rule 29.1).

Pursuant to the Settlement Agreement, Mr. Dariotis and Mr. Fiumidinisi agreed to the following penalties:

(a) To pay to IIROC a total fine in the amount of $350,000; and

(b) To each be suspended from any registered capacity with IIROC for a period of 2 months, to be served consecutively;

Mr. Dariotis and Mr. Fiumidinisi also agreed to pay costs to IIROC in the amount of $50,000.

The Settlement Agreement and the panel's decision dated January 25th, 2012, are available at http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=78CE4D35727747B3B0C16F751D50F13A&Language=en. Documents related to ongoing IIROC enforcement proceedings – including Reasons and Decisions of Hearing Panels – are posted on the IIROC website as they become available. Click here to search and access all IIROC enforcement documents.

IIROC formally initiated the investigation into Mr. Dariotis and Mr. Fiumidinisi's conduct in November 2006. The conduct occurred when Mr. Dariotis and Mr. Fiumidinisi were Registered Representative with the Montréal branch of RBC Dominion Securities Inc., an IIROC-regulated firm. Mr. Dariotis and Mr. Fiumidinisi are now employed with CIBC World Markets Inc. an IIROC-regulated firm.

* * *

IIROC is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Created in 2008 through the consolidation of the Investment Dealers Association of Canada and Market Regulation Services Inc., IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets.

IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees and through setting and enforcing market integrity rules regarding trading activity on Canadian equity marketplaces.

IIROC investigates possible misconduct by its member firms and/or individual registrants. It can bring disciplinary proceedings which may result in penalties including fines, suspensions, permanent bars, expulsion from membership, or termination of rights and privileges for individuals and firms.

All information about disciplinary proceedings relating to current and former member firms is available in the Enforcement section of the IIROC website. Background information regarding

the qualifications and disciplinary history, if any, of advisors currently employed by IIROC-regulated firms is available free of charge through the IIROC *AdvisorReport* service. Information on how to make investment dealer, advisor or marketplace-related complaints is available by calling 1.877.442.4322.

-30-

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Enforcement Notice
Decision

Please distribute internally to:
Legal and Compliance

Contact:
Warren Funt
Vice President, Western Canada
604-331-4750
wfunt@iiroc.ca

Jeff Kehoe
Vice President, Enforcement
416.943.6996
jkehoe@iiroc.ca

10-0240
September 8, 2010

IN THE MATTER OF Malcolm Joseph McKimm – Settlement

SUMMARY

On August 19, 2010, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) accepted a Settlement Agreement between IIROC Staff and Malcolm McKimm.

Mr. McKimm admitted that from 2002 to 2007 he conducted his business in a manner that is unbecoming or detrimental to the public interest contrary to IDA (now part of IIROC) Rules. Mr. McKimm agreed that he provided business advice and consultation to certain business acquaintances, friends and clients while, at times, receiving compensation for his services. All of this business activity was without the prior knowledge or consent of his Member firm employer.

Pursuant to the Settlement Agreement, Mr. McKimm agreed to a fine of $50,000 and payment of costs of $5,000.

In the agreement, Mr. McKimm admitted to the following misconduct:

From 2002 to 2007, inclusive, Mr. McKimm engaged in outside business activities without the prior knowledge or consent of his Member firm, contrary to IDA By-law 29.1 and Dealer Member Rule 29.1.

IIROC formally initiated the investigation into the Respondent's conduct on January 29, 2008. The violations occurred when the Respondent was a Registered Representative with the Red Deer, Alberta sub-branch of Wolverton Securities Ltd., an IDA regulated-firm. The Respondent is not currently registered with an IIROC-regulated firm.

The Hearing Panel issued its Reasons and Decision on August 30, 2010. The Settlement Agreement and the Hearing Panel's Decision and Reasons are available at

http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=611D01765DEC401994E604D798527967&Language=en

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Enforcement Notice
Decision

Please distribute internally to:
Legal and Compliance

Contact:
Alex Popovic
Vice President - Enforcement
416.943.6904
apopovic@iiroc.ca

Jeff Kehoe
Director, Enforcement Litigation
416.943.6996
jkehoe@iiroc.ca

09-0025
January 28, 2009

IN THE MATTER OF Acadian Securities Inc. – Settlement

SUMMARY

On January 16, 2009, in Halifax, Nova Scotia, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) accepted a Settlement Agreement between IIROC Staff and Acadian Securities Inc. (the "Respondent"). Pursuant to the Settlement Agreement, the Respondent admitted that:

(a) From April 21, 1996, the Respondent failed to implement proper controls to ensure complete identification of any related or connected issuers and written monitoring of outside business activities of certain registered representatives, officers and directors, in compliance with IIROC Rules 29.1, 17.2, 17.2A and Regulation 200.1.

Pursuant to the Settlement Agreement, the Hearing Panel imposed the following penalty against the Respondent:

(a) The Respondent has engaged a Consultant, acceptable to IIROC, to review and evaluate the Respondent's policies and procedures and make recommendations to the Board of the Respondent. The Consultant has made a report to the Respondent and IIROC on the findings and the recommendations made to the Respondent's Board;

(b) The Respondent will pay a global fine in the amount of the $100,000; and

(c) The Respondent shall pay the full costs of engaging the Consultant, as described above in (a).

IIROC formally initiated the investigation into the Respondent's conduct on or about August 29, 2007. The violations occurred when the Respondent was a Member of the IDA. The Respondent is currently a Dealer Member of IIROC.

The Hearing Panel's Decision and Reasons is available at:
http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=59A72457D8984A26BB8B1DF2DCF67053&Language=en .

The Settlement Agreement is available at:
http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=D2309F03068A4A45B52EFD7A7A263C51&Language=en .

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Enforcement Notice
Decision

Please distribute internally to:
Legal and Compliance

Contact:

Carmen Crépin
Vice-President, Québec
514 878-1625
ccrepin@iiroc.ca

Jeff Kehoe
Director, Enforcement Litigation
416 943-6996
jkehoe@iiroc.ca

08-0043
July 22, 2008

IN THE MATTER OF STÉPHANE RAIL – DISCIPLINE

SUMMARY

Following a disciplinary hearing held on January 15, 16 and 18 and March 4, 5 and 6, 2008, in Montréal (Québec), a Hearing Panel of the Investment Dealers Association of Canada (IDA), by a majority decision, has found Stéphane Rail (the Respondent) guilty on Count 1 a) as alleged, namely that, in 2000, while employed as a Registered Representative of TD Securities Inc. (hereinafter, TD), he engaged in conduct unbecoming or detrimental to the public interest when he engaged in outside business activities without the consent and without the knowledge of his firm, by introducing one of his clients, HC, to another of his clients, LV, with the aim of facilitating the obtaining of a loan for LV, knowing that his firm had already determined that this loan was too risky and that such behaviour was not consistent with his responsibilities as a registered representative, contrary to Association By-law 29.1;

The Hearing Panel does not uphold Count 1 b), which alleged that Stéphane Rail engaged in conduct unbecoming or detrimental to the public interest, when he engaged in outside business activities without the consent and without the knowledge of his firm, by introducing the owners of P. Inc., PP, DP and RG, to his current client, LV, in order to propose a financial solution to benefit LV, for an amount of $1,000,000, without the consent and without the

knowledge of the firm and knowing that such behaviour was not consistent with his responsibilities as a registered representative.

The Hearing Panel has found Stéphane Rail guilty on counts 2 and 3 of the Notice of Hearing, as alleged, which read as follows:

2. In the year 2000, the Respondent, while employed with TD as a registered representative, made inappropriate use of personal and confidential information regarding two clients, HC and LV, by introducing them to one another in order to facilitate a financing project to benefit LV, thereby engaging in conduct unbecoming and detrimental to the public interest, contrary to IDA By-law 29.1;

3. On or about September 18, 2000, while employed with TD as a registered representative, the Respondent failed to use due diligence to make sure that the cheque made by P. Inc., dated September 14, 2000, in the amount of $333,000 and payable to COC, was properly invested in the account belonging to COC, thereby engaging in conduct unbecoming and detrimental to the public interest, contrary to IDA By-law 29.1;

When the hearing resumed on March 4, 2008, Stéphane Rail entered a guilty plea on counts 4, 5 and 6, acceptance of which plea has been confirmed by the decision of the Hearing Panel. These three counts read as follows:

4. In June and July 2000, the Respondent, while employed with TD as a registered representative, failed to use due diligence and engaged in conduct unbecoming and detrimental to the public interest, by creating an investors group, to which he belonged, for the purpose of investing over $150,000, when he knew or should have known, as a registered representative, that this stratagem constituted a means of illegally taking advantage of the provisions concerning the prospectus exemption stipulated in section 51 of the Québec Securities Act, contrary to IDA By-law 29.1;

5. On or about June 22, 2000, while employed with TD as a registered representative, the Respondent engaged in conduct unbecoming and contrary to the public interest, by depositing in a personal capacity an amount of $48,112 in the account of his client RS, for the purpose of making a private investment, contrary to IDA By-law 29.1;

6. On or about July 18, 2000, the Respondent, while employed with TD as a registered representative, engaged in conduct unbecoming and contrary to the public interest, by depositing in a personal capacity an amount of $35,000 in the account of his client RS, contrary to IDA By-law 29.1.

As for count 7, the Hearing Panel does not uphold Stéphane Rail's guilt. This count alleged that Mr. Rail, on or about October 30, 2000 and on or about March 1, 2001, while employed

as a registered representative with TD, engaged in conduct unbecoming and contrary to the public interest, when he used TD letterhead without the latter's consent and without its knowledge, allowing P. Inc. and its shareholders to believe that they were doing business with the firm, whereas it [P. Inc.] was never a client of the firm, contrary to IDA By-law 29.1.

The IDA had formally launched an investigation into the conduct of Stéphane Rail on June 22, 2005. The misconduct occurred while Stéphane Rail was employed as a registered representative at the Ste-Foy, Québec branch of TD Securities Inc. Since 2002, Mr. Rail has worked as a branch manager with Canaccord Capital Inc., suite 2940, 2600 Laurier Blvd., Ste-Foy, G1V 4M6.

The parties shall be summoned to a penalty hearing, on a date to be determined by the National Hearing Coordinator, in order to hear their representations regarding penalties. The decision and reasons of the Hearing Panel may be viewed at http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=B17C7EBCF6BE47C9B1FE4FDBB58EA177&Language=en.

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

NOTICE / NEWS RELEASE

For immediate release

Enforcement Notice
Decision
12-0133

For further information, please contact:

Enforcement Contact:

Jeffrey Kehoe
Vice President, Enforcement
416 943-6996
jkehoe@iiroc.ca

Media Contact:

David Thomas
Director, Public Affairs
416 943-6921
dthomas@iiroc.ca

IN THE MATTER OF Sandy Joseph Bortolin – Discipline decision – Liability and Penalty

April 13, 2012 (Toronto, Ontario) — Following a disciplinary hearing held February 28, 29 and March 1, 2012, a Hearing Panel of the Investment Industry Regulatory Organization of Canada (IIROC) found Sandy Joseph Bortolin liable for breach of IIROC Dealer Member Rule 29.1 in conducting undisclosed off-shore business activities, engaging in personal financial dealings with clients, facilitating suspicious transactions including insider trading and engaging in money laundering, and misleading IIROC staff in their investigation of his activities.

The panel's decision, dated March 15, 2012, is available at
http://docs.iiroc.ca/DisplayDocument.aspx?DocumentID=4304F2A18D06463F8394B283A403E2F2&Language=en
Documents related to ongoing IIROC enforcement proceedings – including Reasons and Decisions of Hearing Panels – are posted on the IIROC website as they become available. Click here to search and access all IIROC enforcement documents.

Specifically, the panel found Mr. Bortolin contravened IDA By-law 29.1 and IIROC Dealer Member Rule 29.1 by committing following violations:

From as early as 2003 and continuing until 2008, Mr. Bortolin:

(a) carried on outside business activities without the knowledge or approval of his member firm;
(b) engaged in personal financial dealings with his clients without the knowledge or approval of his member firm;
(c) facilitated suspicious transactions; and

(d) misled IIROC staff in their investigation of his activities, hampering the investigation.

The Hearing Panel imposed the following penalty on Mr. Bortolin:

(a) a permanent prohibition from registration with IIROC; and
(b) a $500,000 fine.

Mr. Bortolin is also required to pay costs in the amount of $100,000.

IIROC formally initiated the investigation into Mr. Bortolin's conduct in February 2009. The violations occurred when he was a Registered Representative with the Toronto branch of BMO Nesbitt Burns Inc., an IIROC-regulated firm. Mr. Bortolin is no longer a registrant with an IIROC-regulated firm.

* * *

IIROC is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. Created in 2008 through the consolidation of the Investment Dealers Association of Canada and Market Regulation Services Inc., IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets.

IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees and through setting and enforcing market integrity rules regarding trading activity on Canadian equity marketplaces.

IIROC investigates possible misconduct by its member firms and/or individual registrants. It can bring disciplinary proceedings which may result in penalties including fines, suspensions, permanent bars, expulsion from membership, or termination of rights and privileges for individuals and firms.

All information about disciplinary proceedings relating to current and former member firms is available in the Enforcement section of the IIROC website. Background information regarding the qualifications and disciplinary history, if any, of advisors currently employed by IIROC-regulated firms is available free of charge through the IIROC *AdvisorReport* service. Information on how to make investment dealer, advisor or marketplace-related complaints is available by calling 1.877.442.4322.

Ontario Securities Commission | Commission des valeurs mobilières de l'Ontario | P.O. Box 55, 19th Floor, 20 Queen Street West, Toronto ON M5H 3S8 | CP 55, 19e étage, 20, rue queen ouest, Toronto ON M5H 3S8

IN THE MATTER OF THE *SECURITIES ACT*
R.S.O. 1990, c.S.5, AS AMENDED

- AND -

IN THE MATTER OF
MRS SCIENCES INC. (FORMERLY MORNINGSIDE CAPITAL CORP.), AMERICO DEROSA, RONALD SHERMAN, EDWARD EMMONS, IVAN CAVRIC AND PRIMEQUEST CAPITAL CORPORATION

REASONS AND DECISION

Hearing:	May 7, 8, 11 and 13, 2009 June 10, 11, 12, 22 and 26, 2009 September 3 and 4, 2009 October 7, 2009	
Decision:	February 2, 2011	
Panel:	Patrick J. LeSage, Q.C. Carol S. Perry	- Commissioner (Chair of the Panel) - Commissioner
Counsel:	Derek Ferris	- for Staff of the Ontario Securities Commission
	Peter-Paul DuVernet	- for MRS Sciences Inc., Americo DeRosa, Ronald Sherman, Edward Emmons, Ivan Cavric, and Primequest Capital Corporation

**IN THE MATTER OF THE SECURITIES ACT,
R.S.O. 1990, c. S.5, AS AMENDED**

- and -

**IN THE MATTER OF
FIRESTAR CAPITAL MANAGEMENT CORP.,
KAMPOSSE FINANCIAL CORP., FIRESTAR INVESTMENT MANAGEMENT
GROUP, MICHAEL CIAVARELLA AND MICHAEL MITTON**

STATEMENT OF ALLEGATIONS
OF STAFF OF THE ONTARIO SECURITIES COMMISSION

Staff of the Ontario Securities Commission make the following allegations:

The Respondents

1. Michael Ciavarella is an individual who resides in the Province of Ontario.

2. Michael Mitton is an individual who resides in British Columbia and/or Ontario. Mitton has been convicted of at least 103 counts of fraud, many of which have involved securities fraud. Mitton and his wife, Janet Mitton, are currently subject to a 20 year cease trade order in British Columbia.

3. Kamposse Financial Corp. ("Kamposse") is a corporation incorporated in Ontario with its head office in Richmond Hill, Ontario.

globeandmail.com

Reorganized crime; Our Mafia and Hells Angels have grown in a nice, co- operative Canadian way. Now, big-time crime is run so much like a business that the boundary between legit and crooked is beginning to blur

globeandmail.com
Fri Sep 26 2008, 6:00am ET
Section: Business
Byline: Bruce Livesey

John Xanthoudakis's introduction to the intimate connection between conventional business and criminal business came in the form of brass knuckles. Late on a Friday afternoon in November, 2005, the investment banker arrived at a law office in Place Ville Marie in downtown Montreal. Xanthoudakis was the former CEO of a $1-billion hedge-fund firm, Norshield Financial Group. It was a dire time for Xanthoudakis: Norshield had collapsed a few months earlier, with more than $400 million of investors' money lost. Even his own palatial house in Laval had been seized.

Xanthoudakis had come to the law firm for a meeting with some investors, who turned out to be three lieutenants of Montreal's notorious Rizzuto crime family. The three men got down to business quickly, demanding Xanthoudakis make good on the $5 million the Rizzutos had apparently lost in Norshield's meltdown.

"We represent a group of people who aren't very happy," the largest of the men told Xanthoudakis. "As a matter of fact, they are very unhappy and their unhappiness makes me very, very unhappy."

To drive home the point, "one guy sneaked behind John and whacked him," relates Montreal businessman William Urseth, a friend of Xanthoudakis's. "There was blood all over the room." The brass knuckles snagged Xanthoudakis just above his right eye, leaving a gash.

There was nothing complicated in the assault-the Rizzutos simply wanted their money back. The incident is unusual only in that it has become public. Countless points of contact exist between the legitimate business world and organized crime. "If you look closely, you will see there are distinctions in the underworld that reflect crudely the distinctions in the upper world," says Diego Gambetta, an Oxford University sociologist and expert on the Mafia. "[The Mafia]wouldn't have lasted 150 years if they had been just a gang of extortionists. They served the interests of various portions of the business world."

The pattern is reflected in the case of the Rizzutos. Led by Nicolò Rizzuto and his son Vito-with Vito acting as CEO and front man, and his father and a close-knit group of top lieutenants functioning as senior management-this crime family began infiltrating the business community decades ago. "These are guys who think globally and make full use of global financial markets," says Lee Lamothe, a Toronto journalist who co-authored a book on the Rizzutos, The Sixth Family. "They use lawyers and sharp accountants, and weaknesses in stock market regulation, and are able to get the money they need to do deals." Today, the Rizzuto leadership is mostly behind bars. Sixty-two-year-old Vito is languishing in a prison in Colorado for participating in the 1981 gangland slaying of three fellow mobsters, while his 84-year-old father and 90 of their street bosses and soldiers were swept up two years ago in an RCMP-led crackdown called Projet Colisée. Facing roughly 1,000 charges for drug importing, extortion, gangsterism and bookmaking, the Rizzuto gang are slated to go to trial this fall.

The trial, if it proceeds, will inevitably underline how organized crime can simply be commerce of a different hue, involving the same sorts of challenges with personnel and competition that legitimate businesses face. Carlo Morselli, a criminologist at the Université de Montréal, believes that successful gangsters require exceptional business skills. They work on a tightrope of alternately competing against, and working with, their rivals, while agreeing to deals that can't be enforced by law. Not to mention risking everything at the hands of the police. "The only difference between them and real businessmen is there's no room for error," says Pierre Boucher, a lieutenant with the Sûreté du Québec who has investigated organized crime for many years. Actually, there's one other difference. "You can kill your competition."

More important than the resemblance between the two spheres is the way the border between the two is blurring. While dollar sums are impossible to compile, police sources and other evidence suggest organized crime is growing in Canada, and increasingly bleeding into the legitimate economy. The old stereotypes of greasy goombahs and bikers is being supplanted by profit-minded professionals with top legal help. And Canada, with its porous borders, proximity to the U.S. market, and light sentences for criminal activity, is considered by police to be a haven for organized crime.

Internationally, annual revenues generated by organized crime exceed $800 billion (U.S.)-up dramatically from $595 billion (U.S.) in 2001-according to estimates by Friedrich Schneider, an economist at the Johannes Kepler University of Linz in Austria. Estimates of the portion of the GDP controlled by organized crime reach as high as 13.1% in Italy and, startlingly, 11% in the U.S. As for Canada, the International Monetary Fund suggests that money laundering alone accounts for between 2% to 5% of GDP-or somewhere between $30 billion and $77 billion. Nationwide narcotics sales may be as high as $40 billion a year-as much as our domestic mining production-or even higher. In B.C. , as much as 5% of GDP is estimated to stem from marijuana production.

So why is organized crime prospering? "It's because of income distribution" and the potential for easy money, says Schneider, who observes that the growing chasm between rich and poor is driving the world's indigent toward crime out of necessity. In countries like Colombia, Mexico, Russia, Brazil and Italy, criminal syndicates and drug cartels control swaths of both the real economy and the state, creating, in extreme cases like Colombia, anarchic narco-nations.

Another factor may be the celebration of bikers and mobsters in North American popular culture. Canada, however, is different from the U.S. Our criminals are often less inclined to violence, and more toward co-operation with their rivals.

Money made in the criminal milieu travels various paths. But the general pattern in narcotics-the bedrock criminal commodity-begins with importers, who supply networks of distributors. The money earned by the importers and retailers then flows to bankers and lawyers who launder the loot in the mainstream economy.

The Rizzuto organization extends across Canada, into the U.S. and as afar afield as Latin America, Italy and the banking havens of Switzerland and Liechtenstein. "These guys are so sophisticated it's unfuckingbelievable!" exclaims Salvatore (Big Sal) Miciotta, a former capo and hitman with the Colombos, one of New York's five Mafia families. "Because you're talking about big, big, gigantic money here..They have the gross income of small countries. They are able to sway bond markets, that's how big they are."

While Miciotta may be exaggerating their wealth and ability to influence markets, it's undeniable the Rizzutos created an awe-inducing cash machine. Police say their bookmaking operations in Montreal, Toronto and Ottawa alone did from $500 million to $1 billion in business in one 11-month period in 2005. And that, of course, is only a sideline to the narcotics business. The family is so affluent that Italian authorities claim that in 2005 the Rizzutos were assembling a consortium for the purpose of laundering money via a $7-billion bridge that was to join Sicily to mainland Italy (the money would likely have been laundered through construction companies).

"Vito was involved in everything," says André Cedilot, a veteran journalist at La Presse in Montreal who has followed the Rizzutos' fortunes for years. "He's a co-ordinator, a referee..He received a commission for everything."

Before his incarceration, Vito Rizzuto's days were spent doing what other businessmen do-taking meetings. He tended to get up late at his Tudor-style mansion located on "Mafia row," a secluded street on the north side of the Island of Montreal. It was grand accommodation for someone who was registered for a time as an employee of a funeral home, and later on as a vice-president of a construction company that had sales of all of $34,032 in 2003. Vito's father, Nicolò, who lived two doors down, was officially a pensioner living off $26,574 worth of old-age security and investment income, although he had a condominium in Milan, $5.2 million in Swiss bank accounts, an estimated $1.8 million in blue-chip stocks, and a 1987 Jaguar XJ12 and a 2001 Mercedes E430 in his driveway.

Upon leaving home, Vito would always be on the move (he maintained a Lincoln, a Mercedes-Benz, a Jaguar and more than one Corvette). Often he headed to one of the better golf courses in the area to meet colleagues. Otherwise, he visited cafés, restaurants, nightclubs and bars. A favourite spot was the quiet corner of a raucous nightclub. Vito spoke to people individually, mouths pressed close to ears, his bodyguard Lorenzo Giordano keeping watch on who was coming and going.

These meetings had many purposes, but importing drugs was the key one. A typical deal might involve ordering a

shipment of cocaine into Canada through Rizzuto's Colombian contacts. "He was the only one who had those type of connections," says Normand Brisebois, a former debt collector and the bodyguard of one of Vito's mistresses. Rizzuto might meet with members of the West End Gang-which controlled the passage of drugs through Montreal's port-or the Hells Angels, to see if they were interested in investing in his shipment. "They would make a joint venture," says Cédilot.

A document filed in court describes how the business allegedly worked. Once an order was made, the drugs would be sent from Colombia to a country like Haiti or Jamaica. From there, the Rizzutos would arrange importation via the Pierre Elliott Trudeau International Airport in Montreal. At each point in the process, the legitimate economy had to be twisted to the drug trade's purposes. The Rizzutos' contacts in Jamaica would hide the drugs in containers or baggage with secret compartments, or in the ceilings of planes. Or couriers would bring it in for $500 per kilo. Having corrupted airline employees, baggage handlers, customs officials and staff of transport companies working at the Montreal airport, the Rizzutos knew drugs would arrive and be delivered safely.

Like mainstream business, crime is globalized. Central to their success as importers were the Rizzutos' international connections. They worked with both the Sicilian and Calabrian Mafias, the Caruana-Cuntrera crime syndicate (which branched out from Sicily to Canada and South America), Colombian drug cartels and the five Mafia families of New York, in particular the Bonannos and Gambinos. These relationships were exposed last October when Italian authorities announced they'd uncovered a money-laundering and drug-smuggling scheme involving a Rome-based company called Made in Italy Inc. Ostensibly a company that was promoting Italian wares internationally, Made in Italy was headquartered across the Rome street from where the Italian cabinet meets; the head of the company had political ambitions. The Italian police claim Made in Italy is a front for laundering $600 million in drug profits through Swiss bank accounts. Vito Rizzuto was caught on wiretaps from his U.S. prison cell talking to the head of Made in Italy, which was shipping cocaine from Venezuela to Canada and then on to Italy. In total, 19 people, including bankers, stockbrokers and other businesspeople who helped with laundering cash, were arrested. Two bank workers in the Veneto area in northern Italy were allegedly responsible for depositing huge quantities of drug money into two Swiss bank accounts.

As the case of Norshield showed, the Rizzutos' contacts in the business world were widespread.

> In the '80s, Vito controlled Penway Explorers Ltd., a junior resource company listed on the Alberta Stock Exchange that was used in a pump-and-dump scam. Vito was forced to pay a hefty tax bill on his profits of $1.4 million from Penway.

> When Vito was arrested for impaired driving in 2002, he was behind the wheel of a Jeep Grand Cherokee that belonged to the director of the Quebec division of OMG Media Inc. OMG was an Ontario garbage recycling company that, after extensive lobbying, landed a contract with Toronto city council to place advertising-laden recycling bins on city streets.

> Police have tied Rizzuto associates to Financement Malts Inc., a Laval- based loan and mortgage company that police say was the centre of a money laundering web. Police allege that Rizzuto associate Francesco del Balso funnelled money through nine Montreal-area companies, including sports bars, car leasing companies and two supermarkets. A lawyer who represented Malts also sits on the municipality of Laval's executive committee.

Vito Rizzuto's style of business was a striking contrast to flamboyant American mobsters like John Gotti. Rizzuto stayed at the top of Canada's criminal underworld by keeping a low profile, working only with trusted people close to the family, and spreading the wealth around. In the end, he was brought down not by the cleverness of Canadian law enforcement but by the treachery of his American brethren. A leader in the Bonanno family told the FBI that Rizzuto was one of the shooters in the murder of three Bonanno capos in 1981. Vito is now serving a 10-year sentence in an American prison. Still, in spite of Projet Colisée and other setbacks, the clan's enterprises continue to prosper. Says former Colombo hitman Miciotta: "Right now they are in transition mode, to hand it over to a successor, maybe a distant relative-people they feel they can trust."

For importers like the Rizzutos to be successful, they need competent distributors. And no one runs a better network than the Hells Angels, whose Canadian arm has perfected the art of criminal franchising.

Walter Stadnick was a David among the hirsute Goliaths who make up the Hells Angels. Just 5 feet 4 inches tall, "Nurget" rose through the ranks to become the genius behind the Hells Angels' spectacular growth in Canada.

When Stadnick joined the Hells Angels in 1982, the motorcycle gang had just two chapters in Quebec and fewer

than 30 full-patch members. By the time Stadnick was arrested in 2001 for murder and drug trafficking, the organization had metastasized into 36 chapters across Canada and nearly 500 full-patch members. "Stadnick's legacy is a coast-to-coast empire of crime," says Julian Sher, co-author of two books on the gang. The Hells Angels, who boast chapters in 29 countries and 2,500 members globally, have long embraced a franchising model. The leadership meets regularly to discuss how the chain can be expanded.

In Canada, Stadnick was responsible for turning the Hells Angels from a bunch of violent party boys into one of the richest, most powerful and wiliest organized crime groups in North America. The decentralized network of chapters was designed not only to market narcotics but to withstand police efforts to drive them out of business. The long-time head of the organization in Quebec was Maurice (Mom) Boucher. "Mom Boucher was the thug, the Al Capone who was going to barrel his way to the top by shooting people and prison guards," says Sher. "But Stadnick was the one who also had the business plan. Stadnick was the CEO."

Founded in San Bernardino, California, in 1948 as an outlet for war vets seeking thrills, the Hells Angels were originally all about having a good time and occasionally breaking bones for mobsters. But by the '60s, the Hells Angels had discovered the lucrative business of selling drugs to hippies.

The first Hells Angels chapter in Canada was established in Montreal in 1977. In those days, the bikers seemed more interested in killing each other than in building a criminal enterprise. "It was disorganized crime-they made money for themselves in an often clumsy way," says Jerry Langton, author of a 2006 biography of Stadnick, Fallen Angel.

Growing up in Hamilton, Stadnick was a cunning and ambitious youth who became a small-time drug dealer in high school before forming his own short- lived motorcycle gang. Rejected by the local Satan's Choice chapter, he rode to Montreal and showed up at one of the city's two Hells Angels clubs in 1982. Although he did not speak the language of the francophone clubs, he was immediately accepted as a prospect.

Three years later, the Hells Angels' Sorel club president decided to wipe out five members of the Laval chapter who were snorting more cocaine than they were selling. This massacre marked a turning point for the Hells Angels in this country. "The Hells Angels had divided," says Langton. "There were the guys who wanted to have a good time, make a few bucks if possible, get drunk and kick up shit, and there were the new ones who wanted to make money. These were the guys with short hair who didn't have big bellies and some of them didn't even have motorcycles."

Stadnick and Boucher exemplfied this new breed of business-oriented Hells Angel. "[Stadnick]is part of that key cocaine industry that turns the Hells Angels from basically gofer boys of the Mafia into powerbrokers who are sitting down with the Mafia and negotiating the price of cocaine," explains Sher.

In fact, a Hells Angels chapter is a perfect entrepreneurial franchise for criminality. Each autonomous chapter is led by a president who presides over an executive and a collection of usually about 20 full-patch members. No chapter answers to any other-which means that if the police raid one club, the others keep on functioning. A full-patch member is akin to a "made man" in the Mafia- there are many who aspire but only a few who are chosen. They are basically self-employed businessmen, their value to the chapter rooted in their ability to earn money, says the Sûreté du Québec's Pierre Boucher. While full-patch members are entrepreneurs, they "are working toward a main goal collectively," explains Boucher. All full-patch members give a small portion of their profits to the chapter.

A full-patch member runs his own little empire. "Each Hells Angels member can represent 100 people below him," says Boucher. They have access to puppet clubs-less powerful bikers who do the bidding of the Hells Angels, selling and distributing drugs, running strip bars and prostitution rings, and acting as enforcers. Managing all this keeps the Angels busy. "They start their day with meetings and end their day with meetings and go from one meeting to another," says Boucher.

The Hells Angels have long claimed they are a mere motorcycle club. They market their logo on everything from T-shirts and leather jackets to knickknacks. Their members also own real estate, play the stock market and run legitimate companies. In B.C., for example, leading members of the Hells Angels have owned motorcycle stores, apartment buildings, supermarkets, cafés, construction and waste disposal companies, and cellphone and clothing stores. Then there are the businesses that are legal but seamy. Starnet Communications, a B.C. company run by the Hells Angels during the '90s, became a multimillion- dollar porn and online gambling operation. It got start-up funds via a $2.2- million private placement, and at one point was valued at $900 million on paper. Not surprisingly, members of the gang's provincial leadership live in mansions in some of Vancouver's swankier neighbourhoods. Here and elsewhere, the Angels are as intimate with the mainstream Canadian economy as former biker chick Julie Couillard was with the federal cabinet.

When Stadnick became national president in 1988, his plan was to establish chapters across Canada. The Hells Angels had a burgeoning presence in Quebec, Halifax and B.C., but were completely cut out of Ontario and the Prairies, which were controlled by rival biker gangs. Ontario, with its rich drug market, was especially critical for the Angels. Two approaches were available to Stadnick. He could kill his competitors, or woo them. While the Hells Angels in the U.S. and other parts of the world often wipe out rival gangs-a tendency that was shared by Mom Boucher in Quebec-Stadnick chose a Canadian approach: diplomacy. In Ontario, Stadnick's first effort was to persuade the dominant Outlaws and Satan's Choice gangs to join the Angels. He tried to do the same in Winnipeg, an important distribution hub for drugs. "An informant told me that if he could boil down Walter's philosophy to one sentence, it would be: 'He would rather buy his rival a drink than kick his head in.'" says Langton.

Rebuffed, Stadnick got innovative: In Manitoba, he formed the Redliners club in 1995 to compete with the entrenched Los Brovos and Spartans clubs. Two years later, he was victorious; Stadnick merged the Redliners with Los Brovos and the Spartans to form a Hells Angels chapter. By then, he'd already conquered Alberta, where the Angels had been warmly welcomed.

Ontario proved more difficult. Finally, Stadnick had an epiphany. He knew that full-patch members of the Outlaws and Satan's Choice did not relish the prospect of being reduced to junior status if they joined the Hells Angels. They didn't see the point of getting onside. Stadnick's solution was simple: All full-patch members of those clubs would automatically become full-patch members of the Hells Angels. Thus, 179 members of the Outlaws, Para-Dice Riders, Satan's Choice, Lobos, Last Chance and Rock Machine were "patched over" in just one day in December of 2000, giving Stadnick his lock on Ontario. The power and prestige of the Hells Angels brand was part of the appeal to the lower-profile clubs. "If you can't beat them, buy them," says Sher. "That's exactly what he did..It was a brilliant strategy." Stadnick also helped create a narcotics pipeline to feed his growing network of franchises. As the Hells Angels became established in Quebec, they occupied the mid-level drug distribution tier just below the Mafia. Led by Mom Boucher, they aggressively sought more turf in the cocaine market, leading to a war with the rival Rock Machine biker gang that took more than 160 lives.

The Hells Angels created a new corporate structure to profit from and manage their exploding drug business. In 1994, they founded the Nomads, a superchapter that was not bound by territory. "In Quebec, the Nomads were just the toughest and meanest and most powerful," says Sher. An elite circle of five Nomads, called La Table, set prices and managed the drug trade. "Stadnick and his partners were able to build a pyramid structure that put the Nomads on top of all the other clubs," says Sher, "which you don't see anywhere else. And La Table was a powerful clique, which is why they amassed such huge fortunes."

The Nomads ordered cocaine and hashish shipments and then demanded that all Hells Angels clubs in Quebec buy product only from them. In 2000, La Table had so much clout that it arranged a meeting with Vito Rizzuto at a Montreal restaurant to set the price of a kilo of cocaine at $50,000 and divide up the city's market.

Police got an inkling of just how much money the Nomads were making when, in 2000, they discovered the gang had set up their own bank in a series of apartments in Montreal. Here, cash from drug deals was delivered, counted and stored. Records from the bank show that between March 30, 1999, and December 19, 2000, the Nomads sold $111.5 million worth of cocaine and hashish. Stadnick and one of his Hells Angels buddies had an account code-named "Gertrude," through which the two men bought 267 kilos of cocaine and 173 kilos of hashish from the Nomads, worth $11.1 million, during an 11-month period. Police estimate the duo's profits were between $2 million and $3 million.

But Stadnick's days at the top were coming to an end. Just as his plan for a national chain was realized, he was arrested in March, 2001, as part of Operation Printemps, which took down the Quebec leadership of the Hells Angels. He was charged with drug trafficking and conspiring to commit more than a dozen murders, eventually receiving a 20-year sentence, less double time served.

His network remains very much intact. "Part of Walter's genius is he went to parts of Canada where the Mafia didn't exist," observes Langton. "There is no Mafia in Thunder Bay-but there are bikers. Same as Saskatoon and North Battleford. And you know what? People there want drugs, too."

As criminal organizations like the Hells Angels have grown more skilled at making mountains of money, they increasingly need the services of bankers, accountants and lawyers to help launder their ill-gotten gains. Given the sums involved, they never lack for willing recruits.

Cal Broeker is a gregarious American, a bear of a man with a profane patter that served him well when he infiltrated the criminal netherworld as an undercover operative for the RCMP and the U.S. Secret Service. In 1997, Broeker

began getting close to the Rizzutos, claiming to be a money launderer with ties to Eastern European banks. He once had coffee with Vito Rizzuto in a restaurant in Montreal's Little Italy to talk business. "They wanted me to handle the money laundering for the Hells Angels," recalls Broeker. "The Hells were using [the Rizzutos]to launder their cash. The volume was huge. I had an airtight plan located out of Bulgaria....These guys were freaking over it. The Rizzutos offered me all of the money laundering for the Hells."

The deal never happened, but Broeker gained insight into the white-collar end of organized crime. "When we say 'Mafia,' you think of so many images-least of them is a bank manager with a plastic penholder and round glasses and a short haircut," he says. "But he is as lethal as any enforcer or hitman as far as what he can accomplish for the gangs."

Broeker says the Rizzutos laundered money through an extensive network that one of the family's enforcers told him even included one of the Big Three auto companies in Detroit, thanks to a corrupt contact. "They would send cash along with a false invoice to this contact in Detroit who would put the money through one of the company's divisions," explains Broeker. "In turn, the contact would issue a cheque to the Rizzutos, claiming the payment was for something like car parts when, in fact, it was for this dirty money needing laundering."

Criminals can take a variety of routes into the financial system. The white- collar professionals they employ include lawyers, accountants, stockbrokers, insurance agents, real estate agents and staff at financial institutions and car dealerships. "Within the criminal milieu, money laundering has taken on a life of its own and has become an integral component in the operations of criminal organizations," York University criminologist Margaret Beare has written. "A distinct criminal career has opened up to provide laundering services."

Police forces say Canada is a haven for money laundering, thanks in part to a crazy-quilt regulatory system and a banking industry whose priorities are elsewhere. Take the case of the 'Ndrangheta, the powerful Mafia from Calabria that has annual revenues estimated at $68 billion. Italian magistrates, like Alberto Cisterna of the Anti-Mafia Directorate, say the 'Ndrangheta launders drug profits through Canadian banks and companies (as well as through restaurants, franchises and travel agencies), and even pays for its cocaine shipments from Colombia via its Canadian division. Yet few Canadians have ever heard of the 'Ndrangheta.

Not long ago, money laundering simply involved corrupting a few bank branch officers. In the '80s, the police found that the Rizzuto and Caruana-Cuntrera families laundered at least $35 million (U.S.) through Montreal's City and District Savings Bank (now Laurentian Bank of Canada) and two other financial institutions in exactly this fashion. But this method is no longer as viable, given laws governing the deposit of large amounts of paper money in banks.

The launderers have become more inventive, as was demonstrated by Bermuda Short, a joint FBI-RCMP sting operation. One of the targets was Martin Chambers, an Oxford-educated lawyer. In 1967, Chambers set up his legal practice in Vancouver. "He was very bright and unusual and almost anti-establishment," says one of his peers in the Vancouver bar. Chambers also had a toxic streak in his personality that was eventually accentuated by a cocaine habit.

Canadian lawyers like Chambers have long been favourites of mobsters, especially for money laundering, mainly because they can move cash through trust accounts with little scrutiny by the banks. "If I were a criminal," observes one former RCMP officer, "I would want to become a lawyer." A 2004 study by criminologist Stephen Schneider of York University found that of 149 major money-laundering and proceeds-of-crimes cases the RCMP solved in a five-year period in the '90s, lawyers played a role in half of them, albeit often unwittingly. That lawyers in Canada can set up opaque trust accounts for clients is unusual by global standards. Regulations introduced by the federal government to close this loophole in 2000 were met with lawsuits from the legal profession, which was concerned that the changes would undermine the bedrock principle of solicitor-client privilege. The courts ruled in the lawyers' favour.

Chambers had a history of trouble: In 1981, for instance, he was charged for his role in a conspiracy to import a kilo of cocaine from Miami to Vancouver. He was convicted, but fought the case all the way to the Supreme Court of Canada. He won, but was forced to quit practising law (he was never disbarred per se).

Chambers also tried to help a motorcycle gang named Satan's Angels incorporate their chapters and set up their holding companies. In 1993, he assumed a behind-the-scenes role in a publicly traded company, Marlat Resources Ltd., one of whose principals was allegedly linked to the Russian Mafia. Chambers also became involved in a cigarette smuggling scheme, and borrowed money from Eron Mortgage Corp., a Vancouver mortgage-brokering firm that raised $200 million from B.C. investors in the mid-'90s before going bust amid charges of fraud.

One of Chambers's acquaintances was a Vancouver stock promoter, Jack Purdy. By the late '90s, Purdy had piqued the curiosity of both the RCMP and FBI, who believed he was in cahoots with mobsters. Accordingly, in 1999, the Bermuda Short team assigned veteran RCMP undercover officer Bill Majcher to represent a fictitious Colombian cartel that had bags of cash to launder-up to $2 million a day. The sting was set up in Florida.

Soon enough, Majcher came to the attention of Purdy and his colleague, Kevan Garner, who together ran Garner Purdy Venture Capital, a Vancouver stock promoter. In early 2002, Garner flew to Fort Lauderdale and met with Majcher. Majcher made it clear he had drug profits to wash. Garner returned to Vancouver, then flew back to Florida, where he picked up a "damned big" bag stuffed with $500,000 (U.S.). He laundered some of the money by buying a shell company.

By laundering on the stock market, criminals can increase their profits many times over. "We used to say dumb ones make millions, the semi-smart ones make tens of millions, and the really crafty make hundreds of millions," says Ross Gaffney, a former FBI agent who oversaw Bermuda Short. Using shell companies, criminals can employ pump-and-dump schemes to multiply their wealth. "It's not unheard of to have a stock starting in the pennies and [the promoters]ending up making 40 or 100 times their investment," says Gaffney.

According to testimony given in court, Garner soon returned to Florida, this time with Chambers in tow. In the spring of 2002, Chambers, Garner and Majcher met aboard a boat in Fort Lauderdale's harbour to talk business. Majcher produced a bag containing $500,000 (U.S.), remarking to Chambers that he needed a total of $26 million (U.S.) laundered per year. Chambers quickly agreed to help. Majcher says he next set up a corporation, which was used to open an account at Key West Swiss Investment Bank, based in the Bahamas. The money was then laundered through a casino and a chain of restaurants connected to the bank, as well as through a company of Chambers's called Mystar Holdings, which in turn had an account with the Royal Bank of Canada. "It's called layering-to hide the origins of the money," says Majcher.

Another lawyer ensnared by Bermuda Short was Simon Rosenfeld, a sole practitioner with an office in a handsome brownstone in downtown Toronto. In 2001, Rosenfeld had been convicted and fined $2.8 million (U.S.) by U.S. regulators for operating a pump-and-dump scheme at a company called Synpro Environmental Services Inc. He declared bankruptcy in the wake of that penalty.

In March of 2002, Rosenfeld flew down to Miami to meet with Majcher. According to court testimony, Rosenfeld insisted that any transactions be carried out in Toronto, as he feared the consequences of getting caught in the States. He told Majcher that he'd laundered more than $150 million over the years. "Rosenfeld also explained that in the early '90s, he was a banker in Sicily, and told me about a relationship with the Hells Angels and Vito Rizzuto, " says Majcher.

In June of 2002, Majcher went to Rosenfeld's Toronto office with a bag containing $250,000. He handed Rosenfeld a piece of paper with the number of an account in a bank in Miami. Using a legitimate foreign exchange company in Montreal called Denarius Financial Group, Rosenfeld made three wire transfers to shift the money from Canada to the Miami bank.

In August, 2002, the FBI and RCMP made their move, arresting Purdy, Garner, Chambers, Rosenfeld and more than 50 other alleged launderers, many of whom worked at dodgy brokerages. Of the 58 men arrested, a third were Canadians. In 2003, Chambers received a 15-year sentence. Garner served 15 months in jail and went on to invent a money-laundering board game. A broken man, he apparently took his own life in September of this year. Purdy was acquitted. In 2005, Rosenfeld was given three years in prison and fined $43,230. Five days later, he was released on bail of $1.95 million.

Length: 5505 words
Idnumber: 200809260070

Tone: Negative

THE VANCOUVER SUN

Vancouver promoter implicated in international bribery scandal; Naeem Tyab arranged $2-million payment to wife of Chadian ambassador, according to court document

Vancouver Sun
Sat Feb 2 2013
Page: C2
Section: BusinessBC
Byline: David Baines
Column: David Baines
Source: Vancouver Sun

Vancouver stock promoter Naeem Tyab has found himself at the centre of an international bribery scandal.

According to an agreed statement of facts signed last month by federal Crown prosecutors and Griffiths Energy International Inc., Tyab arranged for the Calgary-based company to pay $2 million to the wife of the Chadian ambassador for "consulting services."

The company also sold four million founder's shares to the ambassador's wife and her nominees for one-tenth of a cent each, for a total of $4,000.

The company has been recently selling its shares for $6 each, which means those four million shares are now worth $24 million.

On Jan. 25, the company pleaded guilty to violating the Corruption of Foreign Public Officials Act and agreed to pay $10.35 million in fines.

Crown prosecutors are trying to recover the cash and shares on grounds that they are proceeds of crime.

The Globe and Mail and the National Post have written lengthy stories about the illicit payments, but have not provided any background information on Tyab, even though the agreed statement of facts indicates he played a central role in the scheme. (It should be noted that Tyab left the company in July 2011, after the events in question. He was not a party to the agreed statement of facts and was not charged with any offence.)

Tyab, 45, has had a long but not-so-illustrious career in the Vancouver securities market. I have written extensively about him.

In 1996, Tyab's brother, Parvez Tyab, incorporated Foresight Capital Corp. and the following year registered it as a securities dealer in B.C.

Naeem Tyab was the firm's principal shareholder and corporate secretary. Naeem's close associate, Gilbert Wong, served as the firm's president and chief executive officer.

In December 1997, B.C. Securities Commission examiners found "significant deficiencies" in the firm's compliance procedures. In particular, they found it was selling risky exempt securities without determining the suitably of those investments for their clients.

Despite repeated warnings, the firm failed to address these deficiencies. Finally, in August 2001, the commission ordered the firm to stop selling exempt securities and ordered Wong to step down as the firm's compliance manager.

In December 2002, the firm - under pressure by BCSC officials - terminated its registration and went out of business, but that didn't end the matter.

In December 2004, BCSC enforcement staff issued a notice of hearing alleging that Foresight, Naeem Tyab and Wong failed to properly supervise client transactions and ensure that its employees complied with securities rules.

For reasons that were never explained, the commission dropped Tyab as a defendant and Wong was later cleared by a BCSC hearing panel on grounds that earlier compliance measures taken by commission staff had effectively dealt with the firm's breaches.

In August 2003, Tyab and Vancouver promoter Larry Kristof suffered the indignity of being accosted by Bellingham detectives while being parked in a rented van at the Bellis Fair Mall.

The detectives found $30,100 in U.S. currency in the vehicle. Tyab and Kristof - as well as Sabir Khan, a cousin of the Tyabs who was on the scene - gave conflicting stories about where the money came from.

The detectives brought in a drug-sniffing dog, which responded positively to the money. Police seized the cash, suspecting that it was the proceeds of drug trafficking. No actual drugs were found.

Khan - who had been arrested on two prior occasions on drug-related matters - later applied to get the money back. The Bellingham city examiner said the evidence established that it was drug money and refused to return it. Nobody was ever charged.

In 2006, Tyab and his brother Parvez, along with Gilbert Wong, reunited in a company called Mogul Energy International Inc., which was based in Seattle and traded on the OTC Bulletin Board in the United States.

Naeem served as Mogul's president, and he and Wong each owned 1.5 million shares. Parvez was the largest shareholder with nine million, or 26 per cent, of its shares.

This is where the narrative in the attempted bribery case picks up.

According to the agreed statement of facts, Naeem and Parvez Tyab - along with late Bay Street financier Brad Griffiths - had been pursuing oil concessions in Chad since mid-2008, first through Mogul and later through Griffiths Energy and Resources Inc.

(Griffiths was known as a smart, colourful and hard-drinking investment executive. During his 30 years on Bay Street, he held senior positions with CIBC, Gordon Capital and Canac-cord Capital, but is best known as a cofounder of Toronto investment dealer Griffiths McBurney Partners.)

According to the agreed statement of facts, Griffiths and Naeem Tyab established contact in 2008 with Chad ambassador Mahamoud Adam Bechir, who arranged an introduction to Chad's minister of petroleum and energy.

In August 2009, the trio incorporated Griffiths Energy to pursue the concessions. Griffiths served as the company's chairman. The head office was initially located in Toronto and later moved to Calgary.

In August 2009, the company prepared a contract agreeing to pay $2 million to a private company, wholly owned by the ambassador, for consulting services.

However, Griffith Energy's outside counsel advised Tyab, who had signed the agreement on behalf of the company, that the ambassador was a government official and could not legally receive a benefit.

The following month, the company drew up a second agreement, with identical terms, except that the named consultant was a company wholly owned by the ambassador's wife, Nouracham Niam. Once again, Tyab signed the agreement on the company's behalf.

The company also sold the ambassador's wife 1.6 million seed shares of Griffiths Energy at one-tenth of a cent each, and another 2.4 million shares at the same price to people nominated by the ambassador's wife, who immediately took steps to transfer 1.6 million of the shares into her personal account.

The agreed statement of fact notes that the shares were among 40 million seed shares sold at one-tenth of a cent during the "founders' seed round."

The following month - in October 2009 - Tyab (on behalf of Griffiths Energy) and the minister of petroleum and energy (on behalf of the government of Chad) signed a memorandum of understanding.

In January 2011, the company finally signed a "production sharing contract" with the Chadian government. Terms included a $40-million US payment to the government. Several days later, the company transferred $2 million into the company account of the ambassador's wife in Washington, D.C., according to the agreed statement of facts.

The Crown did not allege, and the company did not admit, that it actually realized any benefit as a result of the illicit payments.

In July 2011, Griffiths died in a boat accident in Muskoka Lake. That same month, Tyab left the company. New management discovered the payments in question and voluntarily reported the matter to the Crown, RCMP and U.S. law enforcement agencies. They also entered a guilty plea before charges were formally laid.

It was a costly process. The company spent $5 million on lawyers and accountants to investigate the matter. The company also withdrew its planned initial public offering, causing it to write off $1.8 million in attendant expenses. And it agreed to pay $10.35 million in fines.

As of November, Tyab was the second largest shareholder of TSX Venture Exchange-listed Hunter Oil & Gas Corp. (Brad Griffiths' estate is listed as the largest shareholder.)

Tyab is not an officer or director of the company, but in December, his brother Parvez became a director. The company's shares are trading at a mere two cents each.

Tyab is currently serving as chairman of Mogul Energy, whose fortunes have also waned. Despite a five-for-one share consolidation last year, its shares are now trading on the lowly "pink sheets" in the United States at one cent each.

dbaines@vancouversun.com

Illustration:
• Darryl Slade, Postmedia News Files / Bob Sigurdson, Crown prosecutor, and Kris Robidoux, counsel for Griffiths Energy International, outside the Calgary Courthouse Jan. 25. The company was fined $10.35 million on a corruption charge for bribing the ambassador of the African country of Chad regarding production possibilities.

Edition: Final
Story Type: Column
Length: 1268 words
Idnumber: 201302020118

Tone: Neutral
Ad Value: $16,333
Circulation: 185,174

infomart

THE VANCOUVER SUN

Surrey man banned for bogus gold scheme; Securities commission also issues cease-trade order against Bahamian firm

Vancouver Sun
Thu May 24 2012
Page: D3
Section: BusinessBC
Byline: David Baines
Source: Vancouver Sun

The B.C. Securities Commission has permanently banned a Surrey man from the B.C. securities market after he defrauded German and Swiss investors of $1.5 million in a bogus gold futures and foreign-exchange trading scheme.

And in a separate action, the commission issued a cease-trade order against a Bahamian brokerage firm after it traded securities for B.C. residents without being registered in this province.

In the first action, a BCSC hearing panel found that Michael Robert Shantz, who is in his late 20s, set up a dummy office in downtown Vancouver and persuaded 11 European investors to invest $1.53 mil-lion with his company, Canada Pacific Consulting Inc., ostensibly for trading gold futures and foreign exchange currency.

However, instead of investing the money as promised, he wired $1.2 million to bank accounts in Spain and used another $210,000 for personal purposes. Only $18,000 was remitted to investors.

"There is no evidence that Canada Pacific was engaged in any legitimate business," the panel stated.

"Canada Pacific lied to investors, stole their money and took elaborate steps to make the whole scam appear legitimate."

The hearing panel found Shantz had engaged in an illegal distribution of securities and committed fraud. In addition to his market ban, he was ordered to pay to the commission the $1.53 million he obtained as a result of his illegal activity, as well as an administrative penalty of $630,000.

In the second action, a BCSC hearing panel issued a cease-trade order against Gibraltar Global Securities Inc., which is registered as a securities dealer in the Bahamas, for trading and advising in securities in B.C. without being registered here, and for refusing to pro-vide BCSC staff with information relating to B.C. residents who have held accounts with the company.

The panel said BCSC enforcement staff provided evidence that more than two dozen B.C. residents were trading securities through accounts at Gibraltar, and several of those clients have been the subjects of past and ongoing investigations by the BCSC.

The panel also said Gibraltar had opened accounts with Global Securities Corp., a Vancouver-based brokerage firm. Gibraltar had maintained that trading in those accounts was "proprietary and not for the benefit of its clients," but the panel said BCSC staff provided multiple examples where Gibraltar was taking instructions from clients for trading in those accounts, which consisted mainly of shares of TSX Venture Exchange companies.

(The commission earlier issued a freeze order against Gibraltar's accounts at Global, freezing about $2.2 million in cash and securities. That order remains in effect.)

The panel also noted that BCSC staff had asked Gibraltar to provide full details of its B.C. clients and their trading, but the firm had refused. The panel said this refusal rendered Gibraltar "unsuitable to engage in securities related activities in, or connected with, British Columbia."

The Wild West of investing: The biggest financial market you've never heard of

April 2nd, 2012 by Golden Girl Finance

The exempt market is big, unbridled and full of opportunity - but it's not for the faint of heart

If you thought the TSX was the only game in town, you're missing out on a piece of the securities market - a very big piece, as it turns out. Although you may not be familiar with the exempt securities market, at least as much money changes hands here as in the public market.

But while this market provides the high stakes many investors crave, compared to the highly regulated public market, it's a bit of the Wild West. Find out what you need to do to ride this frontier with the hopes of hauling in an investment with blazing potential. But beware: it's not for the inexperienced or the faint of heart.

An investing frontier

Although the exempt securities market has faced stiffer regulation since exempt market dealers (those who sell these securities) came to be regulated by the Canadian Securities Administrators, it still suffers from

limited reporting, low liquidity and higher risk, says Geoff Ritchie, executive director of the Exempt Market Dealers Association of Canada. This is why exempt market dealers must ensure that exempt securities are suitable for the investors who buy them.

This adventure is not for everyone

Just like some of the cowboy-inspired footwear hitting the runway this spring, the exempt securities market isn't the right fit for all investors. Because this market can be risky, investments here are limited to a certain group of investors, namely those who are affluent, savvy and/or able to stomach a wild ride. There are three classes of investors who can buy in (note: rules may vary by province):

- **Accredited Investors:** These are the fat cats of the investing world, including banks, hedge funds and pension funds, as well as high-net-worth individuals. This means investors with $1 million in investable assets, or $5 million in assets, or a before-tax income of at least $200,000. They can invest as much as they want - and they don't have to use a registered dealer.
- **Eligible Investors:** In Alberta, Manitoba, Saskatchewan, Quebec, Prince Edward Island and the Northwest Territories, this type of investor needs at least $400,000 or more in net assets, or an annual net income before taxes of $75,000 for at least two years (or $125,000 with a spouse).
- **Family, Friends and Associates:** If you have a family member or friend who's raising money through the exempt market - or your own company's raising the funds - this can offer a way in (*and* a way to really get to know the investment you're buying).

The good...

The fact that so much money trades over the exempt market isn't happenstance; the exempt market has a lot going for it. This market deals mostly in start-ups, which means that when investors get it right, they'll be holding on to an investment that leaves most others in a cloud of dust. This is because exempt security investors get in so early, they have the opportunity to ride a successful stock all the way to the top. After all, many major Canadian stocks, such as Research in Motion (before its recent challenges), got their start with private funding and went on to produce huge profits for early investors.

Plus, exempt securities tend to be much more focused than those found on the TSX because they represent small companies with limited interests. This means that for investors keen on real estate or resources, for example - two key areas for exempt securities in Canada - this market provides a targeted way to add specific exposure to their portfolios.

Finally, not all exempt market securities are small, back-room deals: many large, public companies also raise money through private issues, providing higher-profile opportunities for exempt market investors.

The bad...

Investors who can stomach exempt securites may ride off with some loot, but compared to typical stocks, this is a relatively unbridled market. Companies can raise equity without being held down by the expensive and cumbersome process required to get onto a stock exchange. This can mean limited access to company

information and reporting for investors. That's why it's so important for investors to do their own due diligence, says Ritchie. This means reading whatever disclosure documents come with the security you're considering and finding out everything you can about the company, its business and its management. Most investors should also make sure they're buying securities through a registered dealer.

The ugly...

Even in the public market, startup companies face a high risk of failure. The exempt market is filled with small, fly-by-night companies whose businesses are untested. If they fail, investors lose. This is especially true with investments structured around projects, Ritchie says, such as a new mining operation.

Lack of liquidity can also be an issue in the exempt securities market, making these strictly buy-and-hold investments. This is because the market is small, and there's no secondary market (i.e. a stock exchange) that allows investors to trade easily with one another. If an investor wants to sell an exempt market security, it can't be done through an online brokerage at the click of a button; it's a process that will take some time. One exception: exempt securities sold by large, public companies may escape this risk. Those shares may become part of the public company's regular, tradable equity, Ritchie says. Exempt securities may also find a sort of secondary market among private equity and venture capital investors. In this case, the size of the company and the sector in which it trades can make a big difference.

New investments, new challenges

It comes down to this: with (careful) risk often comes reward. For those who've been riding the markets successfully for a while, the exempt market can provide new investments with new challenges. Play your cards right, and you may just ride off into the sunset a little bit richer.

Welcome to Canada's exempt market: Exclusive, anything goes investments — but play at your own risk

BARBARA SHECTER | June 15, 2013 7:00 AM ET
More from Barbara Shecter

John Wilson, former senior salesman for First Leaside Group, leaves the Ontario Securities Commission during a hearing about allegations of securities fraud in Toronto on Wednesday, June 5, 2013. Matthew Sherwood for National Post

It's been more than 18 months since Horst Wizemann got news that would wipe out half of his retirement savings — and he's still not sure what happened.

After years of investing his RRSP contributions with bank-owned and independent dealers and insurance companies, he had moved his money — more than a quarter of a million dollars — to a firm that operated in Canada's loosely regulated exempt market. Many investors with enough income or valuable enough assets, or even a big enough lump sum investment, have been drawn to this segment of the capital markets in recent years, often because they could obtain higher

returns than were available from Canada's public markets or government bonds.

But a couple of high-profile blowups in Ontario with nearly half a billion dollars of investor money on the line — and widespread problems uncovered by a recent regulatory sweep of the sector by the Ontario Securities Commission — have raised concerns about the exempt market, even as Canadian regulators consider broadening the profile of investors who qualify to play.

"I am still not sure what really happened," Mr. Wizemann said after watching a day of hearings unfold last week in a fraud case launched by the Ontario Securities Commission against the founder of the First Leaside Group of Companies, the company in which Mr. Wizemann invested along with about 1,000 other Canadians.

"It is a sad story, but it happens all the time," said Mr. Wizemann. "This time, I am in the middle of it."

To be sure, many legitimate firms and dealers operate in this segment of the capital markets.

But there are also cases like First Leaside, which sold real estate limited partnerships, and New Solutions Group, which was in the business of "factoring" receivables, that are keeping regulators busy. Though none of the allegations have been proven in either case, the large dollar amounts of investor money on the line have prompted calls for more scrutiny from groups such as the Foundation for the Advancement of Investor Rights (FAIR).

At its peak, First Leaside had raised $370-million, about $280-million through the sales of proprietary debt and equity securities, and New Solutions had raised more than $200-million. Just last week, the British Columbia Securities Commission accused a former mutual fund salesman of a $65-million fraud involving almost 500 clients with "now worthless" investments in the exempt market.

The OSC sweep of exempt market dealers also exposed

Meltdowns in the Exempt Market

New Solutions Group

Primary Business: Making and administering loans to various businesses, backed by receivables purchased from companies at a discount (factored).

Amount of money raised from investors: About $212-million.

OSC allegations: Ron Ovenden, the 57-year-old "controlling mind" of New Solutions, "misled" or "failed to properly inform investors and potential investors about the true state of affairs of NSFC (New Solutions) and its underlying portfolio."

Expected return to investors from CCAA wind-down: "Gross realization" on securities is 8¢ for every dollar invested.

First Leaside Group of Companies

Primary Business: Purchasing properties in Canada and the U.S. and selling debt and equity securities in real estate limited partnerships and funds.

Assets under management at peak: $370-million, including about $280-million of proprietary First Leaside securities.

OSC Allegations: By failing to disclose a "viability" report, founder David Phillips and former senior salesman John Wilson "engaged or participated in an act, practice or course of conduct relating to securities which he knew, or reasonably ought to have known, would perpetrate a fraud on investors."

Expected Return to investors from CCAA wind-down: About $25-million after repayment of mortgages, but before professional

problems concerning the individuals to whom investments are being sold and how firms collect and track key information about their clients. The exempt market does not require extensive and expensive offering documents and often documentation does not have to pass muster with regulators at all because the firms are supposedly dealing with sophisticated investors who meet minimum investment, income or asset thresholds.

But nearly one-fifth of the dealers reviewed by the OSC in its sweep were selling securities to people who did not fall into the required category of "accredited" investor. And three-quarters of the dealers were found to have "inadequate" processes for collecting, documenting and maintaining information about clients, including their investment objectives and risk tolerance.

The sweep was undertaken after OSC chair Howard Wetston drew attention to the growth of the exempt market, in which capital raising levels had outstripped activity in the public markets, according to the most recent statistics. The regulator says at least $86.5-billion was raised in 2011 alone, the second year in a row of double-digit growth. In a speech last month, Mr. Wetston said the OSC, Canada's largest capital markets regulator, would be "willing to consider the introduction of new tools in the exempt market" — but only if the industry commits to ensuring that investors can be protected.

"In our view, more work needs to be done by the industry to, at minimum, consistently meet existing requirements," Mr. Wetston said.

costs.

Michaels Wealth Management

Primary Business: Advising on the sales of securities to investors.

Amount of money involved: Former mutual funds salesman David Michaels advised 484 clients to purchase over $65-million of "exempt" market securities.

BCSC (B.C. Securities Commission) allegations: Perpetrated a fraud on clients by "repeatedly and falsely claiming that he gave up his registration in 2006 because he foresaw the stock market crash and wanted his clients' money out of the stock market, and omitting to tell the truth that he resigned in the face of an ongoing IDA investigation." Breached securities laws by advising his clients to purchase exempt market securities without being registered to do so.

Expected return to investors: BSCS says "virtually all of the roughly $65-million invested by Michaels' clients is now worthless, leaving many of them financially destitute while their home equity loans remain."

Related

First Leaside before OSC to answer fraud allegations

OSC sweep finds 'substantive' problems in exempt market

Ontario gives OSC new firepower

FAIR lays the blame not only on industry players, but also on the regulators and their "weak"

record in the exempt market.

"Non-compliance with the rules, weak enforcement, and a perception of weak enforcement [including difficulties for investors to obtain recovery of any funds] harms investors and weakens confidence in the exempt market and our capital markets," FAIR said in a submission to the OSC this spring.

FAIR was also critical of regulators' record-keeping on the exempt market, saying that part of the problem is a lack of sufficient data to design effective policy.

"We don't [even] have the statistics to tell us how much fraud there is," says Ermanno Pascutto, executive director of FAIR.

A recent push by proponents of the exempt market to bring even more investors to the party through popular U.S. methods such as crowdfunding — where small investments from a large number of people are pooled — has drawn even sharper criticism from FAIR.

"Crowdfunding, if allowed, will bring Ontarians back to the good 'ol days before modern securities regulation was introduced, a time when promoters would sell 'moose pasture' to naïve consumers," FAIR declared in a newsletter posted to its website on May 30.

That view is countered by groups and individuals who point to the importance of the exempt market for small and medium-sized businesses who have don't have the time, money or expertise to raise money through public markets. They say a few "bad apples" shouldn't spoil the development of this important market segment for the rest.

A "roundtable" organized by the OSC this week to bring players together to discuss crowdfunding drew about 100 people. An informal poll of the group of investors, small business operators and lawyers and other professionals indicated there was widespread interest in allowing more avenues for private investing.

The OSC is compiling the results of a more formal online poll of retail investors and preliminary results indicate that although just over 50% of those who responded indicated no interest in crowdfunding, about 14% expressed "strong" interest. Advocates are urging regulators not to put up

OSC Sweep by the Numbers

• Three-quarters of exempt market dealers had "inadequate" processes for collecting, documenting and maintaining information about clients such as investment

barriers because of the bad experiences of some who have chosen to play in the exempt market.

"It seems every time there's a bad apple in the industry, all the remaining honest and largely compliant players are left to pay the price with yet another regulation," says Stephanie McManus, a principal at Compliance Support Services, an adviser whose clients include those in the financial industry.

She urged regulators "to pause and reflect before overhauling the regulatory landscape yet again" to try to deal with those who flout existing rules. Ms. McManus, who is a lawyer by training and also a board member of the National Exempt Market Association, said the market helps small and medium-sized businesses that account for half the country's GDP to finance their operations "without breaking the bank" on listing fees and other regulatory expenses.

objectives and risk tolerance.

- Nearly 1/5 selling to people who did not fall into the required category of "accredited investor.
- 22% of the dealers made inadequate investment suitability assessments due to inadequate paperwork on how suitability determination is made.
- Two exempt market dealers and one portfolio manager discontinued operations after the regulatory review.
- Regulatory action taken against one exempt market dealer and one portfolio manager.
- "Deficiency" reports issued to 62% of exempt market dealers and portfolio managers in the sweep.

"However," she acknowledged, "the challenge is to ensure that these issuers and the dealers who sell their securities are subject to enough scrutiny by the regulators to keep them on track. It's a difficult balancing act."

Craig Skauge, president of the National Exempt Market Association, says the sector is feeling the impact of the recent regulatory sweep and enforcement actions.

"There are always short-term effects when these types of things come up," he said.

However, he is quick to add that the number of cases where the most serious infractions are alleged is small.

"I'd like to believe that investors and regulators alike are wise enough to not paint an entire industry with the same brush due to a few miscreants," Mr. Skauge said.

He acknowledged that it was "disheartening" to learn that 18% of the players caught in the OSC sweep had "deficiencies" related to who investments were sold to, but he said he is pleased regulators are considering expanding the list of who is qualified to make private investments beyond accredited investors. In Ontario, these well-heeled but not necessarily financially savvy investors must have annual incomes of at least $200,000 and assets, not including a principal residence, of $1-million.

The group is small – less than 4% of the population, according to the OSC.

"While there is no excuse for not following the rules, I can't say that I'm shocked that this [non-compliance] is happening," given that the OSC only allows the products limited to accredited investors to be sold to a tiny percentage of the population, Mr. Skauge said.

Investors outside the "accredited investor" club can still qualify, however, if they have a sizeable minimum investment. And the OSC sweep of 42 exempt market dealers unearthed a troubling trend: some dealers appeared to be encouraging investors who were not accredited to put "a high proportion of their investable assets in a single product" solely to meet that minimum investment threshold.

In the case of Ontario, the minimum investment is $150,000.

UANI Condemns AGF for Maintaining Investments in Fraudulent Bonds that Support Illicit Hizballah and Iranian Activities

741 words
11 September 2012
16:44
Business Wire
BWR
English

NEW YORK--(BUSINESS WIRE)--September 11, 2012--

On Tuesday, United Against Nuclear Iran (UANI) called on Canadian investment firm AGF Management Limited ("AGF") to divest from its Lebanese bonds, and stop supporting the Iranian regime's efforts to circumvent sanctions.

AGF holds fraudulent Lebanese sovereign bonds that support illicit Hizballah and Iranian activities, yet in discussions with UANI AGF has said it will not divest from them, since "there are currently no U.S. or Canadian laws that restrict or prohibit investment in Lebanon."

UANI finds this response to be wholly inadequate in the context of a discussion about fraudulent terror financing, and calls on AGF to immediately reconsider its position.

In a letter to AGF Chairman, President, & CEO Blake Goldring, UANI CEO, Ambassador Mark D. Wallace, wrote:

... UANI is surprised and disappointed to hear your response, especially in the wake of the continuing turmoil in Lebanon and the terrible attack by Hizballah in Bulgaria. I urge you to reconsider this important matter. Determining that there is not currently an explicit legal prohibition on this investment (while nonetheless incorrect) cannot be the end of your inquiry as a fiduciary under U.S., and pursuant to the similar duty of care owed by an investment adviser under Canadian law, and so I recommend that you engage in appropriate diligence with respect to the issues at stake. If you do so, I believe you will realize that, far from being a conflict with your duty to act in your clients' best interest, divesting from Lebanese debt is entirely consistent with (and mandated by) that duty.

As you recall, in our letter we called on AGF to divest from all Lebanese sovereign bond and credit default swaps ("CDS") that it invests in directly, or on behalf of clients or funds, and we showed that the value of these **securities** is based on a massive fraud, one that masks a **money-laundering** operation that not only permits Lebanon to portray a false image of economic stability but also supports terrorism by Hizballah and Iran. I further expressed UANI's belief that Banque du Liban ("BDL") and the Lebanese banking system ("LBS") meet the criteria for determination under Section 311 of the USA PATRIOT Act as a jurisdiction of primary **money laundering** concern that would result in their ban from the U.S. financial system.

UANI believes that divesting from these **securities** is not only the ethical thing to do, but that continuing to hold these **securities**, given what you now know about them, would be a problematic position to take from a compliance and fiduciary perspective, which creates an insupportable level of risk in a variety of areas. Indeed, failure to divest from these **securities** could present an unjustifiable risk to AGF's reputation, its duty to its clients and fund investors, and possibly its efforts to comply with its regulatory obligations.

Firstly, an investment in these **securities** is riskier than it would appear, which does a disservice to you, your clients and investors. Second, your role in facilitating this investment perpetuates an unjustifiable veneer of respectability, masking BDL and LBS's true activities. Finally, because any investment in these **securities** facilitates **money laundering** operations and also shields the true financial health of the Lebanese economy from investors, a facilitating financial institution may subject itself to heightened legal and reputational risks, even with respect to **securities** that, as you note, have not yet been specifically sanctioned by the U.S. or Canadian government authorities. ...

In July, UANI announced the results of a three month-long investigation into the influence of Iran and Hizballah in the Lebanese banking system (LBS) and Lebanon's sovereign bond market, and announced a campaign to compel legitimate financial institutions into divesting from Lebanon's bond market.

UANI has previously announced that Erste-Sparinvest, Eaton Vance, Nord Est Asset Management, Aktia, and Ameriprise Financial have already divested from Lebanese bonds.

Click here to read UANI's full letter to AGF.

Click here to read UANI's June 8, 2012 letter to AGF.

Click here to read the July 3 Wall Street Journal article, "Banks Get Pressed on Beirut."

Click here to view UANI's research, "HIZBALLAH, LEBANON & IRAN: PARTNERS IN A SOVEREIGN **MONEY LAUNDERING** SCHEME."

United Against Nuclear Iran | Nathan Carleton, 212-554-3296 | press@uani.com | SOURCE: United Against Nuclear Iran

Business Wire, Inc.

Document BWR0000020120911e89b000j4

News

Disgraced investment firm ordered to forfeit $15M, pay $750K penalty

PATRICK MALONEY, QMI AGENCY

408 words
12 September 2012
Belleville Intelligencer
BLVLNT
Final
4
English

LONDON -- A disgraced investment firm founder has reached a deal with the province's **securities** watchdog to hand over more than $15 million and pay a $750,000 penalty.

Vincent Ciccone, head of Cambridge, Ont.-based Ciccone Group, had been facing multiple Ontario **Securities** Commission (OSC) charges of fraud and misleading investors out of a total of about $19 million between April 2008 and June 2010.

Ciccone sold shares in a Delaware-based company called Medra, which was presented to investors as specializing in resort real estate development and land buys. But, according to the OSC settlement, Ciccone "misappropriated Medra investor funds and used those funds for purposes completely unrelated to real estate development and land acquisition."

Ciccone admitted his conduct was "contrary to the public interest."

In addition to being forced to "disgorge" of $15.5 million and pay the $750,000 penalty, Ciccone must pay $100,000 to the OSC. He's also permanently banned from trading **securities**.

According to the agreement, Ciccone says he was introduced to Medra by a man who called himself John Gel and stated he was involved in developing time-share properties in Cancun, Mexico. Ciccone says Gel "convinced" him to become Medra's CEO.

Ciccone says he later learned Gel was actually Harris Ballow, who had pleaded guilty to one count of **money laundering** in 2003 in the U.S. and fled before sentencing. Once he became aware of Ballow's true identity, he "advised staff of the (Ontario **Securities**) Commission of these facts."

Ciccone's case has grabbed attention in London, Ont., because of his lifelong ties to local Mayor Joe Fontana, a friend since childhood in their shared hometown of Timmins, Ont.

Fontana has said he was not associated with the investment firm, but in statements to the official receiver in the bankruptcy of Ciccone Group in 2011, the investment firm founder said Ciccone Group "used Joe Sr.'s influence to provide credibility to our products" during a period Fontana was out of politics.

In 2007, Ciccone founded Trinity Global, a charity and tax shelter that's attracted tens of millions of dollars with the promise of providing meals to hungry kids in Canada and medicines for HIV/AIDS sufferers in Africa. Fontana joined the board in 2008, a post he still holds, and his son, Ugo Joseph, or Joe Jr., is president.

Document BLVLNT0020120912e89c0000l

CALGARY HERALD

City & Region

Hearing underway in $400-million Ponzi scheme case

Daryl Slade

Calgary Herald
282 words
6 September 2012
Calgary Herald
CALH
Final
B2
English

A preliminary hearing began this week for two Calgary-area men charged with running a massive Ponzi investment scheme that may have bilked investors of up to $400 million.

Gary Allen Sorenson and Milowe Allen Brost each face two counts of fraud over $5,000 and theft over $5,000 and one count each of possession of stolen property and **money laundering**.

Crown prosecutors Brian Holtby and Peter Mackenzie are expected to call dozens of witnesses in the hearing before Provincial Court Judge Mike Dinkel that is set to run until Dec. 21.

Shamsher Kothari, Brost's lawyer, said it is hoped the hearing to determine if there is sufficient evidence to go to trial can be shortened by as much as two months, but added, "it all depends on how the evidence comes out."

"Currently, the (Crown) disclosure is in excess of 92,000 documents," Kothari said outside court. "Definitely, it's been a voluminous matter, to say the least.

"Disclosure is still coming in witness statements and transcripts from the RCMP and Alberta **Securities** Commission."

Kothari said there are witnesses scheduled to testify from China and other countries around the world by video link in the mammoth case.

No evidence can be reported because of a publication ban.

Both accused have elected to have their trials heard by judge and jury.

Sorenson, who has been out on bail since shortly after he was charged on Sept. 14, 2009, is represented by lawyer Brenda Edwards.

Brost was previously granted bail of $1 million but has not been able to raise the cash.

dslade@calgaryherald.com

Calgary Herald

Document CALH000020120906e8960001q

THE GLOBE AND MAIL

Regulator for mutual fund dealers tries to stay relevant

JANET McFARLAND AND JACQUELINE NELSON
The Globe and Mail
Published Sunday, Dec. 29 2013, 6:00 PM EST
Last updated Monday, Dec. 30 2013, 12:47 PM EST

The watchdog for Canada's mutual fund dealers is searching for ways to be less burdensome on its members, as increased regulation and changing investor demands reshape a maturing business.

In the 11 years since the Mutual Fund Dealers Association of Canada (MFDA) opened its doors to regulate fund sellers, its membership has fallen by nearly half, from 220 firms to just 115 today. Most of those firms are small; 84 of them have less than $1-billion in assets under administration.

More Related to this Story

- PORTFOLIO STRATEGY Rob Carrick's biggest hits (and misses) of 2013
- Investor Clinic The real keys to investing success
- strategy lab A three-step plan for turning your child into a saver

Much of the decline is due to mergers of companies that say the high cost of MFDA compliance and regulation makes it inefficient to run a small fund dealer. While the MFDA's remaining members have grown over the past decade, mutual funds have also grown significantly outside of the regulator's purview.

The association's job is to ensure that individual advisers and firms are following the rules when they sell or trade mutual funds, and to bring action when they're not. The MFDA now oversees companies that handle about $360-billion, or nearly 40 per cent, of Canada's mutual fund assets, a reduction from 56 per cent in 2002. Brokerage firms and portfolio managers – which are regulated by other bodies – have expanded their investment fund operations and captured a bigger share of the market.

The result has been soul-searching within the MFDA about how to become more efficient to attract and retain members.

MFDA president Mark Gordon, who took over the top job at the regulator in October, 2012, says he is concerned that investment firm mergers are being spurred by the cost of the association's regulation. MFDA rules require firms to monitor daily trading and client interactions, which has forced funds to greatly increase their compliance staff and introduce new computer technology to track transactions.

"When our members resign, we ask them why you are resigning, and the majority say, 'The cost is too great to run my own dealer – I'd rather become a branch and focus on my book [of client business] and let somebody else worry about compliance infrastructure,'" Mr. Gordon says.

The trend has prompted the MFDA to revamp its processes to make its regular compliance reviews less onerous. One key change, Mr. Gordon says, is that it has decided to start doing compliance reviews of low-risk firms every four years instead of three, while higher-risk firms will be reviewed every two years.

The regulator is also trying to do quicker reviews of targeted issues rather than "a full review that takes two weeks when you've only got one high risk area you want to look at," Mr. Gordon said.

The MFDA is also working with firms to start fixing issues as soon as it notices them during compliance reviews. The result has been far fewer cited deficiencies when final reports are completed.

"We need to strike that balance between investor protection and regulatory burden and find that right balance, because there are consequences to the burden," he said.

Joanne De Laurentiis, chief executive officer of the Investment Funds Institute of Canada, a trade association for mutual fund companies, says the rule book for MFDA members has grown enormously in the past decade. The cost of hiring highly-trained compliance officers has made smaller firms less viable.

"The need to hire fairly expensive professional individuals, who are now adding to the expense side of the ledger, pretty much forced a reassessment of what size of dealer model made economic sense," she said. "And so you saw consolidation."

Member firms have given the MFDA "an earful" about the costs of undergoing four full regulatory audits in 12 years, Mr. De Laurentiis said, but she believes they now believe the regulator is responding to their concerns.

The pace of industry mergers and the cost of regulation have also fuelled a low rumble of discussion about whether the MFDA should pursue a merger of its own with its larger regulatory cousin, the Investment Industry Regulatory Organization of Canada (IIROC), which oversees brokerage firms.

The MFDA rejected proposals to merge with IIROC in 2005 when talks were under way for a merger between IIROC (then called the Investment Dealers Association of Canada, or IDA) and a third organization, known as Market Regulation Services Inc. (RS), which regulated trading on stock exchanges in Canada.

While the IDA and RS ended up merging in 2008, the MFDA stayed out of the talks.

Ian Russell, chief executive officer of the Investment Industry Association of Canada, an industry association for brokerage firms, says he is in favour of a merger between the MFDA and IIROC because there should be efficiencies for regulatory organizations that combine back office tasks like human resources, administration and IT.

However, Mr. Russell also worries that a merger could be costly and time consuming at a time when the industry is already facing many changes. "The experience with mergers hasn't been a good one in Canada," he said.

Mr. Gordon says the MFDA has not pursued any merger talks because two polls of its members in 2006 and 2011 found "no clear direction" for or against mergers.

He said the organization decided to drop the matter until the fate of a possible new national securities regulator is decided, because it is not clear how self-regulatory organizations like the MFDA or IIROC would fit into a new system.

"I think it's fair to say that members would want a business case made for it. How is it going to impact their operations, are they going to save money, how is it going to impact them," he said. "Our focus, given the lack of clear direction right now, is to just stick with our day jobs."

More Related to this Story

- NUMBER CRUNCHER Investment funds: Japanese equity, health care rose to the top in 2013
- Personal finance More Canadians have TFSAs, but many hazy on details: study
- These four common investing mistakes are holding you back

Tougher advisors' standards up for debate

By Luis Millan

Canada's securities regulators, under pressure to follow in the footsteps of international regulatory developments, are considering a fiduciary duty on financial advisors and dealers that would require them to act in the best interests of retail clients at all times.

But a former chair of the Ontario Securities Commission says this latest initiative does little to alter the landscape because it is just a tentative re-exploration of ground already covered.

On top of that, a brokerage industry lobby group is against the idea, citing bad timing at the very least.

The Canadian Securities Administrators, the umbrella group for Canada's provincial securities commissions, published a paper last fall calling for comments until Feb. 22 over a tougher standard that would raise the bar for financial advisors nearly to the same level as doctors and lawyers. The CSA, which has taken no position on the issue, made no promise that it would introduce change following the consultation. But if it does forge ahead, it will need to draft and specific proposals for further comment.

"The paper was disappointing," remarked Toronto lawyer Edward Waitzer, a former chair of the OSC, who is calling for reforms. "It is not particularly accessible, the issues have been addressed many times and presented a lot more simply, it doesn't take a position, and it doesn't move the ball down the hill at all. The publication of the paper doesn't give one cause for optimism that the securities commissions are going to take a leadership role."

The controversial proposition, opposed by the investment industry but commended by investor advocates, would overhaul the statutory regime and put it in line with international developments. After the 2008 global financial crisis, the United Kingdom, the European Union and Australia introduced legislation that strengthened investors' legal rights while raising the professional bar for investment advisors. The United States also is contemplating making changes. The U.S. Securities and Exchange Commission has recommended that a uniform standard be introduced for broker-dealers and investment advisers.

At present, registered advisers and dealers in Canada are required to deal fairly, honestly and in good faith with their clients, but without a general fiduciary obligation. However, there are four provinces — Alberta, Manitoba, Newfoundland and Labrador, and New Brunswick — that have enacted a statutory "best interests" requirement that applies to advisers or dealers, but only if they have a discretionary authority over their clients' investments.

The CSA consultation paper points out that there has not been a single court or regulatory decision concluding that the current requirement is the equivalent to a fiduciary duty.

"There is a big gap between what everybody thinks and what the law is," noted Marian Passmore, the associate director of the national non-profit advocacy group Canadian Foundation for Advancement of Investor Rights (FAIR Canada). "Investors believe that investment advisers are already acting in their best interests, and are not aware that that is not the standard."

FAIR Canada, which has been calling for a best-interest standard for years, hopes that the securities regulators act expeditiously, particularly since governments and employers are gradually shifting the burden of providing for retirement on to the shoulders of individuals. "I fear that it will be a slow process because a lot of initiatives that have come out of the CSA have taken a long time to come to fruition," says Passmore.

However, any move towards a fiduciary standard will face stiff opposition from the financial services sector. According to Michelle Alexander, the director of policy for the Investment Industry Association of Canada (IIAC), an industry organization for brokerage firms, the timing is not right to implement a higher duty of care. Alexander argues that the CSA and two Canadian securities self-regulatory organizations — the Investment Industry Regulatory Organization of Canada and The Mutual Fund

Dealers Association of Canada — have spent years developing a comprehensive, investor protection regulatory regime that is still being implemented. The regime, called the client relationship model, embodies most of the essential elements of a fiduciary standard, including improved cost and compensation disclosure and performance reporting, says Alexander. The new regulatory regime, approved a year ago and being rolled out in stages, should be allowed to be fully implemented and then be evaluated to determine if there are remaining areas that require further investor protections, adds Alexander.

"At this point the timing is not right to implement a fiduciary standard," said Alexander. "The costs and training that are going on with the client relationship model is huge for the industry — let them grapple with that before going on to something new."

The industry organization also believes that the imposition of a statutory fiduciary standard on advisors would have many negative consequences for both investors and themselves. Besides onerous compliance requirements and increased exposure to risk and liability for advisors, small investors would likely face a fee hike in financial advisory services and reduced access to financial products, contends IIAC in a paper it submitted on the issue last year to the CSA.

That's because the lower the client's sophistication, the higher duty of care; small investors would cost advisors more to serve while increasing their exposure to liability. "We're concerned that those clients would be pushed out of the advice channel and perhaps have to go to the discount brokerage channel," said Alexander.

Vancouver securities lawyer David Mitchell also believes the status quo is working well. He points out that in Canada investment advisors can be held to a fiduciary duty depending on the situation. While there is no such duty for sophisticated retail investors, the courts have recognized that a fiduciary duty exists in cases when unsophisticated retail investors rely exclusively on their investment advisor. The onus of establishing a fiduciary duty, however, rests with the investor.

"The status quo works well right now, other than your unsophisticated retail investor who faces the challenge of establishing a fiduciary duty to obtain relief from the court," said Mitchell. "But I think the system works well for most people. The duties are context-specific."

If securities regulators are "not prepared to take a leadership stance" on a fiduciary standard, there are other actions they can take that will lead to the same result, says Waitzer. Regulating the compensation structures and eliminating commissions for retail investment products as the U.K. and Australia have done "would make a difference," said Waitzer. So too would far more aggressive enforcement. "Instead of spending another 10 years spinning our wheels, let's move on to something else that regulators would be more comfortable doing," said Waitzer.

Close

More consolidation as boutique investment dealers st to survive

BARBARA SHECTER | January 27, 2014 8:53 AM ET
More from Barbara Shecter

National Post

Mid-sized investment dealers were riding high in 2007, feasting on healthy markets and booming commodity prices that drove underwriting, trading and acquisitions.

But today, the approximately 180 smaller or boutique firms in Canada are struggling with chronic weak business conditions in an increasingly tough competitive landscape.

The Investment Industry Association of Canada and other industry watchers have been warning for a couple of years that many of Canada's smaller firms are on precarious ground and many could cease to exist without a significant recovery in the small-cap trading and underwriting business.

Related

Edgecrest Capital set for major expansion as it acquires Stonecap Securities

"The traditional model of the independent firms relying on trading and corporate finance is broken, at least for the moment," says John Turner, a partner who heads to global mining practice at Toronto law firm Fasken Martineau DuMoulin LLP.

On Monday, Stonecap Securities Inc. was swallowed up by Edgecrest Capital, a relatively new player in the industry.

The consolidation follows the closure last April of independent investment dealer Fraser Mackenzie Ltd., which shut its doors after nearly 10 years in business. The firm, which was among those heavily exposed to the fortunes of the junior resource sector, cited difficult business conditions and mounting regulatory expenses.

Another indication of recent trends came in last year's resignation of longtime industry player Loewen Ondaatje McCutcheon Ltd. from membership in its primary regulator. Industry watchers suggested the independent firm planned to pursue business outside the purview — and fee requirements of the Investment Industry Regulatory Organization of Canada.

Some of the difficulties for the independent dealers can be traced to shortly after a banner year in 2007. That was when Canaccord Capital surprised Bay Street by displacing a number of the big banks to claim second place in the league tables of new equity and trust issues.

At the time, commodity prices were booming and the mid-tier brokers were profiting from their expertise and relationships in commodities-driven sectors like junior mining.

But the financial crisis in 2008 dried up a lot of financing and trading activity, conditions that caused the big banks to move "downstream" into the traditional territory of smaller dealers. When deal-making did occur, analysts said, the big banks were most often the winners because they could offer a suite of services to companies — including loans.

The crisis also forced smaller dealers to back away from risky trading, a move that crimped their profits.

"No question the independent brokers focused on the mining sector have had a tough time [in the past few years]," says Mr. Turner.

Still, the Faskens lawyer says, there have been recent signs the independent model is evolving.

"The model going forward will be much more relationship driven, in effect a merchant banking model," he says.

Among the positive signs Mr. Turner sees is the re-emergence of independent stalwarts such as David Beatty, a co-founder of Westwind Partners, and Bob Sangha, formerly of Dundee Securities Corp.

Mr. Beatty has a new firm, Edgecrest Capital, which announced a major financing this month for North American Paladium Ltd. On Monday, Edgecrest said it will acquire the Canadian and U.S. business of independent dealer Stonecap Securities Inc., subject to regulatory approval.

Mr. Sangha has launched Maxit Capital and recently landed work as a financial advisor for Osisko Mining Corp., alongside BMO Capital Markets. Montreal-based Osisko is facing a hostile bid from Goldcorp Inc.

"It's not game on yet for the independent brokers," says Mr. Turner. "However, if it's not the beginning of the end of the downturn for the independents, it seems to be, as Churchill said, at least the end of the beginning."

In the meantime, the country's "big six" banks and two large and diversified independents are prospering, according to the Investment Industry Association of Canada.

Though no longer pushing to the front of the line in competition with Canada's big banks, Canaccord continues to be counted by the IIAC among the eight top dealers. Notably, though, some of those spoils come from a savvy investment in the United Kingdom in 2012 that added operations in the United States and Europe to Canaccord's arsenal, as well as listings capabilities in Singapore.

It's also noteworthy that, in 2010, Canaccord bulked up by merging with another Canadian independent, Genuity Capital Markets. Genuity was founded by former senior investment bankers from the Canadian Imperial Bank of Commerce.

Raymond James rounds out the top eight firms tracked by the IIAC. The industry group says these integrated firms were responsible for nearly all of the securities industry's "respectable earnings rebound" in 2013 a 27% gain in operating profit which reached $4.8-billion on an annualized basis.

In a report last week, the IIAC described the divide between the large and small players as a "feast or famine" situation.

"This divergence in earnings performance [in the past year] is consistent with the pattern over the past five years," Ian Russell, the president of the IIAC, said in a letter to members. He pointed to the "relatively strong earnings at the largest firms, contrasted with mediocre results at the specialized boutiques."

FACTIVA DOW JONES

EDMONTON JOURNAL

Business

St. Albert man charged with fraud; Concrete Equities raised millions for Mexico condominium project

Amanda Stephenson

Postmedia News
822 words
23 January 2014
Edmonton Journal
EDJR
Early
C3
English

Criminal charges have been laid against two men who allegedly used a fraudulent real estate scheme in Mexico to bilk victims out of $23 million.

David Nelson Humeniuk of St. Albert and Varun (Vinny) Aurora, former executives of Concrete Equities - the Calgary-based firm that went into receivership in 2009 after raising $120 million from 3,700 investors - are both charged with three counts of fraud over $5,000 and one count of theft over $5,000.

Humeniuk, who faces an additional count of theft and **money laundering** for allegedly taking $1 million of investors' funds for his personal use, has been arrested and released to appear in Calgary Provincial Court on February 27. A Canada-wide warrant has been issued for Aurora's arrest.

The criminal charges come more than two years after Humeniuk, Aurora, and two other people associated with Concrete Equities were found to have breached Alberta **securities** laws. In January 2012, the Alberta **Securities** Commission slapped Humeniuk, Aurora, David Jones, and Vincenzo De Palma with combined penalties topping $5.6 million - including the largest ever levied on an individual in Alberta.

But while the charges mark the culmination of a 12-month RCMP investigation that involved three full-time investigators, the analysis of more than 1,000 documents, and the extensive tracking of funds that had allegedly been funnelled to multiple business ventures across North America, some victims say it's not enough.

"Maybe it makes some people feel better that they've been charged, but being charged and being convicted and serving time are two different things," said Terry Town, a Calgary businessman who lost $80,000 in Concrete Equities' 'El Golfo de Santa Clara' project. "If we heard they were going to jail for 10 years, that would be a whole other story. But I'd be surprised if they get six months."

Even if the accused go to jail, Town said, it won't make things better for the thousands of people - many of them seniors - who are still seriously hurting in the aftermath of the scandal. "There are people who lost their homes," Town said. "If you lost your life savings, it's gone. There's nothing to be done."

Under the Criminal Code, a conviction for fraud over $5,000 carries a maximum penalty of 14 years in jail.

Concrete Equities was founded in 2005 and went on to offer units in eight realestate-based limited partnerships. They invested in Calgary strip malls and office buildings and in raw land in Mexico.

In July 2009, Concrete and seven of the partnerships were placed in receivership. According to the receiver's report, only five of some 40 Concrete projects had enough value for there to be a chance of some recovery for the investors.

Sgt. Conal Archer of the Calgary Financial Integrity Unit said RCMP chose to focus their investigation on the Mexican condo project, which had 1,300 victims from Alberta, B.C., Saskatchewan, and Ontario. "We had to make a decision," Archer said. "We looked at the egregiousness of this particular fraud. They (victims) were being promised over 500 per cent return on their investment, so it was fairly serious. These people thought they were going to be getting quite wealthy, and of course, that never happened."

Though Jones was Concrete's president and later CEO, he was not a director of the particular partnership that handled the El Golfo deal, Archer said.

No charges have been laid against either Jones or De Palma. In 2012, Jones was levied a $1.2 million penalty by the Alberta **Securities** Commission, while De Palma was issued a $600,000 penalty.

In its ruling, the Alberta **Securities** Commission said Concrete Equities sold investors units of commercial properties, but overstated purchase prices, misled investors about the commissions to be paid, and co-mingled funds from individual projects.

The receiver told the ASC hearing that Concrete couldn't list all its bank accounts.

In its sanction decision, the ASC levied a $3.3 million penalty against Humeniuk, who was at one point senior vice-president and general manager of Concrete. He was also permanently barred from trading in or purchasing **securities**, or acting as an officer or director for any issuer. The sanction was the highest ever issued by the ASC.

Aurora was given a $500,000 penalty, a five-year ban on trading or purchasing **securities**, and a nine-year ban on acting as an officer or director for any issuer.

RCMP are asking anyone with information as to the whereabouts of Aurora contact Sgt. Conal Archer at 403-699-2500 or Crime Stoppers anonymously at 1-800-222-8477.

Two investors speaking on condition of anonymity said friends close to the situation told them Aurora has left the country, and is now living in India.

Edmonton Journal

Document EDJR000020140123ea1n00020

OnLine

'The wolf? He's still big and bad,' says one of 1,500 real-life fraud victims

Jacqui Goddard

1437 words
19 January 2014
Postmedia Breaking News
CWNS
English

When Leonardo DiCaprio's new film The Wolf of Wall Street opened in Bob Shearin's hometown of Manhattan Beach, California, the 66 year-old was one of the first to buy a ticket.

Released on Christmas Day in the United States, and in Britain two days ago, the film, directed by Martin Scorsese, came garlanded with praise by critics who called it "exhilarating" and "hilarious".

But Shearin's interest had nothing to do with the reviews or the lurid trailer which promised three hours of sex, drug-taking and depravity among a group of amoral stockbrokers in Nineties America.

Quite the opposite. The businessman wanted to see the film because he had first-hand experience of the events it depicted, as a victim of the real-life "wolf", Jordan Belfort.

Belfort, played by DiCaprio, was the founder and president of the New York investment banking firm Stratton Oakmont which, between 1989 and 1997, made outrageous profits - even by Wall Street's high standards - while conning small investors out of millions of dollars.

As one of them, Shearin is appalled by the way the film seems to glory in its protagonist's crimes, playing his hedonistic lifestyle for laughs.

"The harm that was done to people around Belfort, and to the small investors, and what that meant - you see none of that," said Shearin. "His depiction is annoying and disturbing, because it makes him more into a mythical figure and skips the reality of what he was about. And what he was about was harming people financially."

Belfort's 1,500 victims are also furious that the con man, who has admitted he was a "greed-fuelled animal", has failed to pay back the money despite a $110 million restitution order by a federal judge, part of his sentence for fraud and **money laundering** in 2003.

The victims, many of whom lost their savings, are also disappointed that DiCaprio made a 30-second video for Belfort's motivational-speaking business, extolling him as a "shining example of the transformative qualities of ambition and hard work".

"It's really time for people to stop glorifying the crooks on Wall Street and for justice to be done," said Diane Nygaard, a **securities** and investment fraud lawyer in Kansas City, Missouri, who has represented several of Belfort's victims. "I was appalled at DiCaprio because he clearly doesn't have a clue as to the heartache this con man cost so many hard-working Americans. I think the film should be called 'My Adventures with other People's Money', because that's what it boils down to. You can steal more money with a pen than you can with a gun."

Three hours long, with more than 500 utterances of the F-word, a feature-film record, The Wolf of Wall Street tells of the upstart New Yorker whose first business - a meat-selling enterprise - left him bankrupt at 24. From the steak market he leaped into the stock market and two years later banked an income of $49 million - and complained "it was three shy of $1 million a week".

With such wealth came a decadent lifestyle. There were private jets, luxurious properties, bodyguards, champagne, wild sex - once on a mattress of $3 million in banknotes - poolside parties, prostitutes, and, in Belfort's words, "enough drugs to sedate Guatemala". At one point, he was hooked on 22 drugs, including cocaine and Quaaludes.

His first expensive car was a white Ferrari Testarossa. Later, he bought a vintage Aston Martin that he kitted out like James Bond's, complete with a gadget to scatter nails on the road to burst the tires of potential pursuers.

From its beginnings in a cupboard at a used-car salesroom, Stratton Oakmont grew swiftly until it was filled with the collective roar of 1,000 young stockbrokers, all urging investors over the telephone to buy. But often they were selling empty promises. Between 1990 and 1997, the firm targeted customers in a classic "pump-and-dump" scam. Brokers would buy large blocks of small public companies, then hard-sell the rest of the shares to inflate the price, before dumping their own shares into the market, causing the price to plummet. This made colossal profits for Belfort and his staff, but left investors' portfolios worthless.

"It started out as a phone call selling me good stock, one of the better brands that made me money, then after they had me hooked they started selling me nothing, just a lot of hot air," said Dr Alfred Vitt, 81, who lost $250,000.

"They were such high pressure people, very persistent, they wouldn't take no for an answer. Sometimes you would just have to hang up on them but other times to get them off the line I'd cave in, unfortunately. Everyone wants to strike it rich, so I borrowed money and I went deep."

Stratton Oakmont's brokers made a minimum of $250,000 in their first year, progressing to seven figures by year three. Even the switchboard operator earned $80,000.

Nothing was taboo. The film opens with a scene in which crazed staff vie for a $25,000 prize in a dwarf-throwing contest; in another, a young female assistant has her head shaved before baying colleagues in exchange for a $10,000 breast implant.

Office sex got so out of hand that notices from the management were handed out declaring the premises a "--? free zone" between 8 a.m. and 7 p.m.

"It was nothing short of a good old fashioned gold rush," Belfort wrote in his 2008 memoir, on which the film is based. "They were drunk on youth, fuelled by greed and higher than kites. And day by day the gravy train grew longer."

The train hit the buffers in 1998 when the FBI and the **Securities** and Exchange Commission pounced. Belfort pleaded guilty to 10 counts of **securities** fraud and **money laundering**. He was sentenced to four years in prison but was released after 22 months, having cut a deal with prosecutors for turning over a number of cronies and agreeing to make restitution. Today, he claims to be a reformed man. Aside from his speaking work, he sells a $2,000 home study course in how to get rich quick "without sacrificing integrity" and hires himself out to companies including Virgin Airlines and Deutsche Bank.

Joel Cohen, a former federal prosecutor who led the case against Belfort, complains that Scorsese's film gives Belfort's business free publicity, especially in its final scene, when DiCaprio appears alongside the real-life Belfort. "What reason could they have for putting the real Belfort on screen as they did in front of a placard advertising his motivational speaking business?"

Last October, the U.S. Attorney's Office for the Eastern District of New York filed a court motion asking for Belfort to be held in default of the restitution order. Of the $11.6?million collected against his $110 million debt, it stated, most came from the sale of seized assets, and Belfort has paid just $243,000 over the past four years

despite receiving $1.7?million from his two books and the film rights. He opposed the motion, arguing that the requirement to pay restitution had expired. The US Attorney's Office has since withdrawn the motion, in order to keep negotiations with Belfort open.

On his Facebook page, Belfort insists "100 per cent of the profits of both books and the movie", amounting to "countless millions of dollars", are destined for the restitution fund. But Robert Nardoza, a spokesman for the attorney's office, countered: "Belfort's Facebook posts are inaccurate. The government has seen nothing to suggest that even 100 per cent of Belfort's profits from his books and movie would yield 'countless millions'. They would not be enough to cover the losses inflicted on the victims."

Shearin, who lost $130,000, said Belfort had "managed to weasel out of" the payments, adding: "That makes me suspicious of the 'recovery' he's claiming."

It is a suspicion based on close observation - Belfort's seafront home is also in Manhattan Beach.

"He's short, cocky, kind of strutting around," said Shearin. "Maybe I should have some resentment, but where would that get me? I'm not going to run up to him and say 'You're a scumbag.' He's just doing what he does. That's what scumbags do."

Canwest News Service

Document CWNS000020140120ea1j000a9

DOWJONES | Newswires

TD Bank Fined $52.5 Million by Federal Regulators

486 words
23 September 2013
14:24
Dow Jones News Service
DJ
English

By Jacqueline Palank and Michael R. Crittenden

WASHINGTON--U.S. regulators fined TD Bank a total of $52.5 million over its role in helping imprisoned attorney Scott Rothstein carry out a $1.2 billion Ponzi Scheme.

The **Securities** and Exchange Commission, Office of the Comptroller of the Currency and the Financial Crimes Enforcement Network announced the charges and fines on Monday. Mr. Rothstein has already pleaded guilty to bilking investors out of more than $1.2 billion and is currently serving a 50-year prison sentence.

The SEC alleged that TD Bank and a former official, Frank Spinosa, defrauded investors by creating misleading documents and making false statements about the accounts that Mr. Rothstein, the founder of a South Florida law firm, held at the bank and used to carry out his Ponzi scheme.

Mr. Spinosa faces penalties and a permanent injunction under the SEC's complaint, filed in the U.S. District Court for the Southern District of Florida. Attorneys for Mr. Spinosa couldn't immediately be reached for comment Monday afternoon. TD Bank didn't admit any wrongdoing under the settlement.

Mr. Spinosa allegedly told investors that TD Bank restricted Mr. Rothstein's ability to move the funds, when it didn't, and that certain accounts held millions of dollars when their balances were actually less than $100 or zero, according to the SEC complaint.

"Financial institutions are key gatekeepers in the transactions and investments they facilitate and will be held to a high standard of accountability when their officers enable fraud," Andrew J. Ceresney, co-director of the SEC's enforcement division, said in a statement. "TD Bank through a regional vice president produced false documents on bank letterhead and told outright lies to investors, failing in its gatekeeper role."

The OCC said in a legal filing the bank also failed to alert the government about suspicious activities in the accounts tied to the Ponzi scheme. For more than a year, bank officials ignored suspicious activities that had triggered the bank's anti-**money laundering** alert system. Officials at the bank incorrectly decided the questionable activities were not suspicious and did not file appropriate reports with the government, the agency said.

The failure to file suspicious activity reports "were significant and egregious for a number of reasons, including the number of alerts generated by these accounts and the volume and velocity of funds that flowed through them," the OCC said in a statement.

TD Bank has previously agreed to pay more than $72 million in a separate settlement reached in the bankruptcy case of Mr. Rothstein's now-defunct law firm, Rothstein Rosenfeldt Adler.

Creditors pushed the Florida law firm into involuntary bankruptcy protection in November 2009, weeks before Mr. Rothstein's arrest. Creditors received their first payment last month, nearly four years into the firm's wind-down. [09-23-13 1519ET]

Dow Jones & Company, Inc.

Document DJ00000020130923e99n000c9

THE VANCOUVER SUN

David Baines
BusinessBC

Accused money launderer and admitted stock offender cross paths in Naramata; Erwin Speckert's B.C. company is listed as the owner of lakefront property, but Ingo Mueller and his wife live there and call it their own

David Baines

Vancouver Sun
973 words
17 April 2013
Vancouver Sun
VNCS
Final
C2
English

In previous columns, I noted that Swiss fiduciary Erwin Speckert has been closely associated with West Vancouver promoter Ingo Mueller.

Mueller has a regulatory history. In 2006, the B.C. **Securities** Commission suspended him from the B.C. **securities** market for three years after he admitted he had disseminated false information about a bulletin board company called Exotics.com Inc.

The U.S. **Securities** and Exchange Commission made similar allegations, which he settled in 2010 without admitting nor denying any wrongdoing, but nevertheless agreeing not to participate in any penny stock offering for the next five years.

BCSC enforcement staff recently accused Speckert of funnelling millions of dollars to an Abbotsford man, Colin McCabe, to secretly promote sketchy stocks quoted on the OTC Bulletin Board in the United States. A hearing is pending.

Manitoba RCMP have also charged Speckert with possessing and laundering the proceeds of an illegal gambling enterprise in Ontario after he was caught last year at a Winnipeg bus depot with $1.3 million in his backpack while en route to Vancouver. That case is also pending.

As noted in previous columns, Speckert and Mueller have been close associates. Among other things, Speckert was a co-director of Mueller's private firm, St. Georges Capital Corp., until he ran into trouble with the BCSC.

I have also linked Speckert and Mueller to a $2.15-million lakefront residential property in Naramata.

The property, located at 4785 Mill Rd., is registered in the name of Naramata Golden Properties Ltd., whose sole director and officer is listed as Speckert.

However, I have been reliably informed that the property is used exclusively by Mueller and his wife, and that they refer to it as their property. This raises the question: Is Speckert simply acting as a front for Mueller?

If he is, it wouldn't be the first time. As noted in my last two columns, the estranged wives of Vancouver-area promoters James Michie and Richard Coglon claimed that Speckert was helping them hide assets through companies he represented. Michie and Coglon denied they had any interest in the assets, but the court found otherwise.

I tried to ask Mueller whether he was the beneficial owner of the Naramata property, but he did not return my call Tuesday.

-

One of the bulletin board companies that the BCSC alleges Speckert and McCabe conspired to promote was Guinness Exploration Inc., which is closely associated with Coglon.

Guinness was being promoted on the basis of prospective gold claims in the Yukon, which it had acquired for cash and restricted shares from Eagle Trail Properties Inc., a private Saskatchewan company owned by Coglon and an associate, Robert Sim.

BCSC investigator David Salzano raised Coglon's name while he interviewing Speckert about funding McCabe's promotion of Guinness. (Transcripts from that interview were tendered at a preliminary hearing into the matter.) "And you know, there's people I know who are involved with the company (Guinness) that I think paid for it (the promotion), and I think they're people you might have heard of, like Richard Coglon or (names one other individual)," Salzano said to Speckert.

"Door No. 1, so far," Speckert replied.

When I called Coglon last week, he adamantly denied any involvement in the management or promotion of Guinness. He also denied he had any dealings with Speckert with respect to Guinness.

-

Speckert has also been involved in bulletin board companies with Ontario **securities** offender James Pincock.

In an August 2002 settlement agreement with the Ontario **Securities** Commission, Pin-cock admitted he had solicited at least $2 million from 150 investors, pooled the funds in offshore accounts, then used the proceeds to buy large blocks of shares from seven junior companies. He then broke up the blocks and distributed the shares to the investors, thereby circumventing minimum investment rules.

Pincock admitted he had not been registered to sell or advise in **securities**, or to act as a portfolio manager. He also admitted he had distributed the shares without filing a prospectus or having an exemption from prospectus requirements. For these offences, he was suspended from the Ontario **securities** market for five years.

He subsequently changed his name to James Werth Longshore.

When his suspension expired, Longshore began promoting a bulletin board company called Xtra-Gold Resources Corp., which is working on a gold project in Ghana. Significant shareholders included:

- G.M. Capital Partners Ltd., a Geneva-based firm owned by Michie. It owned six million shares.

- Alpine Atlantic Asset Management AG, a Zurich-based firm that provided asset management and protection services for its clients. Alpine was owned by G.M. Capital, Michie served as chairman and Speck-ert as a manager. It held just over 250,000 shares.

- Speckert's close business associate, Mikkel Lind of Liechtenstein, who controlled just over one million shares through two companies based in St. Lucia in the Caribbean. (Lind and Speckert are currently listed as co-directors of a private B.C. company called Fun City Properties Inc., business unknown.)

As always, the overarching question is, who were the beneficial owners of these shares?

Whoever they were, they stood to make big money.

Those shares, which they acquired for pennies each, peaked at $2.38 in December 2010, just after the company obtained a listing on the Toronto Stock Exchange. Since then, they have declined to 63 cents, nearly one-quarter their all-time high.

dbaines@vancouversun.com

/ Erwin Speckert: charged with money laundering by RCMP.; / Erwin Speckert: charged with money laundering by RCMP. [VASN_20130417_Final____C2_124893_I001.jpg];

Vancouver Sun

Document VNCS000020130417e94h0002v

FROG Genmed's Harris pleads not guilty in L.A.

Stockwatch
920 words
7 March 2013
Canada Stockwatch
CNSW
English

FrogAds Inc (:FROG)

Thursday March 07 2013 - Street Wire

See Genmed Holding Corp (:GENM) Street Wire

by Mike Caswell

Mark Harris, the former Vancouver promoter facing criminal charges in the United States for several pump-and-dumps, has pleaded not guilty. He entered the plea in a brief appearance before a judge in Los Angeles on Feb. 27, 2013. The judge then allowed his release on a $700,000 bond, with the conditions to include house arrest. (All figures are in U.S. dollars.)

Prosecutors claim that Mr. Harris, 56, was part of a group of serial market manipulators that generated $30-million in illegal profits from a number of pump-and-dumps. The group secretly took control of OTC Bulletin Board companies and promoted the stocks with false or misleading information. The men then allegedly dumped millions of shares and moved the proceeds from the scheme offshore.

Mr. Harris was initially arrested in Arizona on Feb. 13, 2013, when a pair of indictments against him and 13 others were unsealed in California. The U.S. Marshals Service transported him to Los Angeles, where he remained in custody until he pleaded not guilty last week. After he entered the plea, the judge fixed his bond at $700,000, of which $100,000 his wife Jonni would satisfy and the remainder he and his wife would jointly provide.

The judge also ordered him to remain under house arrest at his home in Arizona, to be enforced by electronic monitoring. He may only leave to drive his son to and from school. Other terms of his release include travel restrictions, avoiding contact with his co-defendants, and submitting to drug and alcohol testing.

The move from jail to home will be a substantial upgrade in accommodations for Mr. Harris. The address listed in his release documents is for a 4,407-square-foot home in Scottsdale, Ariz. According to an old real estate advertisement, the house has five bathrooms, a pool and parking for three cars. The average list price of homes in his ZIP code is $1.55-million.

Fraud charges

The charges against Mr. Harris are detailed in a pair of indictments unsealed in the Central District of California on Feb. 13, 2013. The charges included **securities** fraud, wire fraud and international promotional **money laundering**. Prosecutors claimed that Mr. Harris and others ran a pump-and-dump scheme that began around 2009 and continued until at least December, 2012. The promotions, as described in the indictments, all followed a similar pattern: the men took control of an OTC-BB company, promoted it with false or misleading news, and then dumped their shares.

One of the examples prosecutors provided was Genmed Holding Corp., a Dutch company that claimed to be developing generic drugs. The Genmed scheme, as described in the indictment, began in early 2011, when then stock was thinly traded and was around 30 cents. According to prosecutors, the men took control of the

company and then arranged a touting campaign that included paid promoters, a celebrity video and mass mailings that overstated the company's revenues.

(The recipients of that promotional money, as listed in the indictment, included a West Vancouver company called Raincity Marketing Group. The indictment did not accuse Raincity of any wrongdoing, but said that it received $165,000 through wire transfers to HSBC Bank Canada.)

As the promotion began, the stock became far more active, trading hundreds of thousands of shares per day, and reaching a 52-cent high. The company issued a news release in which it claimed to have an agreement with a pharmaceutical distributor in Ireland that would see its products sold in several countries.

Part of the promotion, according to prosecutors, was a video news release with a known actor. (Prosecutors did not identify the actor, but one of the other companies in the indictment claimed to have Pamela Anderson pitching its products.) The video shoot was the subject of a string of text messages that Mr. Harris received on March 20, 2011, prosecutors claimed. One text said the video would be distributed on "CNN Bloomberg, msnbc, local tv as well as cable across the nation ... I believe it will [be] a great tool for [the third party stock promotion groups]."

One of Mr. Harris's co-defendants, Grover Nix, had high expectations for the promotion, according to the indictment. In an intercepted conversation he said, "I'm fucking truly excited like a kid at Christmas." In all, prosecutors claim that the men made $2.1-million from the Genmed promotion.

The defendants, in addition to Mr. Harris, are Sherman Mazur, Ari Kaplan, Grover "Colin" Nix, Regis Possino, Edon Moyal, Joseph Davis, Curtis Platt, Dwight Brunoehler, Tarun Mendiratta, Ivano Angelastri, Joseph Scarpello, Julian Spitari, Peter Dunn and William Mackey. Most of the men are from California.

The stocks, in addition to Genmed, were Sport Endurance Inc., Empire Post Media Inc., FrogAds Inc. and Biostem U.S. Corp. None of the companies are named as defendants.

The case is scheduled for a trial by jury starting April 23, 2013.

Prior to Arizona, Mr. Harris lived in Vancouver on and off for many years, holding himself out as an investor relations man. He ran a private firm called Skylla Capital Corp., which operated from an office on Burrard Street. The Vancouver Sun's David Baines reported in 2006 that he had a child with former Northern **Securities** Inc. broker Jonni-Colleen Sissons.

Canjex Publishing Ltd.

Document CNSW000020130307e937005hd

Business

Woman accused in $135-million scheme; Payday-loan operator had hundreds of investors in alleged Ponzi scam

The Canadian Press
315 words
22 January 2013
Victoria Times Colonist
VTC
Final
B1 / Front
English

The B.C. **Securities** Commission accused a woman on Monday of running an elaborate Ponzi scheme and raising $135.4 million from at least 800 investors in Canada and the United States.

The regulator alleged Doris Nelson operated a payday-loan business called the Little Loan Shoppe and told investors that because her business was so profitable, she could afford promissory notes paying annual interest rates of 40 per cent to 60 per cent.

"Nelson paid out purported returns to some investors, but her business was not profitable," the regulator said. "Instead it consistently lost money due to its high rate of customer loan defaults. Nelson was able to create the appearance of profitability, and to pay high rates of interest on the promissory notes, only because she used money obtained from later investors to make payments to earlier investors."

The commission accused Nelson, a Canadian citizen living under house arrest in Colbert, Washington, of fraud and making false statements to the commission.

The allegations have not been proven.

The regulator said Nelson paid out a total of $118 million to investors, including $2.2 million in commissions to recruiters.

It's alleged that operating losses, money she withdrew from the business for her own use and other unaccounted-for losses made up the remaining $17.4 million, which the regulator said did not appear recoverable.

Nelson stopped making payments to investors in 2009, and three months later a group of investors petitioned one of Nelson's companies into bankruptcy, and another filed a voluntary petition for bankruptcy.

The B.C. regulator's case follows charges in the U.S. where Nelson is awaiting trial on 71 counts of wire fraud, 22 counts of mail fraud and 17 counts of international **money laundering**.

Victoria Times Colonist

Document VTC0000020130122e91m0001c

THE GLOBE AND MAIL

Business

Calgary men, companies face $54-million in sanctions for 'massive fraud'; ASC issues penalties in fraud case for Brost, Morice and Sorenson

JEFF GRAY Law Reporter

262 words
28 September 2012
The Globe and Mail (Breaking News)
GMBN
English

Three Calgary men and their companies have been ordered to pay nearly $54-million in sanctions by the Alberta **Securities** Commission for bilking investors in "a systemic massive fraud."

In a decision released Friday, an ASC panel handed down the sanctions against Dennis Morice, Milowe Brost, Gary Sorenson and their companies, The Institute for Financial Learning Group of Cos. Inc. and Merendon Mining Corp. Ltd.

An ASC panel in April previously found that they had orchestrated a $46-million fraud.

In addition to the large monetary penalties, Friday's order also permanently bans the three men from trading or purchasing **securities**, advising others on **securities** or acting as a director or officer of an issuer.

In April, the Alberta regulator said that the group had "perpetrated a deliberately complex, co-ordinated, far-reaching and massive – almost $46-million – fraudulent investment scheme."

Mr. Brost and Mr. Sorenson have also faced investigations and charges by the U.S. **Securities** and Exchange Commission and the RCMP in connection with other alleged frauds.

The SEC won an order in 2010 ordering the two men to pay more than $310-million (U.S.).

Mr. Brost and Mr. Sorenson also face criminal charges of fraud, theft, possession of stolen property and **money-laundering** in connection with their alleged Ponzi investment scheme. A preliminary hearing in the case got under way earlier this month in a Calgary courtroom.

Globe and Mail Update

The Globe and Mail Inc.

Document GMBN000020120928e89s00336

THE VANCOUVER SUN

David Baines
BusinessBC

Victoria 'wealth creation' firm closes doors after string of bad investment recommendations; President and owner of Wealth By Design, Denise Andison, now promoting fledgling recycling company

David Baines

Vancouver Sun
881 words
8 September 2012
Vancouver Sun
VNCS
Final
C2
English

Wealth by Design, the Victoria financial planning firm that promised to make its clients "financially free" then saddled them with a host of underperforming investments, appears to have shut down its business.

A reader told me this week that the company's office has been shuttered, and I note the company's website is no longer operative. The company's voicemail is still active, but nobody returned my calls on Friday.

As reported in March, Wealth by Design billed itself as a "financial ser-vices education and capital-raising company."

It held seminars and "boot camps" where it purportedly taught attendees how to become "financially free within 10 years or less."

It offered an array of investment products that would purportedly help attendees achieve that goal, but in fact, had the opposite effect.

The president and owner of Wealth by Design was Denise Andison, and the firm's chief executive officer was Stephen McClure.

Among the investments that McClure recommended were Meren-don Mining, which turned out to be a Ponzi scheme; Canadian Humanitarian Trust, a charitable donation tax shelter that was disallowed by Canada Revenue Agency; and Borealis Inter-national Inc., which was shut down by the Ontario **Securities** Commission.

In April, after my columns were published, McClure left the firm, but Wealth by Design carried on. It began promoting another questionable investment offering, One World Polymers Corp., a fledgling company that plans to sell waste plastic products to offshore countries. This is not exactly an arm's-length recommendation: Andison also serves as One World's chief operating officer, which raises a conflict-of-interest question.

Andison has also been heavily involved in the Victoria Real Estate Investors Club, which is run by her husband, Gord Knox. It has been a very symbiotic relationship, with Knox recommending his wife and her firm. He has also presented many other high-risk investments, including distressed property in Arizona. As always, attendees should keep their guard up. Last month, PI Financial Corp. announced it would acquire Union **Securities** Ltd.'s client accounts and its employees - consisting of about 70 advisers and assistants, and about 30 administrative staff.

After the deal closes, which is scheduled for Oct. 15, Union **Securities** will cease operations as a registered dealer, marking the end of its 49-year existence.

The combination solves two problems: The first is that Union was skating pretty close to the edge in terms of capital adequacy. As Union chairman and CEO Norm Thompson pointed out in a release, joining with PI is "a prudent step in providing our clients with the confidence and stability that is needed in these difficult market conditions." The second problem it solves is the terrible public relations image that Union and its advisers created through repeated run-ins with regulators.

Union was founded by Thompson's father, Norman Sr., in 1963. The firm initially focused on Vancouver Stock Exchange-related business, but gradually shifted emphasis to stocks quoted on the OTC Bulletin Board in the United States. This attracted shady clients and errant brokers who, in turn, attracted regulatory attention.

In the summer of 2005, the Investment Dealers Association of Canada pronounced that Union had developed a "culture of indifference toward compliance issues" and ordered the firm be placed under the supervision of Grant Thornton LLP.

The following year, the firm and its three most senior officers - Norm Jr. and his brothers, Rex and John Thompson - admitted to a host of trading and compliance breaches and agreed to pay a total $1.775 million in fines.

The settlement also required Union to retain Grant Thornton to "review and test" the firm's compliance systems and policies for the next three years.

That did not end the matter, how-ever. In succeeding years, a string of Union brokers were named in regulatory actions. (Just this week, Reginald Groome, a broker in Union's Montreal office, was cited for allegedly permit-ting his clients to buy shares of a company that was under a cease-trade order. A hearing is pending.)

PI Financial and its advisers have also had many run-ins with regulators, also due to the firm's fascination with bulletin board stocks.

In August 2001, the B.C. **Securities** Commission cited the company and nine of its most senior officers and directors for allegedly turning a blind eye to mob-related **securities** fraud and **money laundering**. Among them was Max Meier, who still serves as the firm's chairman and CEO.

The hearing - the longest in BCSC history - ended in September 2006 with a split decision absolving the respondents of any wrongdoing. But the adverse publicity - combined with many other instances where PI brokers were named in B.C. and U.S. regulatory actions and court cases - caused the firm immense reputational damage.

Since then, PI - which is 25-per-cent owned by a subsidiary of National Bank of Canada - has done a good job of keeping out of trouble. Hopefully, it will be able to teach some of Union's more adventuresome brokers how to do the same.

dbaines@vancouversun.com

Vancouver Sun

Document VNCS000020120908e89800036

The Gazette

News

Investment adviser found guilty of obstruction; Was fined for a similar crime in 2009

PAUL DELEAN

The Gazette
393 words
14 August 2012
Montreal Gazette
MTLG
Final
A7
English

A high-profile Montreal investment adviser, Michel Marcoux of Avantages Services Financiers, has been found guilty of obstructing **securities** regulators in an investigation of offshore accounts.

The disciplinary committee of the Chambre de la sécurité financière, the body that oversees financial professionals in Quebec, rendered the verdict and will hold a hearing on sanctions at a future date.

Marcoux was convicted of having failed to act "with honesty and integrity" during an Autorité des marchés financiers (AMF) inspection in 2004 by falsely declaring he didn't know the identity of clients of Dominion Investments Ltd. that had accounts with Avantages under names like Martien, Popoye, Banane and Discus.

He was convicted of the same infraction for having told the AMF in 2006 and in 2007 that Dominion Investments and/or its Bahamasbased liquidator owned the accounts.

Dominion Investments, based in the Bahamas, was the investment services company of Quebecer Martin Tremblay, sentenced in 2007 to four years in U.S. jail for **money laundering** after he was videotaped offering to launder $20,000 for two undercover government agents.

The company was put into liquidation after his arrest in 2006.

The disciplinary committee was told Marcoux referred about 50 of his clients to Dominion, of which "eight to 10" opened accounts.

Marcoux, an investment adviser for 17 years, author of several books and regular presenter at workshops hosted by the Chambre de la Sécurité Financière, said he'd always acted honourably and done nothing illegal.

The fact he pleaded guilty in Quebec Court to the same allegations in 2009 and was fined $15,000 for securitieslaw violations is not an admission of the infractions or sufficient evidence for professional sanctions, he argued.

He told the disciplinary committee he pleaded guilty on the advice of his former lawyer and after consulting people in the industry.

Given that he had talked to other people, and is an educated person with considerable industry experience, it's hard to believe he'd have made the admissions without a pretty good understanding of the case against him, the committee said.

It noted the testimony of one witness who said Marcoux not only knew his pseudonym, Gala, "he's the one who asked us to choose one."

pdelean @montrealgazette.com

Montreal Gazette

Document MTLG000020120814e88e0002e

CALGARY HERALD

News

Canadian man charged in U.S. Ponzi scheme

Postmedia News
177 words
18 April 2012
Calgary Herald
CALH
Final
A12
English

The former owner of the Ontario Hockey League's Cornwall Royals has been charged in the United States with operating "a massive Ponzi scheme," to the tune of $129.5 million US.

William Wise, 62, originally from Cornwall, Ont., and California resident Jacquline Hoegel, 55, are accused of marketing and selling fake certificates of deposit to more than 1,200 people.

The U.S. attorney's office says the money was "used to enrich Wise and Hoegel."

According to court documents, Wise and Hoegel opened the Caribbean-based Millennium Bank in 1999 and were allegedly issuing the fraudulent certificates until March 2009, when the **Securities** and Exchange Commission shut down the scheme. Victims of the scheme lost more than $75 million US, according to the indictment papers.

Wise is facing 23 counts, including conspiracy, mail and wire fraud and **money laundering**. Hoegel is charged with four counts of making and subscribing a false tax return, one count of obstruction and one count of false statements.

Calgary Herald

Document CALH000020120418e84i00007

Local / News

Four charged in $16m investment scheme; Hamilton and Halton residents invested in what police say were bogus companies; restitution ordered

Molly Hayes The Hamilton Spectator mhayes@thespec.com 905-526-3214

525 words
12 April 2012
The Hamilton Spectator
HMSP
First
A3
English

HALTON -- An estimated 150 investors, some from in and around the Hamilton-Halton region, are out millions of dollars in what police describe as a $16-million Ponzi scheme.

Four Halton residents - two of whom were jailed more than a year ago after ignoring a stop-trading order from the Ontario **Securities** Commission - are facing charges in the alleged investment scam.

Police say the investors from across southern Ontario and the United States were led to believe they were buying into offshore oil **securities**, poised to generate big profits fast.

But police allege it was a Ponzi scheme; some funds were filtered back to investors in the early rounds of investing but over five years, those investors lost $8 million.

The 18-month investigation began when one investor came forward to Halton Regional Police.

"Many, many more investors" were tracked down through banking documents, said Detective Constable Lorena Mallinson.

Six companies, all based in the Hamilton-Halton region, were investigated. They included: North American Carrier Services; Hillcorp International Services; Hillcorp Wealth Management; Suncorp Holdings (no relation to Suncor Energy); Exxon Holdings (no relation to Exxon Mobil); and Petro Properties (no relation to Petro Holdings).

Police allege the companies were essentially fronts for the scam.

"There may have been some legitimate usage that took place at some point for these companies, but not during this (investigation's) time frame," Mallinson said.

Their investigation - with assistance from the Ontario **Securities** Commission, which regulates the industry in this province - resulted in the arrests of four people.

Paul DiNardo, 52, of Burlington, is charged with two counts each of fraud over $5,000, **money laundering** and possession of proceeds of crime.

Rita DiNardo, 64, of Milton, Danny DeMelo, 43, of Milton, and Steven John Hill, 52, of Burlington, have been charged with single counts of fraud over $5,000, **money laundering**, and possession of proceeds of crime.

DeMelo and Hill were sentenced to 90 days in jail and 12 months probation last year after pleading guilty to breaching OSC cease-trade orders first made against them and their affiliated companies in July 2009, according to documents from the quasi-criminal proceedings.

At that time, Hill was listed as the sole director of "162 limited," which operated as Hillcorp International Services. DeMelo identified himself then as the senior investment adviser (CFO) of Hillcorp Wealth Management - a division of Hillcorp International.

In their OSC sentencing last year, DeMelo and Hill were also ordered to pay restitution of almost $1 million to 22 Ontario investors. Mallinson said that amount is part of the $8-million loss cited in their police investigation.

In the OSC decision, the pair and their affiliated companies - including Hillcorp International Services, Hillcorp Wealth and Suncorp Holdings - were also permanently prohibited from trading. Hill and Paul DiNardo are in custody and appear in court Thursday and Friday. The next appearance for Rita DiNardo and DeMelo is April 23.

mhayes@thespec.com

905-526-3214

Toronto Star Newspapers Limited

Document HMSP000020120412e84c00013

Vern Krishna
Business

Fraud isn't likely to disappear even with convictions

Vern Krishna

Financial Post
1043 words
29 March 2012
Victoria Times Colonist
VTC
Final
D2
English

Accounting and **securities** frauds continue unabated and in increasing amounts. The recent conviction of financier R. Allen Stanford on 13 counts of fraud involving US$7-billion - including **money laundering** and obstructing investigators - is the most recent example, but not the last.

The methods vary depending upon the underlying purpose: managing earnings to boost financial performance, stock prices and executive bonuses; evading income taxes; or just old fashioned Ponzi selling.

North America has seen its fair share of all these types of fraud over the years.

We see confidence, creative bookkeeping, and the respectability of pedigree - the essential ingredients of fraud - in McKesson & Robbins, a classic case from the late 1930s in which Canada played a leading role.

The story begins with Philip Musica - a high school dropout - twice convicted of commercial fraud. Upon his release from prison, Musica reincarnated himself as "F. Donald Coster" and upgraded his academic pedigree by conferring upon himself two advanced degrees, an MD and a PhD from Heidelberg University - the most elite and respected educational institute in Germany at that time. The newly minted "Herr Dr. Dr. Coster" then acquired McKesson & Robbins - a publicly listed pharmaceutical company on the New York Stock Exchange.

Coster wanted to make the company look successful and profit from its publicly listed shares. He incorporated a Canadian company in Windsor, hired his cousin and bought five typewriters. Coster and his cousin then created a fictitious paper financial empire. They did all the things accountants do, but without any underlying business. They typed fictitious sales, purchase and delivery invoices - each on different typewriters - and created substantial paper profits. They went through the entire accounting cycle, recording nonexistent inventories and account receivables of about $35-million on the company's books.

McKesson & Robbins had to comply with **securities** laws and the formalities of preparing financial statements. The company retained one of the most respectable blue-chip accounting firms - Price Waterhouse - as its auditors. As a director of the company testified at trial, "I just took it that when you put PW on the bottom of a statement, it was sterling silver, and everything went." The markets bought the fiction. The company's stock soared.

In 1937, auditing standards did not require auditors to "kick the tires" by physically examining inventories or confirming accounts receivables with debtors. PW auditors phoned Coster's cousin in Windsor. He confirmed that all was well with the Canadian subsidiary and that they had all assets on hand. Coster managed to conceal his fraud for 12 years, always showing substantial inventories and accounts receivable on the books from ever-increasing fictitious sales.

The bubble eventually burst and Coster put a gun to his head. The accounting profession learned a lesson and changed its auditing stan-dards to require physical inspection of all material inventories stated on the financial

statements. The company survived, too; McKesson Corp. is today one of the largest pharmaceutical and medical technology companies in the world.

In what has come to be called the Great Salad Oil Swindle of the 1960s, Anthony "Tino" DeAngelis turned to science to perpetrate his fraud. DeAngelis controlled Ally Crude Vegetable Oil and Refining Corp. Ally's auditors - having learned the risks of not physically verifying inventory in McKesson & Robbins - physically inspected the company's inventory of salad oil at a "tank farm" in New Jersey. They examined each barrel of oil and even inserted a dipstick into the tanks to ensure that they actually contained oil.

However, not all auditors are versed in Archimedean principles. Having created phantom inventory through fictitious warehouse receipts and inventory records, DeAngelis filled the tanks with water and added a little bit of oil. Since oil floats on water, the dipstick readings did not detect the depth of the oil. As the auditors moved ahead from tank to tank with their dipsticks, the company's employees repainted the numbers on the tanks behind them. Thus, as in a Marx Brothers comedy, not only did the auditors count water as oil, but they also counted the same water as oil over and over, thereby multiplying the value of the company's inventory.

The Crazy Eddie fraud had an unusual twist. Eddie Antar was an officer, director and employee of Crazy Eddie Inc., a chain of consumer electronic stores. New York-based Crazy Eddie's management initially falsified the corporate books in the traditional manner - they skimmed cash at their stores and paid employees "off the books." Management reduced corporate taxable income by approximately 20%, and the family deposited more than US$6-million between 1980 and 1983 in offshore bank accounts.

However, Antar's success became his albatross: Where to hide the skimmed money? The Antar family decided to cover up their fraud by going public! Prior to going public, however, they decided to skim less money each year. By stealing less, they increased profit margins and net income. Actual profits rose by 13% from 1980 to 1983. The company's reported profits rose by more than 170%.

The company went public in September 1984 (CRZY) on the Nasdaq at a price of about US$8. Within 18 months, Crazy Eddie stock traded at more than US$75 per share (after accounting for share splits).

The frauds would have remained undetected had it not been for Eddie's bedroom antics. Eddie became involved in an extramarital relationship and was caught out by his wife on New Year's Eve. He learned that hell hath no fury like a woman scorned. The entire fraud, which had been a nice family enterprise, unravelled. At trial, Eddie Antar admitted that he caused the value of the inventory of Crazy Eddie that he reported to the auditors to be overstated by about US$2 million.

As accounting and **securities** frauds evolve and become more sophisticated, they retain their basic features: overstate, understate and shift income between fiscal periods depending upon the ultimate goal. In respectable circles, we speak of this as "earnings management."

Vern Krishna is tax counsel with Borden Ladner Gervais LLP, and executive director of the CGA Tax Research Centre at the University of Ottawa.

vkrishna@blg.com

Victoria Times Colonist

Document VTC0000020120329e83t0002p

THE VANCOUVER SUN

David Baines
BusinessBC

West Vancouver stock promoter languishes in Austrian jail; Aly Mawji has been in prison for 10 months awaiting outcome of multimillion-dollar manipulation charges

David Baines

Vancouver Sun
955 words
29 March 2012
Vancouver Sun
VNCS
Final
D3
English

When we last left West Vancouver stock promoter Aly Babu Mawji in May 2011, he was not in West Vancouver, rather he was in jail in Austria in connection with the alleged multimillion-dollar manipulation of De Beira Goldfields Inc.

Stuttgart public prosecutor Claudia Krauth confirmed in an email this week that Mawji is still in jail. She gave no indication when the case would be dealt with.

Meanwhile, the 33-year-old promoter has sold his luxurious 6,100-sq.-ft home at 627 Kenwood Rd. in the

British Properties. It was listed for $3.79 million and ultimately sold for $3.35 million. He also leased a 2006 Ferrari F430 Spyder.

De Beira was a sham exploration company that went public on the OTC Bulletin Board in the United States in early 2006.

Immediately after clearing the company's shares for resale, the company's president, Vancouver longshoreman Mike Fronzo, handed control to a pair of Australian promoters, Reginald Gillard and Klaus Eckhof.

Gillard and Eckhof announced an option to explore a project in Colombia and - before drilling a single hole - the company's market capitalization jumped from practically nothing to $600 million US.

The stock was co-listed on the Frankfurt Stock Exchange and heavily promoted by German newsletter writer Pascal Geraths, who has also been charged in connection with the alleged manipulation. (A third man has also been charged, but his name has not been released.) Mawji was closely involved in the company's affairs. During an earlier interview, he told me he had introduced the company to the Australian promoters. Also, his personal telephone number was listed on De Beira's press releases, and the company's website was registered in his name.

In June 2006, the B.C. **Securities** Commission issued a cease-trade order against the company on grounds that it had not made proper disclosure of its mineral interests. The stock subsequently unravelled.

.

When we last left Vancouver chartered accountant James Philip on March 21, he was still serving on the board of Vancouver-based NovaGold Resources Inc. even though he and Bodog founder Calvin Ayre had been indicted three weeks earlier by the

U.S. Department of Justice for operating an illegal gambling enterprise and **money laundering**.

I noted that the U.S. charges had caught the attention of the Institute of Chartered Accountants of B.C., of which Philip is a member. "We are monitoring the situation and treating it seriously," Chris Utley, the institute's director of ethics, told me in an interview.

I also noted that unlicensed gambling and **money laundering** are also considered offences in Canada, which means that Canadian authorities - if requested by the U.S. Department of Justice - could arrest him and extradite him to the United States.

That raised the question: Would Philip appear at NovaGold's special meeting for shareholders at the Pan Pacific Hotel on Wednesday?

The question became academic on Monday when NovaGold issued a release announcing that Philip had resigned for "personal reasons." It also wished him luck (in his future endeavours).

.

The B.C. **Securities** Commission's criminal investigations team has been busy these days.

The team investigates **securities** cases with a view to prosecuting the alleged offenders in criminal court, rather than before an administrative tribunal. In court, they can get fines and jail terms. At a hearing, they can get only fines and market suspensions.

So far this month, the team has collared three alleged **securities** offenders:

. On March 6, members of the team, accompanied by Coquitlam RCMP, arrested Amir Beiklik in his Coquitlam home and charged him with one count of fraud and one count of theft. Crown counsel Brian McKinley said the case relates to about $345,000 that a woman gave to Beiklik for investment purposes between October 2004 and May 2008. The Crown alleges he diverted the money for other purposes.

. On March 7, members of the criminal prosecutions team, this time accompanied by Langley RCMP, arrested Hal (Mick) Allan McLeod at his home for breaching a lifetime ban against selling **securities**.

McLeod (who has legally changed his name to Michael Carter Smith) was the mastermind behind the Manna Humanitarian Foundation and related entities, which raised $16 million US from about 800 investors, many of them B.C. residents, between 2005 and 2007.

Investors were told their money would be used to trade foreign exchange currencies, and they would earn up to seven per cent monthly. In fact, it was a Ponzi scheme. Investors lost more than $10 million.

In August 2009, a BCSC hearing panel imposed a permanent **securities** ban on McLeod and three associates, David John Vaughan, Kenneth Robert McMordier (also known as Byrun Fox) and Diane Sharon Rosiek.

RCMP conducted a criminal investigation but ultimately decided there was not enough evidence to recommend charges.

McLeod, meanwhile, began promoting another investment scheme in Surrey called Provina Capital. BCSC enforcement staff conducted an under-cover operation, which led to him being charged with breaching his ban. In a separate matter, RCMP have charged him with uttering forged documents.

. On March 16, members of the team, this time accompanied by Nanaimo RCMP, arrested Michael Chodorowski at the Nanaimo airport and charged him with four counts of fraud, three counts of theft and one count of laundering the proceeds of crime.

Chodorowski allegedly told investors that, if they gave him money, he could generate high returns for them. The total amount of the alleged fraud is more than $2 million.

dbaines@vancouversun.com Blog: vancouversun.com/baines

Vancouver Sun

Document VNCS000020120329e83t00044

Search Summary

Text	securities AND "money laundering"
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	Canada
Language	All Languages

BUSINESS VANCOUVER

Published September 3, 2013

ECONOMY AND FINANCE

Securities fraud still largely undetected in Canada and the U.K. – CFA Institute study

Complex legal system, lack of national securities regulator and enforcement among key factors hindering stock fraud deterrence in Canada

By Richard Chu

If investors think they're less likely to get bilked by investing in companies traded on Canada's main stock exchange, they should think again.

A soon-to-be published study commissioned by the CFA Institute and conducted at York University's Schulich School of Business has found that there were more litigated securities fraud cases involving TSX-listed companies than there were for companies listed on the TSX Venture Exchange between 2005 and 2011.

Douglas Cumming, one of the study's authors, said he was surprised that there were fewer frauds detected on the junior exchange compared with the senior market.

"That was definitely not what we expected in Canada."

The study is the first of its kind to break down the number of fraud cases by stock exchange. Cumming noted there's no easy way for investors on any exchange in Canada, the U.S. or the U.K. to determine the number of frauds occurring on their respective exchanges.

In Canada, the Canadian Securities Administrators recently began listing fraud as a category within its 2012 annual enforcement report, but the organization doesn't break out where the frauds originated. It took Cumming and his team of six MBA students an entire summer to collect and compile the data from the various regulators for their study.

"It was very time-consuming to gather this information. Nowhere can you find statistics that report fraud on an exchange-by-exchange basis. We think that's quite useful information," said Cumming. "Certainly, it would help people decide where to allocate their capital and the associated risks."

On the TSX, the largest category of fraud was non-financial fraudulent misrepresentation and disclosure followed by financial fraud, illegal distribution and one litigated case of insider trading.

On the TSX Venture Exchange, illegal distribution of shares and financial fraud were the two largest fraud categories followed by fraudulent misrepresentation.

The U.K. followed the Canadian pattern with more cases involving companies listed on the country's main board, the London Stock Exchange, than on the junior Alternative Investment Market.

By comparison, the number of litigated frauds in the U.S. was highest on the non-regulated Pink Sheets, followed by the Nasdaq and the New York Stock Exchange (NYSE).

Jim Allen, the CFA's head of capital markets policy, said the study's results confirmed their expectations that smaller companies would have more problems in the U.S. But he said it was surprising that was not the case in Canada or the U.K.

Cumming warned, however, that, given the relatively low number of litigated frauds in both countries, the results underestimate securities fraud in Canada and the U.K.

According to the study, there were 3,037 litigated frauds between 2005 and 2011 in the U.S. on the three exchanges analyzed in the study but only 48 in Canada and 49 in the U.K. in the same period of time.

"Having such a low rate of fraud in Canada could infer that Canadians are super-ethical," Cumming said sardonically. "But more realistically, more needs to be done in Canada to detect fraud."

Toronto-based independent forensic auditor Al Rosen of Rosen and Associates agreed.

"Ninety per cent aren't reported," he said. "There is this feeling in Canada that you are safe. You don't have anything to worry about, and it's not just so. A lot of our cases are foreign people who have come to Canada because they know we are stupid. They know we won't prosecute; we won't even investigate."

He said the low number of litigated frauds is "a matter of where the bucks are" with lawyers having to consider if it's worth pursing and if there is a strong enough chance of winning a favourable decision.

Rosen added that part of the problem is that investors must clear a host of high legal hurdles to try to get some of their money back. The primary way investors pursue fraudsters is through class-action lawsuits, which can take years, even decades to resolve.

Brent MacLean, a Vancouver associate counsel at Davis LLP, said there are also liability caps against issuers for claims of secondary market trading fraud of $1 million or 5% of a company's market capitalization, whichever is greater.

"This is small potatoes compared [with] similar U.S. class-action claims."

The BC Securities Commission (BCSC) launched its criminal investigations team in 2007. But its success rate has been equally low. According to the BCSC, provincial Crown counsel has laid charges in only 26 cases over the past seven years. Two dozen people have been formally charged and only 10 have been convicted.

Stuart Morrow, a Vancouver partner at Davis, noted that even if investors win a favourable decision, they might still not get any money because the perpetrators are bankrupt.

"Evaluating your potential for recovery is an essential precondition to initiating litigation."

National securities regulator needed to protect investors

Cummins suggests having a national securities regulator would help simplify the process for cheated investors. Morrow noted that the CSA has done a good job in terms of preserving and protecting provincial interests and the maintenance of healthy capital markets. But "where effective action against securities perpetrators is concerned, one single national body would be more effective."

Added MacLean, "The SEC [the U.S. Securities and Exchange Commission] has much more substantial powers to commence commercial litigation than our provincial securities commissions do by a long shot to protect investors."

Morrow pointed out that increasing help for bilked investors requires far greater federal and provincial political will than exists today.

But Rosen said that before politicians do anything about Canada's securities laws, investors have to "wake up."

"We've got a system in Canada that is so backward, it's beyond belief. And yet, Canadians are willing to believe they are protected. It's exasperating. Canadians are too trusting of the system they have. There are people who think Canadians are easy prey. They just know Canadians are gullible."

Story URL: http://www.biv.com/article/20130903/BIV0102/309039912/0/BIV0109

Grant Thornton

Reporting Entity Sector Profiles: Accountants Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

Accounting Industry SIC Codes

Code	Description
872	Accounting, Auditing, and Bookkeeping Services
8721	Accounting, Auditing, and Bookkeeping Services

Accounting Industry NAICS Codes

Code	Description
5412	Accounting, Tax Preparation, Bookkeeping and Payroll Services
541211	Offices of Certified Public Accountants
541213	Tax Preparation Services
541214	Payroll Services
541219	Other Accounting Services

Establishments: Accounting, Tax Preparation, Bookkeeping and Payroll Services (NAICS 54121)

Number of establishments in Canada by type and region: December 2012
Accounting, Tax Preparation, Bookkeeping and Payroll Services (NAICS 54121)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	2,859	3,374	6,233	16.7%
British Columbia	2,952	3,594	6,546	17.6%
Manitoba	463	555	1,018	2.7%
New Brunswick	282	256	538	1.4%
Newfoundland and Labrador	190	115	305	0.8%
Northwest Territories	16	20	36	0.1%
Nova Scotia	353	318	671	1.8%
Nunavut	4	5	9	0.0%
Ontario	5,306	8,355	13,661	36.7%
Prince Edward Island	65	45	110	0.3%
Quebec	2,817	4,227	7,044	18.9%
Saskatchewan	440	582	1,022	2.7%
Yukon Territory	21	23	44	0.1%
CANADA	15,768	21,469	37,237	100%
Percent Distribution	42.3%	57.7%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments
by employment size category and region: December 2012
Accounting, Tax Preparation, Bookkeeping and Payroll Services (NAICS54121)

Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	2,333	512	11	3
British Columbia	2,276	661	12	3
Manitoba	320	136	7	0
New Brunswick	205	73	3	1
Newfoundland and Labrador	120	69	1	0
Northwest Territories	6	9	1	0
Nova Scotia	259	88	6	0
Nunavut	1	3	0	0
Ontario	4,025	1,231	41	9
Prince Edward Island	43	22	0	0
Quebec	1,975	818	17	7
Saskatchewan	302	136	2	0
Yukon Territory	15	6	0	0
CANADA	11,880	3,764	101	23
Percent Distribution	75.3%	23.9%	0.6%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Offices of Accountants (NAICS 541212)

Exclusions - Establishments primarily engaged in:

- providing tax return preparation services, without also providing accounting or auditing services (541213, Tax Preparation Services); and
- providing bookkeeping, billing and payroll processing services, without also providing accounting or auditing services (541215, Bookkeeping, Payroll and Related Services).

Number of establishments in Canada by type and region: December 2012
Offices of Accountants (NAICS 541212)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	1,992	1,873	3,865	18.0%
British Columbia	1,926	1,815	3,741	17.4%
Manitoba	316	292	608	2.8%
New Brunswick	192	144	336	1.6%
Newfoundland and Labrador	101	69	170	0.8%
Northwest Territories	9	12	21	0.1%
Nova Scotia	222	167	389	1.8%
Nunavut	2	1	3	0.0%
Ontario	3,238	4,021	7,259	33.8%
Prince Edward Island	40	19	59	0.3%
Quebec	1,852	2,543	4,395	20.5%
Saskatchewan	280	333	613	2.9%
Yukon Territory	7	5	12	0.1%
CANADA	10,177	11,294	21,471	100%
Percent Distribution	47.4%	52.6%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments
by employment size category and region: December 2012
Offices of Accountants (NAICS541212)

Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	1,618	367	5	2
British Columbia	1,439	482	3	2
Manitoba	217	96	3	0
New Brunswick	136	53	3	0
Newfoundland and Labrador	59	42	0	0
Northwest Territories	5	3	1	0
Nova Scotia	157	63	2	0
Nunavut	1	1	0	0
Ontario	2,405	817	10	6
Prince Edward Island	26	14	0	0
Quebec	1,240	599	8	5
Saskatchewan	187	91	2	0
Yukon Territory	5	2	0	0
CANADA	7,495	2,630	37	15
Percent Distribution	73.6%	25.8%	0.4%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Tax Preparation Services (NAICS 541213)
Exclusions - Establishments primarily engaged in providing a range of accounting services (541212, Offices of Accountants).

Number of establishments in Canada by type and region: December 2012
Tax Preparation Services (NAICS 541213)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	168	142	310	14.0%
British Columbia	189	164	353	16.0%
Manitoba	47	52	99	4.5%
New Brunswick	25	16	41	1.9%
Newfoundland and Labrador	30	3	33	1.5%
Northwest Territories	5	0	5	0.2%
Nova Scotia	40	21	61	2.8%
Nunavut	0	1	1	0.0%
Ontario	448	504	952	43.1%
Prince Edward Island	7	4	11	0.5%
Quebec	115	129	244	11.0%
Saskatchewan	58	38	96	4.3%
Yukon Territory	1	2	3	0.1%
CANADA	1,133	1,076	2,209	100%
Percent Distribution	51.3%	48.7%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments
by employment size category and region: December 2012
Tax Preparation Services (NAICS541213)

Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	119	47	1	1
British Columbia	136	53	0	0
Manitoba	31	16	0	0
New Brunswick	14	11	0	0
Newfoundland and Labrador	21	9	0	0
Northwest Territories	0	5	0	0
Nova Scotia	30	10	0	0
Nunavut	0	0	0	0
Ontario	324	123	1	0
Prince Edward Island	5	2	0	0
Quebec	73	41	1	0
Saskatchewan	31	27	0	0
Yukon Territory	0	1	0	0
CANADA	784	345	3	1
Percent Distribution	69.2%	30.5%	0.3%	0.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Bookkeeping, Payroll and Related Services (NAICS 541215)
Exclusions - Establishments primarily engaged in:

- providing a range of accounting services (541212, Offices of Accountants); and
- providing tax return preparation services, without also providing accounting or auditing services (54213, Tax Preparation Services).

Number of establishments in Canada by type and region: December 2012
Bookkeeping, Payroll and Related Services (NAICS 541215)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	699	1,359	2,058	15.2%
British Columbia	837	1,615	2,452	18.1%
Manitoba	100	211	311	2.3%
New Brunswick	65	96	161	1.2%
Newfoundland and Labrador	59	43	102	0.8%
Northwest Territories	2	8	10	0.1%
Nova Scotia	91	130	221	1.6%
Nunavut	2	3	5	0.0%
Ontario	1,620	3,830	5,450	40.2%
Prince Edward Island	18	22	40	0.3%
Quebec	850	1,555	2,405	17.7%
Saskatchewan	102	211	313	2.3%
Yukon Territory	13	16	29	0.2%
CANADA	4,458	9,099	13,557	100%
Percent Distribution	32.9%	67.1%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments
by employment size category and region: December 2012
Bookkeeping, Payroll and Related Services (NAICS541215)

Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	596	98	5	0
British Columbia	701	126	9	1
Manitoba	72	24	4	0
New Brunswick	55	9	0	1
Newfoundland and Labrador	40	18	1	0
Northwest Territories	1	1	0	0
Nova Scotia	72	15	4	0
Nunavut	0	2	0	0
Ontario	1,296	291	30	3
Prince Edward Island	12	6	0	0
Quebec	662	178	8	2
Saskatchewan	84	18	0	0
Yukon Territory	10	3	0	0
CANADA	3,601	789	61	7
Percent Distribution	80.8%	17.7%	1.4%	0.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Searches from Onesource

Sic Code – 8721 - Accounting, Auditing, and Bookkeeping Services

Province	Number of Establishments
Alberta	1,386
British Columbia	1,940
Manitoba	290
New Brunswick	218
Newfoundland and Labrador	75
Northwest Territories	13
Nova Scotia	268
Nunavut	3
Ontario	3,006
Prince Edward Island	34
Quebec	1,520
Saskatchewan	354
Yukon	26
Total	9,133

Source: Onesource

NAICS Code – 541211- Accounting, Tax Preparation, Bookkeeping and Payroll Services

Province	Number of Establishments
Alberta	1,697
British Columbia	2,197
Manitoba	411
New Brunswick	301
Newfoundland and Labrador	172
Northwest Territories	17
Nova Scotia	386
Nunavut	3
Ontario	2,176
Prince Edward Island	54
Quebec	2,036
Saskatchewan	439
Yukon	28
Total	9,917

Source: Onesource

NAICS Code – 541213- Tax Preparation Services

Province	Number of Establishments
Alberta	312
British Columbia	262
Manitoba	121
New Brunswick	83
Newfoundland and Labrador	97
Northwest Territories	4
Nova Scotia	119
Ontario	1,366
Prince Edward Island	20
Quebec	526
Saskatchewan	88
Yukon	2
Total	3,000

Source: Onesource

NAICS Code – 541214- Payroll Services

Province	Number of Establishments
Alberta	9
British Columbia	17
Manitoba	8
Newfoundland and Labrador	3
Nova Scotia	6
Ontario	39
Prince Edward Island	1
Quebec	19
Saskatchewan	2
Total	104

Source: Onesource

NAICS Code – 541219- Other Accounting Services

Province	Number of Establishments
Alberta	325
British Columbia	491
Manitoba	70
New Brunswick	37
Newfoundland and Labrador	19
Northwest Territories	5
Nova Scotia	112
Nunavut	1
Ontario	781
Prince Edward Island	17
Quebec	235
Saskatchewan	108
Yukon	13
Total	2,214

Source: Onesource

Canada's Accounting Top 30

Rank by Revenue 2013	Rank by Revenue 2012	Accountant/Year End/ Head Office	Revenue 2013 ($000)	Revenue change (%)	Partners / Principals (#/-)	Professional Staff (#/-)	Revenue per professional staff	Number of offices	Revenue splitting A/A/M&C/ Tax/Other
1	1	Deloitte LLP / June 1, 2013 / Toronto	1,776,000	-5.6	865 (+2)	5,316 (-145)	334,086	55 (-1)	N/A
2	2	PricewaterhouseCoopers LLP / June 30, 2013 / Toronto	1,211,200	0.7	513 (-18)	4,263 (+132)	284,119	25	N/A
3	3	KPMG LLP / Sept. 30, 2013 / Toronto	1,203,102	3.5	696 (+35)	3,795 (+240)	317,023	37 (+2)	N/A
4	4	Ernst & Young LLP / June 28, 2013 / Toronto	968,000	6.3	358 (+17)	2,992 (+166)	323,529	17	N/A
5	5	Grant Thornton Canada[1] / December 31, 2013 / Toronto	582,000	6.8	404 (-5)	2,983 (+146)	195,106	135	N/A
6	7	MNP LLP / December 31, 2013 / Calgary	487,000	13.3	357 (+28)	1,026 (+108)	474,659	58	N/A
7	6	BDO Canada LLP / December 31, 2013 / Toronto	465,000	4.3	392 (+9)	2,229[2] (+106)	208,614	111 (+6)	N/A
8	8	Collins Barrow National Co-operative / Dec. 31, 2013 / Kitchener, Ont.	177,570	13.2	207 (+24)	541 (+46)	328,226	41 (+4)	N/A
9	9	Richter / December 31, 2013 / Montreal	80,289	0.4	58 (+10)	415 (+78)	193,467	2 (+1)	40/25/30/5
10	10	Mallette / August 31, 2013 / Québec	63,982	13.0	66 (+7)	472 (+30)	135,555	24 (+2)	60/15/20/5

[1] Includes Grant Thornton LLP and Raymond Chabot Grant Thornton (Quebec)
[2] BDO Canada's 2012 professional staff count amended to 2,123

Rank by Revenue 2013	Rank by Revenue 2012	Accountant/Year End/ Head Office	Revenue 2013 ($000)	Revenue change (%)	Partners / Principals (#/-)	Professional Staff (#/-)	Revenue per professional staff	Number of offices	Revenue splitting A/A/M&C/ Tax/Other
11	11	HLB/ Schwartz Levitsky Feldman / Dec. 31, 2013 / Montreal	38,000	-4.0	46 (-2)	176 (-8)	215,909	7	66/4/17/13
11	12	Crowe MacKay LLP / December 31, 2013 / Vancouver	38,000	-0.8	36	171 (-9)	222,222	7	69/6/18/7
13	13	Crowe Soberman LLP / December 31, 2013 / Toronto	35,309	-0.4	23	86 (-23)	410,570	1	66/8/18/8
14	14	Welch LLP / January 26, 2014 / Ottawa	26,800	-3.9	38 (-8)	227 (+67)	118,062	12	74/3/17/6
15	15	PSB Boisjoli LLP / December 31, 2013 / Montreal	22,918	4.4	17	70 (+13)	327,400	1	48/27/19/6
16	17	Ginsberg Gluzman Fage & Levitz LLP/ Dec. 31, 2013 / Ottawa	21,725	7.3	12 (+2)	80 (+5)	271,563	9	35/2/10/53
17	18	KNV Chartered Accountants LLP / Dec. 31, 2013 / Surrey, B.C.	21,045	4.7	13	123 (+22)	171,098	3	52/6/37.5/4.5
18	19	Manning Elliot LLP / December 31, 2013 / Vancouver	20,050	0.3	23 (+1)	97 (-8)	206,701	2	79/5/16/0
19	16	Davidson & Company LLP / December 31, 2013 / Vancouver	19,000	-9.5	15 (+1)	62 (-16)	306,452	1	80/0/20/0
20	24	Demers Beaulne / December 31, 2013 / Montreal	18,672	14.4	15	79 (-1)	236,354	1	50/18/32/0

Rank by Revenue 2013	Rank by Revenue 2012	Accountant/Year End/ Head Office	Revenue 2013 ($000)	Revenue change (%)	Partners / Principals (#/-)	Professional Staff (#/-)	Revenue per professional staff	Number of offices	Revenue splitting A/A/M&C/ Tax/Other
21	20	Millard Rouse & Rosebrugh LLP / July 31, 2013 / Brantford, Ont.	18,562	0.1	21 (-2)	70 (+6)	265,171	6	67/7/23/2
22	22	Zeifmans LLP / January 31, 2014 / Toronto	18,550	6.0	12 (+1)	63 (+3)	294,444	1	54/16/30/0
23	21	DMCL LLP / December 31, 2013 / Vancouver	18,350	0	17 (+2)	78 (-84)	235,256	3	68/1/31
24	25	Durward Jones Barkwell & Co. LLP / Dec. 31, 2013 / St. Catharines, Ont.	16,685	3.1	25 (-4)	72 (+27)	231,736	8	55/15/19/11
25	23	Smythe Ratcliffe LLP / December 31, 2013 / Vancouver	16,241	-4.9	13	101 (-20)	160,802	4	72/0/12.5/15.5
26	27	Kingston Ross Pasnak LLP / Dec. 31, 2013 / Edmonton	15,402	13.7	18 (+2)	65 (+7)	236,954	2 (+1)	62/4/24/10
27	28	Lemieux Nolet / August 31, 2013 / Levis, Quebec	13,327	1.1	19	76 (+1)	175,355	4	68/3/15/14
28	30	RLB LLP / December 31, 2013 / Guelph, Ont.	12,932	5.3	12 (-1)	74 (+33)	174,757	3	54/9/29/8
29	29	Wolrige Mahon LLP / December 31, 2013 / Vancouver	12,700	2.4	18 (+1)	70	181,429	1	65/15/20/0
30	--	Segal LLP / December 31, 2013 / Toronto	12,622	3.2	13 (-5)	26 (-9)	485,462	1	80/3/16/1

Source: The Bottom Line – April 2014

Accounting Industry - Market Value
Canada Accountancy Market Value: US$ billion, 2008-2012

Year	US$ billion	% Growth
2008	11.3	
2009	11.6	1.9%
2010	11.6	0.5%
2011	11.9	2.2%
2012	11.9	0.2%
Compound Annual Growth Rate (CAGR): 2008-2012		1.2%

Source: MarketLine, August 2013

Accounting Industry - Market Value Forecast
Canada Accountancy Market Value Forecast: US$ billion, 2012-2017

Year	US$ billion	% Growth
2012	11.9	0.2%
2013	12.0	0.8%
2014	12.1	1.2%
2015	12.3	1.3%
2016	12.5	1.4%
2017	12.6	1.4%
Compound Annual Growth Rate (CAGR): 2012-2017		1.2%

Source: MarketLine, August 2013

Accounting Industry – Market Segmentation
Canada's Accountancy Market Category Segmentation: US$ billion, 2012

Category	2012	%
Audit	5.2	43.7%
Advisory	3.6	30.3%
Tax	3.1	26.0%
Total	11.9	100%

Source: MarketLine, August 2013

Accounting Services – Canada - $ millions

	2008	2009	2010	2011	2012p
Operating revenue	12,796.80	13,197.20	13,942.50	14,274.90	14,959.20
Operating expenses	9,191.60	9,517.80	10,034.00	10,192.10	10,777.70
Salaries, wages and benefits	5,142.10	5,338.60	5,577.90	5,674.40	6,009.70
Operating profit margin	28.20%	27.90%	28%	28.60%	28%

Source: Statistics Canada

Appendix B: Examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Vatican official charged with money laundering. Associated Press, Jan 21, 2014.
2. Ex-Vatican accountant hit with new money laundering charge. Digital Journal, January 21, 2014.
3. Accountant sentenced for money laundering. Montreal Gazette, January 15, 2014.
4. Mississauga chartered accountant sentenced to jail and fined for tax fraud scheme. Canada Revenue Agency. May 6, 2013.
5. Ontario court approves $117-million settlement with Sino-Forest auditors. Globe and Mail, March 20, 2013.
6. Livent auditors appeal misconduct ruling. Canadian Business, June 6, 2008.
7. Corrupt tax auditor gets three years. The Toronto Star, Jan 29, 2014.
8. Former accountant gets 7-year prison term for tax fraud. Torstar News Service, June 17, 2013.
9. OSC accuses Ernst & Young of shoddy audit of TSX Venture-listed Zungui Haixi. The Globe and Mail, June 24, 2013.
10. Accountant sentenced for money laundering. The Champion, January 17, 2014.
11. Accountancy giant EY's GBP750,000 Farepak fine. The Scotsman, December 20, 2013.
12. KPMG pays €7 million to settle Dutch bribery case. The FCPA Blog, January 13, 2014.
13. Deloitte to pay $2 million to settle charges over audit rule violations. Reuters, October 22, 2013.
14. Deloitte fined $10mn in US money laundering case. Live mint. June 19, 2013.
15. Big Four Chinese units face US suspension. ICAS.org.UK, Jan 23, 2014
16. KPMG to pay USD 8.2m to settle SEC auditing charges. Deccan Herald, January 24, 2014.
17. PWC fined $2.17 million by U.K. regulator over JP Morgan client-money audit. Bloomberg, January 5, 2012

18. Accountants fined pounds 14m over MG Rover; Watchdog says Deloitte in serious ethical breaches: Record-breaking penalty for Phoenix Four advisors. The Guardian, September 10, 2013.

19. Deloitte under investigation over Rover; Nearly seven years after the collapse of car manufacturer MG Rover, its advisor Deloitte has been placed under investigation by industry regulators. The Telegraph Online, February 2, 2012.

20. MG Rover debacle can't hide accounting regulation failures. The Conversation, September 10, 2013.

21. When accountants play role of bankers. The New York Times, September 13, 2013.

22. The Big Four's new math; A decade after Sarbanes-Oxley forced them to scale back on consulting work, accounting giants are beefing up the business of dishing out advice. Crain's Chicago Business, October 7, 2013.

23. Former Detroit public schools accountant sentenced on fraud and money laundering charges. Federal Bureau of Investigation, December 18, 2013.

24. Accountants' professional conduct in relation to taxation. Lexology. March 18, 2014.

25. Auditors at big firms cited for more deficiencies. CFO Journal, October 1, 2013

Vatican Official Charged With Money Laundering

NICOLE WINFIELD, ASSOCIATED PRESS ON JAN 21, 2014

VATICAN CITY (AP) — A Vatican monsignor already on trial for allegedly plotting to smuggle 20 million euros ($26 million) from Switzerland to Italy was arrested Tuesday in a separate case for allegedly using his Vatican bank accounts to launder money.

Financial police in the southern Italian city of Salerno said Monsignor Nunzio Scarano, dubbed "Monsignor 500" for his purported favored banknotes, had transferred millions of euros in fictitious donations from offshore companies through his accounts at the Vatican's Institute for Religious Works.

Police said they seized 6.5 million euros in real estate and bank accounts Tuesday, including Scarano's luxurious Salerno apartment, filled with gilt-framed oil paintings, ceramic vases and other fancy antiques.

A local priest was also placed under house arrest and a notary public was suspended for alleged involvement in the money-laundering plot. Police said in all, 52 people were under investigation.

Scarano's lawyer, Silverio Sica, said his client merely took donations from people he thought were acting in good faith to fund a home for the terminally ill. He conceded, however, that Scarano used the money to pay off a mortgage.

"We continue to strongly maintain the good faith of Don Nunzio Scarano and his absolute certainty that the money

came from legitimate donations," Sica told The Associated Press.

The Salerno investigation was already under way when Scarano was arrested in June in Rome on the smuggling accusations.

Police and Sica have said the money involved in both the Swiss smuggling case and the Salerno money-laundering case originated with one of Italy's most important shipping families, the d'Amicos.

On Tuesday, financial police said more than 5 million euros had been made available to Scarano by the D'Amicos via offshore companies.

Police and Sica described the laundering plot as follows: Scarano allegedly withdrew 555,248 euros from his Vatican account in cash in 2009 and brought it into Italy. Since he couldn't deposit it in an Italian bank without drawing suspicion, he selected 50 friends to accept 10,000 euros apiece in cash in exchange for a check or wire transfer in that same amount.

The money then went to pay off a mortgage on a Salerno property held in the name of a company Scarano partly owned.

The D'Amico family, from Scarano's hometown of Salerno, denied its involvement in a July 1 statement. Their communications firm did not immediately respond to a request seeking new comment Tuesday. No one in the family has been arrested in either case.

Scarano was fired from his job as an accountant in the Vatican's main financial office and Vatican prosecutors seized the 2.3 million still in his accounts after his arrest.

The Vatican's top prosecutor said last week that the Holy See had responded to two official requests from Italy for information about Scarano's accounts, while making its own request to Italian authorities for help in its own money-laundering investigation of him.

The Vatican's own investigation into Scarano's banking activity showed that some 7 million euros had come into and out of his Vatican accounts over the past decade.

The Vatican's documentation arrived on Salerno prosecutors desks in recent weeks, leading to his re-arrest on Tuesday, Italian media reported.

Scarano's original arrest in June led to the resignations of the Vatican bank's top two managers and accelerated efforts to make the troubled institute conform to international anti-money-laundering norms.

Pope Francis has made reforming the bank a priority and has named a fact-finding commission to look into its activities and legal structure.

Scarano's initial arrest in the smuggling case was reduced to house arrest because of his ailing health. Sica said the prelate would serve the new arrest warrant also under house arrest.

In the Rome smuggling case, prosecutors say Scarano, a financier and a carabinieri officer devised an elaborate plot to transport 20 million euros in a private jet from Switzerland to Italy avoid paying customs duties. The plot

fell apart because the financier reneged at the last minute.

Sica has said Scarano in that case was merely acting as a middleman.

Ex-Vatican accountant hit with new money laundering charge

Posted Jan 21, 2014 by Dario Thuburn (AFP)

A former Vatican accountant already under house arrest and on trial for alleged corruption and attempted money laundering has been notified of fresh charges against him, Italy's financial police said on Tuesday.

, Italy's financial police/AFP

This handout picture taken from a video released by the Italian financial police on June 28, 2013 shows Nunzio Scarano (front left) shortly after he was arrested in Rome

A former Vatican accountant already under house arrest and on trial for alleged corruption and attempted money laundering has been notified of fresh charges against him, Italy's financial police said on Tuesday.

The police said in a statement that they had seized Monsignor Nunzio Scarano's luxury 17-room apartment and blocked nearly 9.0 million euros ($12 million) on current accounts linked to the senior Italian cleric.

The Vatican in July last year said it had already frozen assets belonging to Scarano and the police on Tuesday said these funds amounted to 2.2 million euros.

"This is very significant," the police said in a statement, a reference to unprecedented levels of cooperation between Vatican and Italian judicial authorities on a high-profile financial crime case.

Vatican bank spokesman Max Hohenberg told AFP: "All activity on his accounts over the past 10 years has been extracted, analysed and submitted to authorities.

"This investigation is based on information provided by the Vatican," he said.

The police said a priest in Scarano's hometown of Salerno who was an aide to the monsignor, Father Luigi Noli, has also been charged and put under house arrest.

A total of 52 people are being investigated in the case, including a notary who allegedly helped organise the money laundering scheme and lawyers, doctors and businesspeople who are suspected of making use of it.

Scarano is accused of taking cheques marked "Donation for the Poor" and in return giving cash from accounts at the Vatican bank, officially known as the Institute of Religious Works or IOR under its Italian acronym.

The police said they had seized two bank accounts at a branch near the Vatican of Italy's UniCredit, one in Scarano's name and the other belonging to a company in which the prelate held 99 percent of shares.

One of the cash withdrawals made by Scarano and traced by police was for 588,248 euros and the police said he gave it to 50 people and used it to pay back a mortgage.

Gabriel Bouys, AFP/File

The headquarters of the Institute for Religious Works (IOR) in the Vatican, on February 18, 2012

They said they managed to find at least five million euros that Scarano "had at his disposal" and alleged he made extensive property investments in Salerno.

The prelate's lawyer, Silverio Sica, said his client used the money for charity and could not be responsible for the provenance of donations he received.

"These are donations we received over the years from wealthy people. They are free donations. It is not up to us to say where the money came from," he told AFP.

Silverio Sica said the latest accusations had been a "blow" for Scarano and that he had requested that a psychiatrist be allowed to visit him, adding: "He is completely in shock, he is very disoriented."

The police said their suspicions were first aroused in January 2013 when Scarano reported a theft from his home of "several million euros' worth of valuables".

They said the sum was "significantly disproportionate" to Scarano's declared income.

Scarano was arrested in June of last year on suspicion of being an intermediary for suspect payments from Monaco to Italy, carried out through the Vatican bank.

The clergyman has since been suspended from his duties as chief accountant for APSA, the organisation that manages the Vatican's vast real estate portfolio.

Investigators said Scarano used IOR accounts to make transfers to friends and attempted to repatriate from Switzerland 20 million euros that were untaxed, on behalf of a family of ship owners from Naples.

Scarano's trial started in December last year.

The Vatican, the world's smallest sovereign state, has launched a series of reforms aimed at bringing its bank into line with international standards against money laundering.

The bank has been plagued by scandals in the past and its former president, Paul Marcinkus, sheltered in the Vatican for years to fight off repeated attempts by Italian judicial authorities to arrest him in the 1980s.

The Gazette

News

Accountant sentenced for money laundering

PAUL CHERRY

The Gazette
542 words
15 January 2014
Montreal Gazette
MTLG
Early
A6
English

An **accountant** arrested as part of an investigation into an alleged plot to launder dirty money through the construction of residential developments has been sentenced to a threeyear prison term for his role in the affair.

Jean Siminaro, 47, appeared relaxed as a special constable placed handcuffs on him before he entered the prisoner's dock in the third-floor courtroom at the Montreal courthouse, where Superior Court Justice Claude Champagne delivered the sentence. The prison term was part of a joint recommendation, so there was no element of surprise for Siminaro. He even shared a joke with a special constable as he was cuffed.

Last year, Siminaro pleaded guilty to conspiracy, **money laundering** and a gangsterism charge.

The **accountant** was arrested in 2009 and charged, along with 13 other people, in Operation Diligence, a Sûreté du Québec investigation into Normand Marvin (Casper) Ouimet, 44, alleged to be a member of the Hells Angels, and his involvement with construction companies. The case against Ouimet and eight other people is still pending as Champagne continues to hear motions filed in the case. Champagne has placed a general publication ban on all evidence presented in the case because of the possibility it will eventually be heard by a jury. For that reason, details of Siminaro's role in the plot cannot be published.

His lawyer, Marc Labelle, read from a statement detailing what Siminaro did. He also noted that Siminaro has no criminal record and, previous to his arrest, was very active as a volunteer coach for youth soccer, hockey and football programs in Repentigny. Labelle suggested the sentence will take a heavy toll on Siminaro's personal life. He is a father of three and has already been stripped of his professional title.

The defence lawyer suggested that the Parole Board of Canada tends to be tough on inmates who have been convicted of a gangsterism charge and Labelle made reference to a civil lawsuit Siminaro is facing. It appears to be a reference to a $750,000 lawsuit that a construction company filed against Siminaro last year.

"We both added water to the wine," Labelle said in reference to the negotiations with prosecutor Marlene Archer to reach an agreement on the length of the sentence. "It's his first sentence, so three years is not nothing."

Archer said that while Siminaro had no criminal record before his arrest "that is often the way it is in **money laundering** cases." She also said the recommended sentence was in line with what two other men - François Boivin, 54, and Yves Lafontaine, 48 - arrested in Operation Diligence have already received. Both men were sentenced to twoyear prison terms after pleading guilty to gangsterism charges filed in Operation Diligence.

Champagne described the sentence recommendation as "more mild than harsh" before he agreed with it. He

also wished Siminaro "good luck" before he was led away into custody.

"I hope there isn't a next time," Champagne said.

"I hope so, too," Siminaro replied.

pcherry@montrealgazette.com

GAZETTE FILES / Normand Marvin (Casper) Ouimet, the focus of Operation Diligence.; GAZETTE FILES / Normand Marvin (Casper) Ouimet, the focus of Operation Diligence. [MTGZ_20140115_Early_A6_01_I001.jpg];

Montreal Gazette

Document MTLG000020140115ea1f0001u

Mississauga chartered accountant sentenced to jail and fined for tax fraud scheme

Brampton, Ontario, May 6, 2013...The Canada Revenue Agency (CRA) announced today that Mr. Imad Kutum pleaded guilty on November 27, 2012 in the Ontario Court of Justice in Brampton, to one count of fraud over $5,000 under the *Criminal Code*. He was sentenced to two years in jail and a fine of $100,000.

Mr. Kutum, a chartered accountant, operated Kutum and Associates, providing tax preparation services and accounting related services. A CRA investigation discovered that false charitable donation claims totalling $3,674,000 were made on 487 income tax returns prepared by Mr. Kutum for clients for the 2003 to 2008 tax years. The false claims were supported by fraudulent charity receipts. The false claims reduced the amount of federal taxes owed by $1,045,111.

The information in this news release was obtained from the court records.

"Canadian taxpayers must have confidence in the fairness of the tax system," said Darrell Mahoney, Assistant Commissioner, Ontario Region, CRA. "To maintain that confidence, the Canada Revenue Agency is determined to hold tax evaders accountable for their actions."

Taxpayers who claim false expenses, credits or rebates from the government are subject to serious consequences. They are liable not only for corrections to their tax returns and payment of the full amount of tax owing, but also to penalties and interest. In addition, if convicted of tax evasion, the court may fine them up to 200% of the tax evaded and sentence them for up to a five-year jail term.

Taxpayers who have not filed returns for previous years, or who have not reported all of their income, can still voluntarily correct their tax affairs. They may not be penalized or prosecuted if they make a valid disclosure before they become aware of any compliance action being initiated by the CRA against them. These taxpayers may only have to pay the taxes owing, plus interest. More information on the Voluntary Disclosures Program (VDP) can be found on the CRA's Web site at www.cra.gc.ca/voluntarydisclosures.

Further information on convictions can also be found in the Media Room on the CRA website at www.cra.gc.ca/convictions.

-30-

For media information:

Keith Brooks
Manager, Communications
(519) 675-3248

Date modified: 2013-05-06

THE GLOBE AND MAIL

Ontario court approves $117-million settlement with Sino-Forest auditors

JEFF GRAY - LAW REPORTER
The Globe and Mail
Published Wednesday, Mar. 20 2013, 8:15 PM EDT
Last updated Thursday, Mar. 21 2013, 1:48 PM EDT

An Ontario judge has approved a $117-million deal to settle allegations levelled by investors in Sino-Forest Corp. against Ernst & Young LLP for allegedly failing to properly scrutinize the books of the scandal-plagued company.

The ruling, issued on Wednesday, dismisses objections to the deal raised by a small group of investment funds with holdings in the insolvent Toronto-based Chinese forestry firm. Sino-Forest had a market capitalization of $6-billion before a short seller alleged the company was a "Ponzi scheme" in June, 2011, and caused its shares to plummet.

More Related to this Story

- LITIGATION Sino-Forest investors face off over deal with auditors
- Getting to the bottom of the Griffiths Energy bribery case
- COURTS Burned Sino-Forest investors squabble among themselves

The E&Y deal, first announced last year, would see Sino-Forest's primary auditors settle the allegations against them contained in a $9.18-billion class-action lawsuit launched on behalf of Sino-Forest investors against the company, its former executives, auditors and underwriters. E&Y did not admit liability as part of the deal.

The accounting firm still faces serious allegations from the Ontario Securities Commission that it showed a "lack of diligence" in reviewing the documentation of Sino-Forest's purported ownership of standing timber reserves in China. E&Y has denied those allegations and says its work met professional accounting standards. Sino-Forest and some of its former senior executives are also facing OSC fraud allegations, and the RCMP launched an investigation in the case.

The E&Y settlement was first announced as part of Sino-Forest's court-supervised restructuring to transfer the company's subsidiaries to its debt holders after no suitable buyer could be found. But the deal immediately stirred up a controversy.

Lawyers acting for the group of dissident Sino-Forest investors, which includes Invesco Canada Ltd.,

Northwest & Ethical Investments LP and Comité Syndical National de Retraite Bâtirente Inc., tried to block the settlement.

They argued it unfairly precluded them from opting out of the class-action and suing Ernst & Young on their own, by wrongly using Sino-Forest's insolvency court proceedings as a shield. They also questioned whether the settlement, which proponents say is the biggest ever extracted from an auditor in a case like this in Canada, was adequate.

But Mr. Justice Geoffrey Morawetz of the Ontario Superior Court dismissed their arguments, saying that class-actions have often been settled in the same way, as part of an insolvency proceeding. A lawyer for the investment firms could not be reached for comment. It was not known if the group would seek to appeal the ruling.

Sino-Forest's restructuring deal also includes a list of other defendants in the class action, such as some of the company's former directors and executives, who would be eligible to negotiate settlements similar to Ernst & Young's.

But Dimitri Lascaris, a class-action lawyer for the Sino-Forest investors, said no such deals are in the works before April, when the lawsuit is due back in court: "Our intention is to pursue these claims vigorously."

Livent auditors appeal misconduct ruling

While lawyers representing Livent co-founders Garth Drabinsky and Myron Gottlieb were trying to convince a criminal court judge that their clients were not guilty of criminal fraud charges in connection with the collapse of the theatre company, a second set of lawyers representing the auditors from Deloitte & Touche were in a courtroom of another sort trying to overturn the decision of a panel of accounting judges who ruled their clients' handling of Livent's audit amounted to professional misconduct. Over the past week lawyers representing former Livent auditors Douglas Barrington, Claudio Russo and Anthony Power have been arguing before the Institute of Chartered Accountants of Ontario Appeals Committee that a rulingby the ICAO disciplinary panel last February erred in finding their clients guilty of professional misconduct. The panel ruled that the accountants failed to exercise the required professional skepticism when they continued to rely on the representations of the company's senior managers even after company officials lied to them. "The auditors said that their skepticism was `sky high,'" the panel ruled last year. "However, with respect to the impugned conduct, the evidence disclosed that the auditors failed to exercise the professional skepticism required." The panel could have thrown the men out of the accounting profession, but instead ordered the three receive written reprimands and pay fines and penaltiesof more than $1.25 million the highest fine ever meted out by the Institute that oversees the professional conduct of Ontario's chartered accountants. Two of the Deloitte auditors Douglas Barrington and Anthony Power have retired. Only Claudio Russo remains employed with Deloitte. The accountants were never charged with failing to detect the alleged massive fraud that ultimately destroyed the once high-flying theatre company. However, the appeal touches on some of the most contentious and important issues regarding how auditors deal with company managers, namely: just how much trust should accountants place in the representations of managements and how should auditors react once it has been proven that managers have lied to their auditors? Besides a host of legal and procedural grounds, the appeal of the accountants essentially boils down to three main issues: first, the accountants were found guilty of conduct for misbehaviour that was not included in the original charges; second, that the

panel ignored the evidence of experts who testified that the accountants did act appropriately and lastly, that the panel's finding that the auditors reach "a correct conclusion" in their audit work is incompatible with the legal definition of professional misconduct. The accountants are asking the panel to set aside the decision, as well as to strike down the fines levied against them. Much of the evidence in the original disciplinary panel ruling, as well as the appeal, centres on how the Deloitte accountants dealt with the issue of a secret "Put Agreement" between Livent and Dundee Realtyregarding redevelopment of the Pantages Theatrein Toronto that allowed Dundee to pull out of the project ahead of other investors. Livent managers told Deloitte the agreement had been cancelled since the agreement would disqualify Livent from booking any revenue associated with the project until a later time. However, Deloitte accountants auditing Dundee"s books learned the agreement had not been cancelled and was, in fact, still in place. The accountants demanded letters of explanation from Livent co-founder Myron Gottlieb (who was also a member of the audit committee of Dundee Realty's parent company), and Dundee and Livent's outside lawyers. All three provided letters that said the agreement had already been cancelled. However, explanations as to when and how the agreement was dropped differed significantly. Those inconsistencies should have cast doubt on all of the assertions of Livent's managers and caused Deloitte to increase its scrutiny of the company, the panel ruled. "The auditors failed to consider the broader implications of the admitted deception, including the representations made by management throughout the audit," the panel said in their original ruling. But considerations about the Dundee agreement should not have been used to determine professional misconduct since the original charges made no mention of it, lawyers for the accountants argue. "By making the Put Agreement, an aspect of the fraud and a matter that was not a subject of the Charges, `fundamentally important` to its decision the Panel materially changed the case against [the accountants] and unjustly denied them a fair hearing," lawyers for the accountants argue. And even if the panel does choose to consider the impact of the Put Agreement, there is not enough evidence to prove that the agreement was still in effect at the time of the audit, the lawyers contend. After all, there was no evidence that Livent managers were lying about the cancellation of the put and even a re-audit of Livent's books after the massive alleged fraud was uncovered, failed to determine once and for all whether the agreement was still in force or not. Lawyers representing the ICAO's professional standards committee argue just the opposite. There was not enough evidence for the auditors to conclude the put was cancelled in the first place. The fac

that accountants who re-audited the books after the fraud was discovered could not determine whether the Put Agreement was in force or not proves the original auditors did not have enough evidence to allow Livent to recognize the revenue in the first place. "The appellants did not have sufficient appropriate audit evidence to conclude that the representations of management were true," committee lawyers write (wrote?) in their response to the accountants' appeal. "Notwithstanding the lack of audit evidence they released their audit opinion based upon the representations of management." The fact that managers lied should have caused a reasonable accountant to re-assess every decision made in the audit that was based on representations of management, professional committee lawyers say. "(They) did not revisit the representations of management as required by generally accepted standards of practice of the profession." The put agreement was not included in the original charges because the accused accountants themselves introduced most of the evidence relating to the agreement hoping it would bolster their case that they were innocently duped by Livent's managers. However, the disciplinary committee saw it as evidence that the accountants failed to live up to their professional obligation and are entitled to consider the evidence in their decision, the professional standards committee says. That failure to question management occurs again and again during the Livent audit when auditors accepted the verbal assurances of the company's senior managers regarding invoices that were booked to the company's fixed assets with no supporting documentation to a whopping $27.5 million write-off of pre-production costs that Livent managers insisted upon after the accountants had completed their work. "All of these facts should have heightened the level of concern of the auditors with respect to the veracity of management representations," the professional committee states. It is interesting to note that while the Dundee Put Agreement is the mainstay of the ICAO's case against Deloitte, it is not mentioned once in the crown's criminal fraud charges against Drabinsky and Gottlieb. It appears, when it comes to Livent, there is enough alleged fraud to go around for everyone. It could be several months before the ICAO appeal committee delivers its decision. Who knows, by then there may be a decision in the Livent criminal trial as well. (Note: A previous blog post suggested that ICAO fines could only be collected from current members of the Institute. This is not the case. In fact, fines may be filed and collected through the Ontario court. The post has been corrected.)

thestar.com

Corrupt tax auditor gets three years

Wed Jan 29 2014
Section: News | Toronto Star
Byline: Marco Chown Oved(https://author.thestar.com/content/thestar/authors.oved_marco.html)
Illustrations: Jeffrey Granger has been sentenced to three years in prison after pleading guilty to accepting bribes.

He went from wearing Harry Rosen suits to panhandling on the streets. And after pleading guilty to accepting over a million dollars in bribes, former government tax official Jeffrey Granger is now going to prison.

At Newmarket court Wednesday, Granger, 39, was sentenced to three years for his involvement in a scheme to help wealthy developers evade taxes and frame Caledon's mayor for taking kickbacks.

Speaking slowly and articulately, the former Canada Revenue Agency((www.cra-arc.gc.ca)) team leader apologized for the harm he caused the mayor but said the plot also destroyed his life.

Since his arrest in 2010, Granger says he's lost his wife, his kids, his home, job and assets. His health has suffered - he's put on more than 70 pounds - and he's entered treatment for alcoholism and gambling addiction.

Granger pleaded guilty in November to breach of trust by a public officer, accepting bribes and fraud over $5,000.

At the plea hearing, the Crown and Granger submitted an agreed statement of facts that describes how several major developers in Peel Region paid Granger $1.1 million to stymie government tax audits of their businesses and attempt to frame Caledon Mayor Marolyn Morrison((m.thestar.com)) for taking bribes.

The developers deny these allegations and maintain Granger was hired as a legitimate tax consultant.

Morrison could not be reached for comment on Wednesday.

Morrison angered developer Benedetto (Benny) Marotta when Caledon town council blocked development on a tract of land he owned in 2008. He threatened to sue the city for $500 million.

Tensions grew worse in June of that year, when Morrison's husband was threatened and assaulted((www.thestar.com)) at their home by a man who demanded she change her vote on the development. No one was ever arrested or charged in the assault.

According to the agreed statement of facts, Marotta asked his accountant, Edward Favot, to investigate rumours that Morrison was corrupt and accepting bribes from developers.

Favot brought in Granger, who used his computer access at the CRA to initiate an audit into Morrison, the document says.

Marotta later gave police a USB stick containing digital copies of cheques other developers had made out to Morrison.

Because Morrison had not declared these cheques in her taxes, they appeared to show she had been taking bribes.

Police later determined the cheques were falsified.

Granger denies he provided this USB stick to Marotta.

Both before and after the forged documents were given to police, Marotta wrote Granger nine cheques for more than $500,000. Marotta's lawyer previously told the Star that those payments were for legal tax consulting services.

No one else has been charged in the case.

In an elevator during a court recess, Granger expressed frustration that he was the only person charged in the scheme.

"This is bigger than me," he said. "I'm the scapegoat."

Describing himself as a softie, in the same conversation with the Star, he said he spent all the money on his family, buying a Harley-Davidson for his father's retirement and living in a million-dollar house with his now ex-wife. He gambled much of the money away and donated large sums to charity, he said.

But Justice Joseph Kenkel said such large sums of money don't simply disappear and that his explanation of lavish expenditures wasn't credible.

After receiving his sentence, Granger stood up calmly. As the court officer handcuffed him, he quietly said, "Thank you."

Former accountant gets 7-year prison term for tax fraud

By Staff
Torstar News Service

There's only so much money to go around. Welfare recipients would be hurt by proposed changes to a federal grant program, opponents say. Torstar News Service

A 68-year-old, former chartered accountant, who lived lavishly in a Markham mansion by swindling Canadian taxpayers of almost $10 million in just five years, will soon be residing in much more modest surroundings.

A judge sentenced soft-spoken Roy Francis Smith to seven years and eight months in prison on Monday for a massive fraud in which he collected $9.8 million in refunds from the federal government after submitting phoney returns for the goods and services tax (GST) on behalf of a big energy company.

And before a police officer slipped a pair of handcuffs on the nattily attired Smith and led him away from a Newmarket court, Mr. Justice Simon Armstrong also slapped the fraudster with a $935,506 fine for dodging his own personal income taxes for several years. He must pay the penalty within a year.

Related:

- Does Toronto need a wax museum?
- Apartment still without heat after five weeks despite Landlord Tenant Board order
- Toronto's water birds hit hard by brutal winter weather

"It was a deliberate and flagrant fraud," Justice Armstrong told Smith, who showed little emotion. "It was a fraud of the public purse and, as such, affects everyone."

Sporting a white shirt and dark sweater at the sentencing, the thin, greying, bespectacled Smith had pleaded guilty to fraud earlier this month. Crown prosecutors dropped several other related charges against him. He would be eligible for parole after serving a third of his sentence.

The Canada Revenue Agency (CRA) had charged Smith in early 2010 but he claimed police had infringed on his rights in the seizure of evidence under the Charter of Rights and Freedoms. He lost the Charter challenge after two years of proceedings and then pleaded guilty just before the start of the trial.

The Crown dropped several related charges against Smith, who had three previous convictions for impersonation, forgery and fraud.

A statement of facts in the case showed Smith, who is married with adult children, used the refunds from his complex scheme to fund major renovations at his sprawling mansion in an exclusive enclave of multimillion-dollar estate homes in Markham's northwest end. His former house included pitched roofs, a stone exterior, a three-car garage, circular driveway and mature trees.

"He definitely lived high," said Crown prosecutor Ghazala Zaman.

Zaman, who sought an eight-year prison term, said outside court that Smith spent about $1.7 million in renovations and landscaping alone on the mansion.

The CRA placed a lien on the mansion to recover any equity and it continues to pursue other assets such as properties he bought in Florida. To date, the agency has seized about $700,000 in assets, according to Zaman.

"Hard-working Canadians who pay their taxes are entitled to have these cases pursued vigorously and to see a just outcome," she noted.

Smith eventually moved to a modest townhouse in another part of Markham after the CRA charged him.

The scheme unfolded in 2000 when Direct Energy Marketing hired Smith on a short contract to put its financial affairs in order, after Centrica of the United Kingdom bought the firm along with NGW Natural Gas Wholesalers. Smith's work involved looking at arrangements between the two Canadian firms and an audit of the NGW Natural transaction.

The statement of facts indicated Smith gained access to NGW's books and then posed as a company official to change the company's mailing address to one that he rented and controlled in Richmond Hill. Smith also asked for the addition of his name as an authorized contact for NGW Natural and also incorporated a similarly named company NGW Inc. to ease deposits of GST refunds at a bank.

In early 2001, he opened an account in the name of NGW Inc. at a credit union in Toronto and held signing authority as its first director. During the next five years unbeknownst to NGW Natural, he submitted 58 fictitious monthly GST returns to the agency and received 55 refund cheques.

"Smith collected nearly $190,000 per month consecutively for approximately five years," Zaman said.

connection to Smith, who hadn't worked with NGW for years. An investigation ensued which included getting account records from U.S. banks.

Mark Cullen, another federal prosecutor, said the Crown has sought longer jail sentences in the last year to reflect the scale of fraud and tax evasion, and the harm to victims.

Furthermore, he said the stiffer sentences will hopefully act as deterrent to others contemplating fraud.

THE GLOBE AND MAIL

REGULATION

OSC accuses Ernst & Young of shoddy audit of TSX Venture-listed Zungui Haixi

JANET McFARLAND
The Globe and Mail
Published Monday, Jun. 24 2013, 1:51 PM EDT
Last updated Monday, Jun. 24 2013, 6:22 PM EDT

Ernst & Young LLP is facing allegations from the Ontario Securities Commission that it failed to properly audit the books of a small Chinese athletic-shoe manufacturer.

The case unveiled Monday is the second from the OSC in the past six months in which Ernst & Young is accused of doing poor work auditing the books of a Chinese-based company. In December, the OSC alleged the firm was negligent as auditor of failed forestry giant Sino-Forest Corp., which collapsed in 2011.

More Related to this Story

- Ontario court approves $117-million settlement with Sino-Forest auditors
- OSC bans Chinese shoe maker, key executives for breaching securities laws
- LITIGATION Sino-Forest investors face off over deal with auditors

No allegations have been proven in either case.

The latest allegations involve shoe manufacturer Zungui Haixi Corp., which listed its shares on the TSX Venture Exchange in 2009, raising $39.8-million in its initial public offering.

Ernst & Young audited the firm's books in preparation for the IPO, but the OSC has alleged the audit was not in accordance with generally accepted auditing standards. The OSC also alleged Ernst & Young did not do appropriate work on Zungui's 2010 year-end audit.

The OSC alleged the auditors "failed to treat multiple red flags about the company's revenue and earnings with appropriate skepticism" and said Ernst & Young "failed to conduct a sufficient review of the audit evidence, leaving the review of key evidence in the hands of a staff member with limited experience."

The OSC also alleged Ernst & Young identified a risk that Zungui could use fictitious distributors to fraudulently inflate its revenue, but then disregarded evidence that suggested the company had

indeed "grossly exaggerated its sales to purported distributors."

Ernst & Young said in a statement that problems at Zungui were revealed as a result of its audit work, and it will "vigorously defend" itself against the OSC allegations.

"Issues concerning Zungui Haixi came to light as a result of actions we took during our 2011 audit," the firm said. "We brought these issues to the attention of the audit committee and management, and eventually resigned as auditor. We have co-operated with the OSC throughout its subsequent investigation.

"A statement of allegations, by its nature, is designed to present one side of events, and not the whole picture. The evidence will show that the OSC allegations do not fully describe all of Ernst &Young's audit work, which met all professional standards."

The OSC alleged the initial senior manager on the audit file informed the partner in charge of the file that she was not the right person to handle it because she did not speak Chinese and had no experience with audits of China-based companies. She was replaced with another senior manager who also did not speak Chinese and had no experience with Chinese company audits, the OSC alleged.

The manager on the IPO audit was a new employee who had recently joined the firm from a South African auditor, the OSC added. He had never audited a China-based firm and had never done an audit with Ernst & Young before.

"However, despite this limited experience, the manager was given significant responsibility for overseeing and reviewing key audit work," the OSC alleged.

Zungui announced in August, 2011, that Ernst & Young had suspended its audit of the firm, sending its share price plummeting. The company's independent directors and chief financial officer resigned days later.

In November, 2011, the OSC filed allegations against the company and its remaining directors, alleging multiple violations, including a failure to file financial statements. The company's shares were permanently cease-traded in 2012.

The case involving Ernst & Young's audit of Sino-Forest is still ongoing and hearing dates have not been scheduled. The firm has also denied the allegations.

Accountant sentenced for money laundering

Posted by Carla Parker on January 17, 2014 in Crime, DeKalb News No comments

An accountant with an office in south DeKalb was sentenced to six years in federal prison for his connection to a national drug trafficking and money laundering organization.

Matthew Ware, 57, of Tucker was convicted after a jury trial in January 2013 on one count of money laundering conspiracy. On Oct. 29, U.S. District Judge Richard W. Story sentenced him to six years in federal prison, followed by three years of supervised release.

Ware, owner of Padgett's Business Services in Lithonia, was the accountant of Jiles and Shannon Johnson, who owned KC Pit BBQ Restaurant in Sandy Springs. The Johnsons used their barbecue restaurant to cover up their illegal activity.

Ware was convicted of accepting bags of cash in excess of $10,000 from Jiles Johnson, according to the U.S. District Attorney's office. Ware provided the cash to some of his accounting firm's clients and they repaid him with checks made payable to Johnson and his businesses.

Ware and the Johnsons were among 14 people from metro Atlanta, Pennsylvania and California who were connected to the drug trafficking and money laundering organization and were sentenced to federal prison terms ranging from two to 15 years. All the defendants entered guilty pleas except for Ware.

"Businesses and professionals who use legitimate organizations to filter laundered drug proceeds denigrate legitimate earnings while destroying the jobs of those who work in those businesses," said U. S. Attorney Sally Quillian Yates. "Illegal drugs lure many into that lifestyle with offers of big money, easily made. In the end, what really happens is lives are destroyed, businesses close, and the dealers go to jail. We will continue working to remove harmful drugs from our streets."

In 2003, Jiles Johnson, who was also a commercial truck driver, began driving kilograms of cocaine from California to Philadelphia on behalf of Mark Walker to supplement his restaurant income, according to the U.S. District Attorney's office. Walker was a Philadelphia cocaine distributor with access to street-level dealers, including his brother and others. Johnson also supplied cocaine to Kansas City and Washington D. C., according to the U. S. Attorney's Office

As Johnson and Walker generated cash from cocaine sales, they purchased real estate in Georgia through Linda Tong, a local real estate broker. Tong made "structured" deposits of more than $500,000 into bank accounts. According to the U.S. District Attorney's office, "structuring" occurs when a person breaks down more than $10,000 in cash into smaller deposits under $10,000 to avoid the filing of a Currency Transaction Report (CTR) by a financial institution.

The Johnsons invested more than $3 million in real estate holdings, including an 80-acre motorcycle racetrack in Twiggs County, according to the U. S. District Attorney's office.

Ware accepted the bags of cash from Johnson and then provided the cash to some of his clients. When the cash volume increased, Ware connected Johnson to another client, financial planner Jacques Degaule, to assist with the laundering.

Degaule traveled to banks in Georgia, Missouri, Pennsylvania and New Jersey where he deposited more than $7 million. No Internal Revenue Service 8300 Forms were filed, which are required when a trade or business receives cash more than $10,000, according to the U. S. District Attorney's office.

The Johnsons used the funds to underwrite their investments and their restaurant's operations. Evan Francis, a local car broker, coordinated the delivery of loads of cocaine, solicited customers and structurally deposited cash, according to the U. S. District Attorney's office. Schawn Lemon Wortham laundered Walker's funds while he remained incarcerated.

The cocaine originated from Mexico and was supplied from California by Jose Gastelum and Lorenzo Vargas, according to the U. S. District Attorney's office. When Johnson experienced financial losses, Gastelum and Vargas collateralized his drug debt on behalf of the source of supply by taking ownership interests in his restaurant and racetrack. Ware assisted them in the process.

The organization broke down in 2010 when Johnson and two associates attempted to deliver 35 kilograms of cocaine to Philadelphia. The cocaine was intercepted by law enforcement, which ultimately led to the organization's dismantlement.

Harry S. Sommers, the Special Agent in Charge of the DEA Atlanta Field Division, said all of the defendants in the case were deserving of the sentences handed down.

"Several of these individuals masked themselves as legitimate businessmen, while everyone lined their pockets with excessive profits gained from drug trafficking," Sommers said. "These sentences should serve as a clear reminder to those business operators who facilitate fraud and money laundering schemes that while you think you may be flying under the radar, you are not. It's just a matter of time before you get caught and brought to justice. I express gratitude to the law enforcement partners who helped make this case a success."

Ware was an active community leader in south DeKalb. He was president of the 100 Black Men of DeKalb County, a mentoring organization for youth that he headed for two years. He was also the organization's treasurer.

According to his accountant firm's website, he was the vice chairman and chairman of the board of directors of the Georgia Lottery from 2000 to 2005. He is married to E. Noreen Banks-Ware, an attorney and special assistant administrative law judge and they have two children, according to the website.

The Scotsman

Accountancy giant EY's GBP750,000 Farepak fine

The Scotsman (Edinburgh, UK)
Fri Dec 20 2013
Page: 36
Byline: Martin Flanagan

Seven years after the failure of Christmas savings club Farepak Food and Gifts, its **auditor**, EY, has been **fined** GBP750,000 for sub- standard work.The Financial Reporting Council (FRC) also reprimanded EY - formerly known as Ernst & Young - and ordered it to pay GBP425,000 in costs, while individual **auditor** Alan Flitcroft, who carried out the work for EY, was **fined** GBP50,000 and reprimanded.Farepak went bust in 2006, owing GBP37 million to 120,000 customers who had put money into the club as a way of spreading the cost of Christmas over several months.The FRC said EY and Flitcroft admitted in a settlement with the watchdog on 12 December that their conduct fell below the standards reasonably to be expected."The result in this case underlines the FRC's commitment to promote public confidence and ensure the accountancy profession has proper regard for the technical and professional standards expected of members," Paul George, FRC executive director of conduct, said.The FRC said EY and Flitcroft "failed to properly consider Farepak's ability to continue as a going concern".EY said the settlement reached with the watchdog did not allege any "causative link" between EY and Flitcroft's conduct and Farepak's entry into administration and losses suffered by the savers. "However, EY regrets that aspects of our 2005 audit fell beneath our usual high standards," the accountancy firm added.Flitcroft, who could not be reached for comment, left EY in 2008 to become chief operating officer of Cardiff City Football Club, and later finance director for Ascot Racecourse, a position he stepped down from in October. EY is to pay Flitcroft's fine and costs.

Length: 266 words
Idnumber: 201312200002

Tone: Negative

KPMG pays €7 million to settle Dutch bribery case

Monday, January 13, 2014 at 3:58AM

Geert Vermeulen in Auditors, Ballast Nedam, KPMG, Netherlands, Transparency International, accountants

Accountants should provide reasonable assurance that the books and records of their clients accurately reflect the reality and that the internal accounting controls of their clients meet certain standards. There have been a number of cases in recent years where non-compliant behavior of issuers was egregious but accountants weren't charged.

That changed just before the end of the year in a remarkable case in The Netherlands. On December 30, KPMG reached a €7 million settlement with the Dutch authorities. The total settlement consists of a fine of €3.5 million and a forfeiture of €3.5 million.

KPMG allegedly helped their client, the Dutch construction company Ballast Nedam, disguise suspicious payments. Ballast Nedam itself settled with the Dutch authorities in 2012 for €17.5 million, including a €5 million fine and waiver of efforts to recover €12.5 million from tax authorities.

Ballast Nedam made a number of suspicious payments between 1996 and 2003 to foreign agents in order to obtain business in Saudi Arabia. According to the Dutch public prosecutor, KPMG knowingly failed to verify the payments to foreign agents between 2000 and 2003 and could not determine the ultimate beneficiary of the payments.

The Netherlands hasn't had an impressive anti-bribery enforcement record. In a report issued a couple of months ago, Transparency International put the country in the 'limited or no enforcement' category. Recent developments seem to indicate that the Dutch authorities are determined to change this.

This investigation started once the Dutch tax authorities approached Ballast Nedam in 2009, at least 6 years after the last suspicious payments were made. Ballast Nedam started an internal investigation and provided the results to the Dutch authorities in January 2011. Almost 2 years later, Ballast Nedam settled with the Dutch authorities and it took another year for the authorities to settle with KPMG.

KPMG said they "are shocked by the facts that have emerged from this case and find these totally unacceptable." They said 2 of the 3 accountants involved have retired and the employment of the third accountant has been ended. Disciplinary measures have been taken and KPMG has agreed to implement additional compliance measures. The firm is also still investigating services delivered to other clients by the three (former) accountants and to clients in similar industries.

The public prosecutor is also still investigating the three former accountants, as well as some of the former managers of Ballast Nedam.

Geert Vermeulen is a compliance professional. He is a frequent speaker at international compliance conferences and teaches at the Dutch Compliance Institute. He is also a Board member of the Dutch Compliance Officers Association. Recently he wrote a chapter on third party due diligence in the first Dutch book on anti-corruption (Ondernemen zonder corruptie). This article reflects the personal views of the author.

REUTERS

Print This Article | Close this window

Deloitte to pay $2 million to settle charges over audit rule violations

Tue Oct 22, 2013 7:31pm EDT

By Sarah N. Lynch

WASHINGTON (Reuters) - Deloitte & Touche DLTE.UL will pay a $2 million penalty to settle civil charges that it violated federal audit rules, in one of the largest civil penalties ever imposed by the U.S. audit watchdog.

The Public Company Accounting Oversight Board, which is tasked with policing auditors, said on Tuesday that it was censuring Deloitte for allowing its former partner to continue participating in the firm's public company audit practice, even though he had been suspended over other rule violations.

The former partner, Christopher Anderson, settled with the PCAOB in 2008 by agreeing to a $25,000 fine and one-year suspension after the watchdog said he violated rules during a 2003 audit of the financial statements for a unit of Navistar International Corp (NAV.N).

A spokesman for Deloitte said the company is pleased the matter has been resolved. "Deloitte takes very seriously all orders and actions of the PCAOB," the spokesman said.

The penalty matched a record PCAOB fine last year against Ernst & Young.

The PCAOB was created by the 2002 Sarbanes-Oxley Act in response to the accounting scandals at companies like Enron and Worldcom. It sets audit standards, conducts routine inspections and disciplines rule breakers in the audit industry.

The oversight board said on Tuesday it first launched disciplinary proceedings against Deloitte in March, but because of secrecy provisions in the Sarbanes-Oxley law, the board was not able to make them public until now.

"When the board suspends an auditor, it does so to protect investors," said James Doty, the head of the PCAOB.

"Deloitte permitted the former partner to conduct work precluded by the Board's order and put investors at risk."

According to the board, Anderson previously worked as a partner in Deloitte's Chicago office.

The PCAOB said that Anderson gave Navistar and Navistar Financial Corp a clean audit opinion on its 2003 financial statements, even though $19.7 million in errors, that led to an overstatement of the company's assets and earnings, had been uncovered.

After he settled the case and agreed to a one-year suspension, the PCAOB said Deloitte placed Anderson into another position that still allowed him to be involved in the preparation of audit opinions.

Allowing a suspended auditor to continue working in that capacity is a violation of PCAOB rules, unless the Securities and Exchange Commission gives the firm permission.

Jonathan Gandal, the spokesman for Deloitte, said that while the audit firm took "several significant actions" at the time of Anderson's suspension to restrict his activities, "more could have been done" to monitor compliance.

"The robust policies and monitoring procedures we have since instituted fully address the issue and will prevent a similar matter from arising in the future," he added.

(Reporting by Sarah N. Lynch; Editing by Tim Dobbyn)

live mint

Print Close

Wed, Jun 19 2013. 09 33 AM IST

Deloitte fined $10 mn in US money laundering case

New York state imposes fine on Deloitte for its actions in advising Standard Chartered Bank over money laundering

The New York Department of Financial Services said the fine, which the company agreed to in a settlement, was to cover its "misconduct, violations of law, and lack of autonomy" in advising Standard Chartered. Photo: Brent Lewin/Bloomberg

New York: Big accountancy Deloitte was fined $10 million by New York state on Tuesday for its actions in advising Standard Chartered Bank over money laundering.

Deloitte's unit Deloitte Financial Advisory Services Llp was fined and also banned for one year from work in New York state after state authorities said it did not carry out its duties independently in advising the bank on how to avoid money laundering.

Standard Chartered was fined $667 million by federal and New York state authorities last year for permitting hundreds of billions of dollars to be laundered through its US branch by clients from Iran, Myanmar, Libya and Sudan, in violation of US sanctions on the countries.

The transfers took place mainly between 2001 and 2007.

In 2004, the New York Department of Financial Services required the London-based bank to contract an independent adviser to help it comply with money-laundering statutes.

But even after Deloitte Financial Advisory Services took that role, the laundering continued.

The department said the fine, which the company agreed to in a settlement, was to cover its "misconduct, violations of law, and lack of autonomy" in advising Standard Chartered.

"At times, the consulting industry has been infected by an 'I'll scratch your back if you scratch mine' culture and a stunning lack of independence," said Benjamin Lawsky, New York superintendent of financial services, in a statement.

"Today, we are taking an important step in helping ensure that consultants are independent voices—rather than beholden to the large institutions that pay their fees."

In a statement Deloitte emphasized that its advisory unit was not accused of participating in the laundering.

"We are pleased that, as the agreement states, a thorough investigation by DFS found no evidence that Deloitte FAS knew of, or aided, abetted or concealed any alleged violation of law" by Standard Chartered.

"Deloitte FAS looks forward to working constructively with DFS to establish best practices and procedures that are ultimately intended to become the industry standard."

Big Four Chinese unit face US suspension

23 Jan 2014

The Chinese arms of all Big Four accounting firms face a six-month ban on practicing in the US in the latest development in a long-running row over giving regulators greater access to audit documents for work conducted by Chinese accounting firms for Chinese companies that list in the US markets.

In a new ruling, Securities and Exchange Commission (SEC) Judge Cameron Elliot has censured the Chinese affiliates of KPMG, Deloitte & Touche , PwC and EY, saying they had 'willfully' failed to give US regulators the audit work papers of certain Chinese companies under investigation for accounting fraud. A fifth firm, Dahua, was also censured by the judge but not suspended.

The auditors have cited concerns about violating Chinese secrecy laws as the reason for failing to hand over the audit details. Last year, the US announced that an agreement had been reached whereby Chinese regulators would hand over some audit documents of US-listed Chinese companies to the SEC. However, the papers filed in the latest case suggest that not all the papers requested were produced, according to *Reuters*.

The Big Four firms have indicated that they intended to appeal against the ruling, issuing a joint statement saying: 'In the meantime the firms can and will continue to serve all their clients without interruption.'

Paul Gillis, an accounting professor at Peking University, said: 'This decision will be a huge shock in Beijing. The SEC has pushed a lot of chips out on the table.'

Gillis claimed that if the ban goes ahead, mid-tier firms might find it hard to take over auditing of the Chinese companies previously handled by the Big Four because of the workload and capacity required.

Pat Sweet
Online reporter

View profile and articles. (/pat-sweet)

Related Article

SEC fines KPMG 5m for independence violations (/sec-fines-kpmg-5m-independence-violations)
KPMG has agreed to pay $8.2m (£5m) to settle charges by the US Securities and Exchange Commission (SEC) that the firm violated the rules around auditor independence in its work for three US clients

27 Jan 2014

The SEC had sought to have a permanent bar imposed on the Big Four's Chinese affiliates, but the judge in the case said a six-month bar was in the public interest, and that he had 'little sympathy' for the firms.

Matthew Solomon, chief litigation counsel in the SEC's enforcement division, said: 'These records are critical to our ability to investigate potential securities law violations and protect investors.'

The ruling will not take effect immediately, and the issue is now likely to be addressed through diplomatic channels.

KPMG to pay USD 8.2 mn to settle SEC auditing charges

Washington, Jan 24, 2014, (AFP)

US accounting firm KPMG violated rules aimed at maintaining auditors' independence from their clients and will pay USD 8.2 million to settle the charges, regulators said today.

The Securities and Exchange Commission found that KPMG broke the rules by providing prohibited non-audit services such as bookkeeping, corporate finance and expert services to affiliates of companies whose books they were auditing.

In addition, the SEC said in a statement, some KPMG personnel also owned stock in companies or affiliates of companies that were KPMG audit clients, in a further violation of the rules designed to ensure auditors maintain objectivity and impartiality in reviewing a client's books.

"KPMG compromised its role as an independent audit firm by providing prohibited non-audit services to companies that it was supposed to be auditing without any potential conflicts," John Dugan, associate director for enforcement in the SEC's Boston regional office, said in the statement.

"Auditors are vital to the integrity of financial reporting, and the mere appearance that they may be conflicted in exercising independent judgment can undermine public confidence in our markets."

According to the SEC, KPMG repeatedly represented in audit reports through the 2007-2011 period that it was "independent", despite providing services to three audit clients "that impaired KPMG's independence."

KPMG did not admit to or deny the SEC findings.

But it agreed to pay USD 5.3 million in disgorgement of fees received from the three clients plus interest of USD 1.2 million, and a USD 1.8 million penalty, the SEC said.

The SEC did not identify the clients.

The regulator also said the company pledged internal changes to enhance compliance with auditor independence rules and to hire an independent consultant to monitor the changes.

KPMG, in an emailed statement to AFP, said it was "fully committed" to ensuring its independence as an auditor.

"In the years since the events discussed in this SEC action, KPMG has

implemented internal changes that are designed to ensure its ability to comply with restrictions on providing non-audit services to SEC audit clients and/or their affiliates," the company said.

Bloomberg

PwC Fined $2.17 Million by U.K. Regulator Over JPMorgan Client-Money Audit

By Ben Moshinsky - Jan 5, 2012

PricewaterhouseCoopers LLP was fined a record 1.4 million pounds ($2.17 million) for failures concerning reports on client-money accounts at JPMorgan Chase & Co. (JPM)'s London securities unit.

PwC's "acts of misconduct merit a severe reprimand," the Accountancy & Actuarial Discipline Board said in a judgment released today. PwC failed to notice that J.P. Morgan Securities Ltd. hadn't properly segregated an average of $8.6 billion of client funds from the firm's accounts in reports to the U.K.'s Financial Services Authority for the seven years through 2008.

JPMorgan discovered the error in 2009 and reported it to PwC and the FSA, which fined the bank a record 33.3 million pounds in 2010. The U.K. financial regulator has focused on client-money segregation after the winding up of Lehman Brothers Holdings Inc.'s former European unit was slowed by years of litigation among creditors fighting over the issue.

"We regret that one aspect of our work on the private client money report to the FSA fell beneath our usual high standards," PwC said in an e-mailed statement. "When the issue was identified, and before any complaint had arisen, we took action to ensure that staff received additional training in the client monies area."

The AADB, the U.K.'s audit regulator, sought a record fine against PwC to top the 1.2 million-pound sanction against Coopers & Lybrand LLP in 1999. The tribunal also ordered that PwC pay costs to the AADB totaling 83,902 pounds.

Due Skill, Care

"PwC accepted that it did not carry out its professional work in relation to these reports with due skill, care and diligence," the AADB said in an e-mailed statement. The firm earned a reduction in the fine, which would have been 2 million, for cooperating.

The AADB is probing PwC in a similar investigation into whether the firm's reports on client assets at Barclays Capital Securities Ltd. broke financial rules.

The FSA fined the U.K. bank 1.12 million pounds in January 2011 for failing to put as much as 752 million pounds a day of client money into protected accounts that were separate from its own money-market deposits.

PwC compiled reports to the regulator between 2001 and 2009 outlining Barclays Capital's compliance with client-asset separation rules.

To contact the reporter on this story: Ben Moshinsky in London at bmoshinsky@bloomberg.net

To contact the editor responsible for this story: Anthony Aarons at aaarons@bloomberg.net.

the guardian

Guardian Financial Pages

Accountants fined pounds 14m over MG Rover: Watchdog says Deloitte in serious ethical breaches: Record-breaking penalty for Phoenix Four advisers

Jennifer Rankin

652 words
10 September 2013
The Guardian
GRDN
27
English

Deloitte, one of the UK's largest accountancy firms, has been fined a record-breaking pounds 14m for a conflict of interest that occurred when it advised **MG Rover** Group and the Phoenix Four directors who bought the British carmaker before it collapsed.

It is the largest fine issued by the Financial Reporting Council (FRC), the body that regulates accountants, which has also given **Deloitte** a severe reprimand.

Maghsoud Einollahi, a former director of the accountancy firm, was fined pounds 250,000 and given a three-year ban from the profession.

In a stinging reprimand to **Deloitte**, the FRC said the sanctions were needed because of the seriousness of the ethical breaches and the substantial benefit that had arisen through the misconduct.

The pounds 14m penalty dwarfs a pounds 1.4m fine given to PricewaterhouseCoopers in November 2011 after it wrongly said JPMorgan Chase bank was keeping customer money separately from its own.

Yesterday the FRC said its report sent "a strong and clear message" that all accountants had a responsibility to act in the public interest and comply with their code of ethics.

"The sanctions imposed are in line with the FRC's aim to ensure penalties are proportionate and have the deterrent effect to prevent misconduct and bolster public and market confidence," said Paul George, executive director of the FRC. The outcome is one of the final twists in the tale of **MG Rover**, which was bought in 2000 for pounds 10 by four local businessmen, John Towers, Nick Stephenson, John Edwards and Peter Beale. The Phoenix Four went on to pay themselves and the managing director, Kevin Howe, pounds 42m before the firm collapsed in 2005 with debts of pounds 1.4bn and the loss of more than 6,000 jobs. **Deloitte** had faced a pounds 20m fine after the FRC tribunal concluded in July that it had failed to meet ethical and public interest standards when it advised the Phoenix Four and **MG Rover**.

Among 13 charges found against the company, **Deloitte** had failed to consider a conflict of interest in which the firm benefited from schemes devised by the Phoenix Four.

Deloitte, which has 28 days to appeal against the fine, argues that the tribunal decision could restrict the choice and quality of advice that accountants can offer firms. It said: "We remain disappointed with the outcome of the tribunal and disagree with its main conclusions. As a firm, we take our public interest obligations seriously in everything we do. We are disappointed that the efforts we and others made did not successfully secure the long-term future of the **MG Rover** Group."

Richard Burden, the Labour MP for Birmingham Northfield, said that some of the proceeds of the pounds 14m fine should go to the former employees of MG Rover. The firm's former employees were awarded compensation of just pounds 3 each in 2012 after a seven-year battle for redundancy payments.

"The unprecedented scale of this fine raises the question of compensation for the workers, who did everything that was asked of them by the Phoenix Four," said Burden. "There are thousands of people affected and many issues that need addressing, so the money wouldn't be enough to change lives. But it would help the community draw a line under the MG Rover saga and move into the future.

"The pounds 14m must not only deter accountants from acting in this way again, it must mean change for the people and the community who suffered so much from the collapse of MGR and are still to be repaid."

The fine is earmarked for the Consultative Committee of Accountancy Bodies, an industry umbrella group. No one from the CCAB was immediately available to respond to Burden's proposal.

Guardian Newspapers Limited

Document GRDN000020130910e99a00003

The Telegraph

Deloitte under investigation over Rover; Nearly seven years after the collapse of car manufacturer MG Rover, its adviser Deloitte has been placed under investigation by industry regulators.

By Anna White

399 words
2 February 2012
06:34
The Telegraph Online
TELUK
English

A complaint was logged yesterday by the Financial Reporting Council (FRC) over the conduct of the second largest accountancy firm in the UK and its former mergers and acquisitions partner Maghsoud Einollahi.

Tom Martin, FRC executive counsel referred the case to the Accountancy and Actuarial Discipline Board (AADB) to review **Deloitte**'s conduct as auditors and advisers to various companies in the **MG Rover** Group sale.

The complaint alleges that in connection with certain transactions, **Deloitte** and Mr Einollahi "failed adequately to consider the public interest; the potential for there to be different commercial interests between the Phoenix Four, **MG Rover** Group and associated companies and shareholders; and the conflicts of interest and self-interest threat in relation to advising the Phoenix Four whilst maintaining client relationships with the **MG Rover** Group."

The accountancy arbitrators said the investigation is extremely serious, as demonstrated by the amount of time it took to file the complaint against **Deloitte** (formerly **Deloitte** & Touche.)

Both the AADB and **Deloitte** confirmed the inquiry is into the "transactions" overseen by **Deloitte** not the audit work.

Since the car company collapsed in 2005 along with 6,500 UK jobs the AADB has been scrutinising **Deloitte**'s role as auditor and adviser to Rover and its parent company Phoenix Venture Holdings, run by John Towers, Peter Beale, Nick Stephenson and John Edwards - otherwise known as the Phoenix Four.

A 2011 report commissioned by Lord Mandelson and completed by the National Audit Office revealed how the four directors and former **MG Rover** chief executive Kevin Howe paid themselves a total of £42m during their five-year ownership of the company, which they bought for a token £10 and left with more than £1bn of debt.

In 2011 the Government banned the Phoenix Four from serving as company directors.

A spokesman for **Deloitte** said: "We are disappointed that the AADB has taken the view that limited aspects of our advisory work relating to two transactions in 2001-2 falls short of acceptable standards.

"We do not agree with the AADB and are confident...the tribunal will conclude that there is no justification for criticism."

Deloitte made £31m in fees from MG Rover in the five years before it collapsed.

MG Rover debacle can't hide accounting regulation failures

Prem Sikka, Professor of Accounting, Essex Business School at University of Essex

786 words
10 September 2013
The Conversation
CONVAU
English

https://c479107.ssl.cf2.rackcdn.com/files/31113/width668/v67rvnv9-1378833352.jpg
[https://c479107.ssl.cf2.rackcdn.com/files/31113/width668/v67rvnv9-1378833352.jpg]

The UK accountancy watchdog has barked. The Financial Reporting Council (FRC) has fined **Deloitte** & Touche £14 million [http://www.frc.org.uk/News-and-Events/FRC-Press/Press/2013/September/FRC-publishes-Final-Report-of-Disciplinary-Hearing.aspx] for failures relating to the demise of **MG Rover**. The report [http://www.frc.org.uk/Our-Work/Publications/Professional-Discipline/Tribunal-Report-Deloitte-Touche-and-Mr-Maghsoud-Ei.pdf] says **Deloitte** was engaged in huge conflicts of interest as the firm acted both as auditor and advisor to the company and its directors.

The **MG Rover** debacle began in 2000 when four businessmen (subsequently known as the Phoenix Four) bought the ailing carmaker from BMW for just £10. The purchase was accompanied by a loan of £423 million from BMW and the UK government also provided additional funds. **Deloitte** acted as auditor of **MG Rover** and an adviser to the Phoenix Four. The company continued to receive a clean bill of health from auditors. Between 2000 and 2005, the Phoenix Four collected around £42 million in remuneration. With advice from **Deloitte** some £7.7 million ended up in an offshore trust [http://www.thesundaytimes.co.uk/sto/business/Companies/article1091072.ece] in Guernsey. In 2005, the company collapsed with debts of nearly £1.4 billion. Some 6,000 workers lost their jobs.

Following a public outcry, the Department of Business Innovation and Skills appointed inspectors, one of whom was an accountant, to investigate the debacle. The two volume report (here [http://www.berr.gov.uk/files/file52782.pdf] and here [http://www.berr.gov.uk/files/file52783.pdf]) cost £16 million and was published in 2009. The report noted that between 2000 and 2005, **Deloitte** received £30.7m in fees, of which £28.8m related to consultancy, that is, only £1.9 related to audits.

Deloitte was advising the company and its directors and then audited the resulting transactions. Hence the concerns about possible conflicts of interest and the disciplinary tribunal's conclusion that **Deloitte** "failed to be sufficiently objective in its work for **MG Rover** ". **Deloitte** is found guilty of "misconduct" and the FRC report [http://www.frc.org.uk/Our-Work/Publications/Professional-Discipline/Tribunal-Report-Deloitte-Touche-and-Mr-Maghsoud-Ei.pdf] states: "the acts which amount to misconduct were quite deliberate" and the firm and its lead partner "placed their own interest ahead of that of the public and compromised their own objectivity. This was a flagrant disregard of the professional standards."

The FRC's reputation as an accounting watchdog was severely battered by the banking crash. All distressed banks received a clean bill of health [http://www.essex.ac.uk/ebs/research/working_papers/wp_09-04.pdf] from their auditors even though depositors were queuing outside banks to withdraw their cash and governments were bailing out banks. The FRC failed to investigate any of the auditing firms. The **MG Rover** debacle has given it an opportunity to reinvent itself. The £14 million fine on **Deloitte** is the highest ever against any accounting firms. But all is not what it seems.

For any regulatory system to be effective regulators need to act swiftly. That has not been the case for the FRC. It initially announced [http://www.frc.org.uk/FRC-Documents/FRC/FRC-Progress-Report-MG-Rover-Group-Companies-Act-I.aspx] its intention to investigate the conduct of **Deloitte** as auditor and adviser to the

MG Rover Group in August 2005. The wheels of the profession grind slowly and then it claimed that will proceed after the inspectors' reports if finalised, which was published in 2009. It has taken the FRC another four years to do anything. This is hardly a model of swift action.

The £14m fine may be the largest ever, but needs to be seen in perspective. It is less than half of the £30.7m fees collected by **Deloitte**. So despite failures and "misconduct", the firm has still made considerable profit. The firm's UK revenues [http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/About%20Deloitte/uk-deloitte-annual-results-2013.pdf] are around £2.5 billion; that's £6.85m a day. The fine amounts of the loss of about two days' revenue. This is unlikely to make accountancy firm partners quake in their boots.

The fine will fill the coffers of the FRC and will not be used to compensate creditors, employees, or taxpayers who provided social security and other benefits for the redundant workers.

The **MG Rover** episode does not herald a new dawn in the regulation of auditors. Despite the toxic effects of conflicts of interest and calls from parliamentary committees, the FRC has resisted [http://www.ft.com/cms/s/0/a16fbee8-967a-11df-9caa-00144feab49a.html#axzz2eTUdpIVR] a total ban on auditors acting as consultants for companies. So companies will continue to audit the transactions they themselves have overseen. Some of the darker practices could be flushed out and given public visibility by compulsory tendering of audits [http://www.frc.org.uk/News-and-Events/FRC-Press/Press/2013/August/FRC-responds-to-Competition-Commission-s-Provision.aspx], but the FRC opposes that too.

For the time being, the **MG Rover** episode may legitimise the FRC's regulatory credentials but the fault lines are as big as ever and will not go away.

Prem Sikka does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

The Conversation Media Group Limited

Document CONVAU0020130911e99a0000l

The New York Times

HIGH & LOW FINANCE
Business/Financial Desk; SECTB

When Accountants Play Role Of Bankers

By FLOYD NORRIS

1524 words
13 September 2013
The New York Times
NYTF
Late Edition - Final
1
English

Here's a novel concept: Accountants have an obligation to always work in the public interest.

That is the law in Britain, a regulatory tribunal declared this week. The tribunal ruled that **Deloitte** L.L.P. had failed in its professional responsibilities in its work for **MG Rover**, the failed automaker, and for the "Phoenix Four," four businessmen who took over the automaker in 2000 and ran it into the ground, taking out millions of pounds for themselves in highly dubious transactions before the company failed.

The tribunal issued a "severe reprimand" to **Deloitte** and levied a fine of £14 million ($22 million) against the accounting firm, a record in Britain. It fined Maghsoud Einollahi, a retired **Deloitte** partner, £250,000 and barred him from the profession for three years.

"They placed their own interests ahead of that of the public and compromised their own objectivity," said the tribunal, convened by the Financial Reporting Council. "This was a flagrant disregard of the professional standards expected and required."

Deloitte was the auditor for **MG Rover**, but the audits have not been challenged. Instead, it was the corporate finance work, run by Mr. Einollahi, that drew the condemnation.

The ethics rules of the Institute of Chartered Accountants in England and Wales -- a group that all accountants and accounting firms must belong to -- require accountants to consider the "public interest." This ruling appears to be the first that makes clear just how far that can go.

"It has been put to us that in corporate finance work and tax work the only duty that a member owes is to his client, provided that he acts with integrity, and that the public interest is not a matter that needs to concern him," the tribunal wrote. "We do not accept this."

British auditing firms have gained some success in competing with investment banks in providing advice on mergers and corporate restructurings and have been able to charge high fees that are contingent on the success of a transaction. The ruling did not say such fees were barred, but it did say that accounting firms must carefully guard against conflicts of interest.

It conceded that the requirement to take the public interest into account could make it harder for accountants to win such business, but said that did not matter. "It is this duty to consider the public interest that provides comfort to the client that matters are being dealt with properly and with integrity."

Deloitte argued that the public interest was not involved because **MG Rover** was a private company. The board rejected that, noting that **Deloitte** itself bragged about its role in preserving jobs when the Phoenix

group took over MG Rover from BMW, the German carmaker, and that Mr. Einollahi cited the public interest in preserving jobs when he wrote to British tax authorities seeking favorable tax rulings.

In 2000, BMW concluded that it had made a mistake in acquiring MG Rover and set out to find a buyer. After one deal fell through, it settled on a company called Phoenix Venture Holdings, which bought the company for £10.

Even that nominal price drastically overstated what was paid. BMW chipped in what was called a dowry -- a £427 million interest-free loan for up to 49 years.

That loan became the source of some of the money the businessmen took out of MG Rover before it failed in 2005. Rather than have the loan go to the car company, the Phoenix Four directed it to their parent company, which then lent the money to the car company, charging interest. They then distributed the "profits" that they realized from the interest to themselves.

Another strange deal involved the men's being owed £10 million by the company even though they had invested only £60,000 each.

They wanted the figure to be £75 million, but that arrangement could not be completed. According to a later government report on the fiasco, Peter Beale, one of the Phoenix Four, blamed Sue Lewis, a partner in Eversheds, a prominent law firm that was advising the company, for keeping them from realizing the full amount.

Ms. Lewis testified that Mr. Beale had told her "it wasn't her position to be raising questions about the directors' remuneration and that she had done it on a number of occasions in a way that he had thought was inappropriate."

The law firm, Mr. Beale said, was not "anybody's moral guardians."

"Mr. Beale," said the report, compiled by inspectors appointed by the government, "considered that Mr. Einollahi of **Deloitte** was less prone to raising objections." It added that **Deloitte** "played a very prominent part" in some of the transactions the inspectors deemed inappropriate.

In the end, Mr. Beale, his three colleagues -- John Edwards, Nick Stephenson and John Towers -- and Kevin Howe, MG Rover's chief executive, took out £42 million from the company. That doesn't count the £1.6 million in consulting fees paid to a woman who the report said did little but had a "personal relationship" with Mr. Stephenson.

The British Serious Fraud Office declined to bring charges against the Phoenix Four, who have kept the money. They were, however, barred from serving as corporate directors in Britain. Mr. Beale, who downloaded and ran on his computer a program called "Evidence Eliminator" just before government inspectors arrived, denied he had tried to obstruct the investigation.

The tribunal this week said that **Deloitte** had failed to take needed steps to avoid conflicts of interest and to make clear to independent directors of **MG Rover** that it was working for the Phoenix group, not for the company, in its consulting work. To the contrary, the tribunal said, **Deloitte** made a presentation to the MG Rover board "suggesting they were acting for MG Rover and not the Phoenix Four." **Deloitte** said it did make clear to the MG Rover board that it needed to obtain independent advice.

Deloitte was aware of potential conflicts in at least one regard. The government report concluded that in helping to arrange one transaction, it avoided dealing with one interested bank because it was a **Deloitte** client and involving it might keep **Deloitte** from being able to collect a £7.5 million contingency fee.

One transaction that outraged investigators later was a deal that transferred the benefit of MG Rover tax losses to another company owned by the Phoenix partners without MG Rover receiving any compensation. Mr. Einollahi told the Financial Reporting Council that he was aware of that fact but not very interested in it. "It was of no concern to me ultimately where the benefit sat, in which company," he said. "What was of concern to me here is my client is asking me to help turn some losses into value."

The tribunal concluded that the transaction was not in the interest of MG Rover and that "in those circumstances, the respondents should have considered the public interest in relation to the transaction."

MG Rover was able to stay in business for a few years thanks to the BMW loan and the sale of its Land Rover business to Ford. But efforts to find a Chinese joint venture partner were unsuccessful and the company failed in 2005, leaving behind £1.3 billion in debt.

A **Deloitte** spokeswoman said the firm was "disappointed with the outcome of the tribunal" and disagreed "with its main conclusions." The firm added that the decision "could have negative implications for the advice that can be provided" by British accountants. "Over the coming weeks," it concluded, "we will continue our discussions with relevant stakeholders and professional bodies about the potentially wide-ranging impact on the profession and wider business community of the tribunal findings."

The tribunal denied it was doing anything new. "It seems to be being suggested that we have been attempting to set new standards and principles," the tribunal wrote in its decision. "This is not the case. We have found breaches in the regulations which have been in existence for a lengthy period of time."

Accountants in many countries have suffered from what might be called "banker envy," in which they contrast their remuneration with that of bankers also involved in putting together deals. In Britain, they have won the right to do transaction advice and to be compensated based on the size of the deal, as bankers are. That is not allowed in the United States.

The Financial Reporting Council says **Deloitte** received £1.9 million for audits and £1.8 million for tax work from MG Rover from 2000 to 2005. It collected £26.7 million in corporate finance advisory fees from the Phoenix entities that controlled MG Rover.

In helping the Phoenix Four, **Deloitte** may have jeopardized that source of profits, not only for itself but for other large accounting firms.

Floyd Norris comments on finance and the economy at nytimes.com/economix.com

Employees of MG Rover. A tribunal ruled that Deloitte had failed in its responsibilities in its work for Rover. (PHOTOGRAPH BY DAVE CAULKIN/ASSOCIATED PRESS) (B7)

The New York Times Company

Document NYTF000020130913e99d00099

CRAIN'S CHICAGO BUSINESS

THE BIG FOUR'S NEW MATH; A decade after Sarbanes-Oxley forced them to scale back consulting work, accounting giants are beefing up the business of dishing out advice

STEVEN R. STRAHLER; sstrahler@crain.com

1236 words
7 October 2013
Crain's Chicago Business
CCHI
19
Volume 36; Number 40
English

For accounting's Big Four, it's a generally accepted principle of deja vu all over again.

A decade after the Sarbanes-Oxley Act restricted the advisory work they can do for audit clients, the Big Four are rebuilding lucrative and conflict-prone advisory practices—to the dismay of critics who fault the firms for missing signs of the financial crisis.

Advisory revenue (excluding tax) at **Deloitte** LLP, Ernst & Young LLP, PricewaterhouseCoopers LLP and KPMG LLP last year surged to $36 billion for their global networks, a rate four times the 3.4 percent gain in audit fees, according to Monadnock Research LLC in Gloucester, Mass. KPMG's audit revenue, the smallest of the Big Four, actually fell.

With pedals to the metal, the firms are squeezing smaller advisory firms—snapping them up when they falter—as well as big law's lobbying, tax advisory and compliance-monitoring efforts (see Page 22).

Against this backdrop, the Big Four since mid-2012 have installed new city or regional chiefs in Chicago. To succeed in their new roles, they need to get a grip on the trend and its risks. **Deloitte**, the biggest of the Big Four, with the largest advisory business, last summer named an advisory-side person to head an expanded Chicago-based central region, covering 17 states.

Providing more than 10,000 local jobs, many high-paying professional positions, the Big Four are among Chicago's top private-sector employers and emblematic of the city's long-term economic shift from manufacturing to service-sector employment and its accumulation of intellectual capital. Big Four employment in Chicago grew 5.5 percent, to 10,454, in the 12 months ended June 30, with nearly twice as many in advisory services (4,760) as in audit (2,427).

The firms command about 17 percent of global consulting revenue, and their share will double to 35 percent by 2020 if competitors match Ernst & Young's ambitious goals, Monadnock CEO Mark O'Connor says.

That outcome, requiring sustained double-digit annual growth, might be a stretch. But merely positing it rekindles thoughts of auditors going easy on clients to win advisory assignments—a worry shadowing Sarbox's enactment in 2002 after Enron Corp. imploded and took auditor Andersen with it. More recently, the Big Four audited a string of financial industry failures: Bear Stearns Cos. (**Deloitte**), Lehman Bros. Holdings Inc. (Ernst & Young), Countrywide Financial Corp. (KPMG) and MF Global Inc. (PwC).

At **Deloitte**, the first of the Big Four to report fiscal 2013 revenue, consulting and financial advisory revenue now exceeds audit's, which grew less than 1 percent during the period, while the firm made some 30

acquisitions. Three years ago, the consulting and financial advisory segments combined were four-fifths of audit revenue.

"There are companies that are pushing the envelope and waiting to be caught," says Francine McKenna, a Chicago-based CPA and PwC and KPMG Consulting Inc. alumna who writes industry blog "Re: the Auditors."

Last month, **Deloitte**'s U.K. parent was fined an equivalent of $22 million by a British tribunal reviewing audit and tax work for **MG Rover** Group and **Deloitte**'s simultaneous, and much more remunerative, consulting services for the failed automaker's owners. A "disappointed" **Deloitte** said it disagreed with the tribunal's "main conclusions."

PwC, meanwhile, declines to comment on a subpoena it received in an ongoing New York investigation into chummy relationships between consultants and Wall Street clients.

After a recent decline in class-action lawsuits against accounting firms (and their insurers), Cornerstone Research in New York predicts a possible rebound as a result of whistle-blower suits and the Jobs Act exemption for emerging-growth companies to disclose auditor reports on internal controls. Accounting-related filings represented 30 percent of class actions in 2012, but they involved 91 percent of $2.9 billion paid out in settlements.

DEMAND DRIVERS

For a few years, Sarbox was a boon to the Big Four, which feasted on the compliance work it produced. Once that waned and noncompete agreements involving sold-off consulting practices expired, the Big Four ramped back up, benefiting in a slowly recovering economy by deferred spending on information technology, cyber security upgrades and "cost-optimization" initiatives. A reviving IPO market also is driving demand, as is helping clients understand implications of social media and "customer experience" concepts.

Non-audit fees paid to auditors by 95 Illinois public companies tracked by Audit Analytics of Sutton, Mass., nearly doubled, to almost $120 million, in 2012 from $67 million in 2009, while audit fees rose only modestly, to $398 million from $382 million. Though spinoffs involving Abbott Laboratories (Abbvie), Kraft Foods Inc. (Mondelez International Inc.) and Sara Lee Corp. (Hillshire Brands Co.) goosed non-audit revenue, advisory's momentum is unmistakable.

The Big Four can leverage familiar brand names, distribution channels and pricing power to grow both internally and via acquisitions. PwC bought Chicago's Diamond Management & Technology Consultants Inc. in 2010 and startup Ant's Eye View, a Seattle-based social media strategy firm, last year. **Deloitte** bought assets of Monitor Group in Cambridge, Mass., out of bankruptcy for $120 million.

Because of the emphasis on consulting, campus recruiting is changing. Besides harvesting hires from the University of Illinois at Urbana-Champaign and other undergraduate plantations for accounting majors, the Big Four are wooing master's degree recipients in IT, computer science, organizational change and, of course, accounting, finance and statistics. Ernst & Young says it's active at the University of Michigan and Indiana University, among other campuses.

DIFFERENT WORLDS

Cultural issues, however, accompany acquisitions, especially when salty, middle-market practitioners join highly bureaucratic organizations, with their sensitivity training and torturous client-conflict reviews; many new arrivals count the days until earn-out agreements run their course and they can leave.

"There's definitely a huge difference between both those worlds," says Steven Sherman, who this year departed KPMG LLP—on good terms, he says—after 30-plus years to build a consulting practice at Loop Capital Holdings LLC. "The acquisition model has historically underdelivered."

Byron Spruell, **Deloitte**'s new central region managing partner, said in July he would emphasize more internal collaboration and teamwork. He declines to be interviewed.

In 2007, a KPMG subsidiary acquired assets of New York-based Keen Consultants and Keen Realty, whose principals later defected to Deerfield-based restructuring adviser Great American Group LLC.

"I think after three years of being there, we just liked being smaller better. . . .I look back on the experience as an overall positive,"says Matthew Bordwin, a New York-based co-president of Great American unit GA Keen Realty Advisors.

Hires also can be frustrated by Sarbox's auditor independence rules, which lay out what consultants can and cannot do for their firms' audit clients.

"We're happy with the way the integration has gone," says Charles Kuoni, who joined **Deloitte** in Chicago last year when the firm subsumed New York-based restructuring firm CRG Partners. "The downside is, there are rules and regulations that small firms don't necessarily concern themselves with. The issue for us was understanding 'independence' . . . (which) is still a learning process for us."

Crain Communications, Inc.

Document CCHI000020131010e9a70000f

Detroit Division

Former Detroit Public Schools Accountant Sentenced on Fraud and Money Laundering Charges

U.S. Attorney's Office
December 18, 2013

Eastern District of Michigan
(313) 226-9100

Sandra Campbell, 60, a former Detroit Public Schools contract accountant and School Board candidate, was sentenced to nearly six years in federal prison today by United States District Judge Julian Abele Cook on charges of program fraud conspiracy, money laundering conspiracy, and tax charges, following a five-week jury trial that took place in August, United States Attorney Barbara L. McQuade announced today.

McQuade was joined in the announcement by Special Agent in Charge Paul M. Abbate, Federal Bureau of Investigation; Special Agent in Charge, Erick Martinez, Internal Revenue Service, Criminal Investigation; and Detroit Public Schools Emergency Manager Jack Martin.

Sandra Campbell was sentenced to 70 months in federal prison on charges of program fraud against the Detroit Public Schools, money laundering, and criminal tax fraud. In addition, Campbell was ordered to pay restitution to the Detroit Public Schools in the amount of $530,091. Co-defendant Domonique Campbell, daughter of Sandra Campbell, is set to be sentenced on January 7, 2014, at 11 a.m.

The evidence presented at trial established that between 2004 and 2008, Sandra Campbell and Domonique Campbell obtained in excess of $530,000 from the Detroit Public Schools through a fraudulent scheme in which orders were placed with the Campbells' sham company for books and educational materials never provided to the schools. Sandra Campbell and Domonique Campbell conspired to launder the fraud proceeds and to defraud the Internal Revenue Service and failed to report the money they fraudulently obtained from the Detroit Public Schools as income on their tax returns.

United States Attorney Barbara L. McQuade said, "Anyone who considers defrauding our schools should take note that we are scrutinizing records and conduct, and we will prosecute those who steal funds intended to educate our children."

DPS Emergency Manager Martin stated, "This sentence sends a powerful message that fraudulently converting DPS resources for personal gain and thereby depriving students of the tools they need to prepare for educational and employment opportunities will not be tolerated. If you steal DPS resources, you will get caught, and you will be prosecuted."

FBI Special Agent in Charge Paul M. Abbate stated, "In this case, the defendant's criminal actions amounted to stealing the opportunity for a quality education from our children. Such conduct cannot, and will not, be tolerated. The FBI Detroit Field Office, together with our local, state, and federal partners, will continue to battle public corruption and hold those responsible accountable for their actions."

IRS Special Agent in Charge Erick Martinez stated, "Those who profit at the expense of our children and steal from our community will be held accountable for their greedy actions."

The case was investigated by special agents of the FBI, IRS, and Department of Education-Office of Inspector General, with the assistance of Detroit Public Schools-Office of Inspector General. The case was investigated and prosecuted by Assistant United States Attorneys J. Michael Buckley and Bruce Judge of the Public Corruption Unit.

Detroit Division Links

Detroit Home

Contact Us
- Overview
- Territory/Jurisdiction

News and Outreach
- Press Room | Stories
- In Your Community

About Us
- Our People & Capabilities
- What We Investigate
- Our Partnerships
- Detroit History

Wanted by the FBI - Detroit

FBI Jobs

Accountants' professional conduct in relation to taxation

CMS Cameron McKenna
Simon Garrett, Aaron Fairhurst and John Enoch

United Kingdom
March 18 2014

The Chartered Institute of Taxation has published final guidance on professional conduct standards to be applied by advisers when giving tax advice. This publication is timely in light of recent debate as to the extent to which accountants may legitimately advise clients on tax planning. HMRC has approved this guidance as an acceptable basis for its dealings with tax advisers. We have increasingly seen PI claims against advisers who have had a hand in tax mitigation schemes and this note provides some guidance based on our experience of these complaints.

General Points

The Guidance provides examples of situations likely to confront tax advisers, but advisers must observe fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour across all their professional activities.

In addition to the overriding principle of demonstrating integrity at all times, particular themes stressed throughout the report include: the need to preserve client confidentiality in all situations other than where the law compels the adviser otherwise; the obligation that the adviser both understands and explains to the client the risks associated with tax-related decisions and the potential consequences of challenge; the importance of assessing money-laundering implications before and at all stages of financial transactions; and the criticality of documenting all advice given. Advisers must also remain vigilant to the possibility of tax evasion when involved in what is ostensibly lawful planning.

Specific Points

Tax returns: Advisers must act in good faith in dealings with HMRC. An adviser must not assert a tax position which he considers has no sustainable basis. An adviser must exercise appropriate professional scepticism when making statements or asserting facts on behalf of a client. The adviser must ensure that the client understands his responsibility for the accuracy of the tax return and approves the return before submission, even if it is submitted electronically.

Compliance with HMRC: The Guidance distinguishes between informal requests from HMRC and the exercise of their statutory powers. Disclosure in response to informal requests can only be made with the client's permission. The adviser should advise the client as to the reasonableness of any informal request and the likely consequences of non-compliance so that the client can decide on his preferred course of action. With regard to statutory requests, especially those made under Schedule 36 Finance Act 2008, advisers are reminded that such

a request may override the adviser's duty of confidentiality to his client; failure to comply may expose the adviser to serious penalties.

Irregularities: The Guidance provides a flowchart on steps the adviser should take, including informing HMRC or filing MLRO/NCA reports if appropriate. In essence, an adviser must inform the client as soon as possible of any error and its consequences and seek to persuade the client to behave correctly. The adviser must also consider whether the irregularity could give rise to a circumstance requiring notification to PI insurers. The adviser must take care that he or she does nothing to assist a client plan or commit any offence or conceal any offence which has been committed. An adviser is not under a duty to make enquiries to identify irregularities which are unrelated to the work in respect of which he has been engaged, but if he does become aware of any irregularity in a client's tax affairs he should follow the Guidance. Where the client and adviser have complied with all their obligations under tax law and HMRC has failed to take any necessary action to start an enquiry or amend an assessment, the adviser is generally under no legal obligation to draw HMRC's failure to their attention.

Voluntary disclosure under special disclosure facilities: The Guidance warns advisers of risks associated with accepting engagements where a client is seeking to regularise tax affairs through voluntary disclosure of past evasion or concealment. Before accepting an assignment, advisers must seek reassurance that the client will make a full and frank disclosure to the adviser and regularise his affairs in all respects. The adviser must be mindful of the fact that tax regularisation can be a money-laundering tool. Extra customer due diligence checks are required.

Tax planning, tax avoidance and tax evasion: The Guidance refers to recent HMRC publications on tax avoidance and the General Anti-Abuse Rule (GAAR). It points out risks to advisers resulting from involvement with tax avoidance schemes, including regulatory scrutiny or investigation and possible criticism from the media, Government and other stakeholders. Factors that may indicate tax avoidance are listed. The difference between tax avoidance and tax planning is discussed.

An adviser should be aware of the client's expectations around the aggressiveness of tax planning or tax avoidance arrangements and ensure that the engagement letter reflects and limits the adviser's role and responsibilities. Ultimately, it is the client's decision, having received advice, as to what planning is appropriate. The adviser must however warn the client clearly of potential risks. An adviser should not recommend any plan if the adviser concludes that it would be ineffective based on the GAAR or tax law. Factors to consider and advise on include: the strength of any legal interpretation (counsel's opinion) relied upon; the potential application of the GAAR; implications in relation to the client's tax return; the risk of HMRC challenge; the risk of litigation; reputational risk; stress for the person or business in the event of prolonged dispute with HMRC; or the potential impact on tenders for government contracts.

Comment

We are seeing an increasing number of complaints against accountants, tax advisers and financial advisers arising out of failed tax mitigation schemes. Much of the criticism concerns a lack of clear warning about the potential for HMRC challenges and the potential scale of the exposure if HMRC's challenges are successful. While the Guidance strictly only constitutes

advice given by the Chartered Institute of Taxation to its members, courts may find it persuasive as to the expected professional behaviour of all advisers operating in the tax sphere, such as members of the law society or even those operating in an unregulated capacity. All advisers should therefore consider putting appropriate measures in place commensurate with the size of their practice and the extent to which they are involved in areas which constitute tax planning/mitigation, including training, technical briefings and protocols to ensure quality and consistency of treatment and advice. Clear engagement letters are critical, as are clear written advices explaining fully and frankly all the potential advantages and disadvantages of any particular course of action. Proper records of face to face meetings at which advice is discussed are critical evidence if a complaint is later received.

Auditors at Big Firms Cited for More Deficiencies

By EMILY CHASAN

Senior Editor

The Big Number: 37.5%

That's the proportion of audits by large accounting firms found to have deficiencies.

Auditors at the seven largest U.S. accounting firms were cited for deficiencies in 37.5% of audits inspected by U.S. regulators in 2011, according to an analysis of the most recent data from the government's audit watchdog.

That figure, which includes audits completed by PricewaterhouseCoopers LLP, Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP, BDO USA LLP, McGladrey LLP and Grant Thornton LLP, was up from 32.6% in 2010, and has more than doubled from 14.8% in 2009.

About 31% of the deficiencies involved auditors' evaluation of the market prices companies supplied for complex assets, down from about half in the prior year, according to an analysis by business-valuation firm Acuitas Inc.

In previous years, the most common valuation errors were caused by auditors' failure to understand methods and assumptions used by third-party pricing services. But one in three of those deficiencies uncovered by the 2011 inspections involved failures to test managers' assertions about the methods and data used to value assets.

Auditors also were cited for failing to get enough evidence in their audit of a company's internal controls or financial statements, according to the Public Company Accounting Oversight Board, the government agency that inspects audits.

Grant Thornton

Reporting Entity Sector Profiles: Life Insurance Appendices

Prepared for FINTRAC | March 31, 2014

Appendix 9

Appendix A: Industry statistics and reporting entity data

Life insurance SIC codes

Code	Description
6411	Insurance Agents, Brokers, and Service
6311	Life Insurance

Life insurance NAICS codes

Code	Description
524113	Direct Life Insurance Carriers
524114	Direct Individual Life, Health and Medical Insurance Carriers
52421	Insurance Agencies and Brokerages

Using NAICs codes, searches for statistical data on the Life Insurance Industry sector were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Direct Life, Health and Medical Insurance Carriers (NAICS 52411)

Exclusions

- Government establishments providing health insurance (91291, other Provincial and Territorial Public Administration); and
- Establishments primarily engaged in reinsuring life, health and medical insurance (52413, Reinsurance Carriers).

Number of establishments in Canada by type and region: December 2012
Direct Life, Health and Medical Insurance Carriers (NAICS 52411)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	61	24	85	11.7%
British Columbia	78	20	98	13.5%
Manitoba	31	4	35	4.8%
New Brunswick	16	6	22	3.0%
Newfoundland and Labrador	9	1	10	1.4%
Northwest Territories	1	0	1	0.1%
Nova Scotia	21	4	25	3.4%
Nunavut	0	0	0	0.0%
Ontario	214	52	266	36.6%
Prince Edward Island	3	0	3	0.4%
Quebec	121	27	148	20.4%
Saskatchewan	24	9	33	4.5%
Yukon Territory	0	1	1	0.1%
CANADA	579	148	727	100%
Percent Distribution	79.6%	20.4%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Direct Life, Health and Medical Insurance Carriers (NAICS52411)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	20	31	7	3
British Columbia	24	46	6	2
Manitoba	15	12	2	2
New Brunswick	2	8	5	1
Newfoundland and Labrador	3	4	2	0
Northwest Territories	0	1	0	0
Nova Scotia	7	11	1	2
Nunavut	0	0	0	0
Ontario	60	117	30	7
Prince Edward Island	1	1	1	0
Quebec	40	60	15	6
Saskatchewan	12	10	1	1
Yukon Territory	0	0	0	0
CANADA	184	301	70	24
Percent Distribution	31.8%	52.0%	12.1%	4.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Direct Individual Life, Health and Medical Insurance Carriers - (NAICS 524111)

Exclusions

- Government establishments providing health insurance (9s1291, Other Provincial and Territorial Public Administration); and
- Establishment primarily engaged in: reinsuring life insurance (524131, Life Reinsurance Carriers); and reinsuring health insurance (524132, Accident and Sickness Reinsurance Carriers).

Number of establishments in Canada by type and region: December 2012 Direct Individual Life, Health and Medical Insurance Carriers (NAICS 524111)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	41	16	57	10.2%
British Columbia	59	16	75	13.4%
Manitoba	22	2	24	4.3%
New Brunswick	10	5	15	2.7%
Newfoundland and Labrador	7	1	8	1.4%
Northwest Territories	1	0	1	0.2%
Nova Scotia	16	1	17	3.0%
Nunavut	0	0	0	0.0%
Ontario	175	39	214	38.4%
Prince Edward Island	2	0	2	0.4%
Quebec	95	23	118	21.1%
Saskatchewan	19	7	26	4.7%
Yukon Territory	0	1	1	0.2%
CANADA	447	111	558	100%
Percent Distribution	80.1%	19.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Direct Individual Life, Health and Medical Insurance Carriers (NAICS524111)				
Province or Territory	**Employment Size Category (Number of employees)**			
	Micro 1-4	**Small 5-99**	**Medium 100-499**	**Large 500+**
Alberta	15	24	0	2
British Columbia	23	32	2	2
Manitoba	11	9	1	1
New Brunswick	1	7	1	1
Newfoundland and Labrador	2	4	1	0
Northwest Territories	0	1	0	0
Nova Scotia	5	8	1	2
Nunavut	0	0	0	0
Ontario	46	98	24	7
Prince Edward Island	1	1	0	0
Quebec	35	46	10	4
Saskatchewan	11	7	0	1
Yukon Territory	0	0	0	0
CANADA	150	237	40	20
Percent Distribution	33.6%	53.0%	8.9%	4.5%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Insurance Agencies and Brokerages (NAICS 52421)

Number of establishments in Canada by type and region: December 2012 Insurance Agencies and Brokerages (NAICS 52421)				
Province or Territory	**Employers**	**Non-Employers/ Indeterminate**	**Total**	**% of Canada**
Alberta	1,007	523	1,530	11.8%
British Columbia	1,240	613	1,853	14.3%
Manitoba	354	159	513	3.9%
New Brunswick	208	89	297	2.3%
Newfoundland and Labrador	113	34	147	1.1%
Northwest Territories	4	0	4	0.0%
Nova Scotia	202	90	292	2.2%
Nunavut	0	0	0	0.0%
Ontario	3,323	1,895	5,218	40.2%
Prince Edward Island	34	10	44	0.3%
Quebec	1,532	1,051	2,583	19.9%
Saskatchewan	339	167	506	3.9%
Yukon Territory	6	1	7	0.1%
CANADA	8,362	4,632	12,994	100%
Percent Distribution	64.4%	35.6%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Insurance Agencies and Brokerages (NAICS52421)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	539	463	5	0
British Columbia	607	625	7	1
Manitoba	179	174	1	0
New Brunswick	121	86	1	0
Newfoundland and Labrador	63	50	0	0
Northwest Territories	2	2	0	0
Nova Scotia	94	108	0	0
Nunavut	0	0	0	0
Ontario	1,918	1,381	23	1
Prince Edward Island	21	13	0	0
Quebec	954	569	8	1
Saskatchewan	189	149	1	0
Yukon Territory	3	3	0	0
CANADA	4,690	3,623	46	3
Percent Distribution	56.1%	43.3%	0.6%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Direct Group Life, Health and Medical Insurance Carriers (NAICS 524112)
Exclusions

- Government establishments providing health insurance and establishments primarily engaged in: reinsuring life insurance (524131, Life Reinsurance Carriers); and
- Reinsuring health insurance (524132, Accident and Sickness Reinsurance Carriers).

Number of establishments in Canada by type and region: December 2012 Direct Group Life, Health and Medical Insurance Carriers (NAICS 524112)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	20	8	28	16.6%
British Columbia	19	4	23	13.6%
Manitoba	9	2	11	6.5%
New Brunswick	6	1	7	4.1%
Newfoundland and Labrador	2	0	2	1.2%
Northwest Territories	0	0	0	0.0%
Nova Scotia	5	3	8	4.7%
Nunavut	0	0	0	0.0%
Ontario	39	13	52	30.8%
Prince Edward Island	1	0	1	0.6%
Quebec	26	4	30	17.8%
Saskatchewan	5	2	7	4.1%
Yukon Territory	0	0	0	0.0%
CANADA	132	37	169	100%
Percent Distribution	78.1%	21.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Establishments: Direct Group Life, Health and Medical Insurance Carriers (NAICS 524112)

Exclusions

Number of employer establishments by employment size category and region: December 2012 Direct Group Life, Health and Medical Insurance Carriers (NAICS524112)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	5	7	7	1
British Columbia	1	14	4	0
Manitoba	4	3	1	1
New Brunswick	1	1	4	0
Newfoundland and Labrador	1	0	1	0
Northwest Territories	0	0	0	0
Nova Scotia	2	3	0	0
Nunavut	0	0	0	0
Ontario	14	19	6	0
Prince Edward Island	0	0	1	0
Quebec	5	14	5	2
Saskatchewan	1	3	1	0
Yukon Territory	0	0	0	0
CANADA	34	64	30	4
Percent Distribution	25.8%	48.5%	22.7%	3.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Sic Code 6411 – Insurance Agents, Brokers, and Service

Province	Number of Establishments
Alberta	1,700
British Columbia	1,926
Manitoba	652
New Brunswick	441
Newfoundland and Labrador	245
Northwest Territories	10
Nova Scotia	475
Nunavut	2
Ontario	4,994
Prince Edward Island	77
Quebec	3,037
Saskatchewan	678
Yukon	15
Total	14,252

Sic Code 6311 – Life Insurance

State Or Province	Number of Establishments
Alberta	1
British Columbia	12
Manitoba	5
New Brunswick	2
Ontario	36
Quebec	35
Saskatchewan	2
Total	93

NAICs Code 524113 - Direct Life Insurance Carriers

State Or Province	Total
Alberta	1
British Columbia	12
Manitoba	5
New Brunswick	2
Ontario	36
Quebec	35
Saskatchewan	2
Grand Total	93

NAICs Code 524114 - Direct Life Insurance Carriers

State Or Province	Total
Alberta	5
British Columbia	7
Manitoba	1
New Brunswick	2
Newfoundland and Labrador	5
Ontario	57
Quebec	4
Grand Total	81

NAICs Code 524210 - Insurance Agencies and Brokerages

Province	Number of Establishments
Alberta	1,512
British Columbia	1,732
Manitoba	601
New Brunswick	407
Newfoundland and Labrador	223
Northwest Territories	9
Nova Scotia	444
Nunavut	2
Ontario	4,627
Prince Edward Island	69
Quebec	2,767
Saskatchewan	647
Yukon	12
Total	13,052

OSFI Federally Regulated Life Insurance Companies	
Canadian Life Insurance Companies	42
Foreign Life Insurance Companies	35

Canadian Life Insurance Companies

- ACE INA Life Insurance
- Allstate Life Insurance Company of Canada
- Assurant Life of Canada
- Aurigen Reinsurance Company
- Blue Cross Life Insurance Company of Canada
- BMO Life Assurance Company
- BMO Life Insurance Company
- Canada Life Assurance Company
- Canada Life Financial Corporation
- Canada Life Insurance Company of Canada
- Canadian Premier Life Insurance Company
- Capital Financial Security Insurance Company
- CIBC Life Insurance Company Limited
- CIGNA Life Insurance Company of Canada
- CompCorp Life Insurance Company
- Co-operators Life Insurance Company
- CT Financial Assurance Company
- CUMIS Life Insurance Company
- Empire Life Insurance Company
- Equitable Life Insurance Company of Canada
- Foresters Life Insurance Company
- Great-West Life Assurance Company
- London Life Insurance Company
- Manufacturers Life Insurance Company
- Manulife Financial Corporation
- MD Life Insurance Company
- National Life Assurance Company of Canada
- Primerica Life Insurance Company of Canada
- Provenance Life Insurance Company
- RBC Life Insurance Company
- Reliable Life Insurance Company
- RGA Life Reinsurance Company of Canada
- Scotia Life Insurance Company
- Standard Life Assurance Company of Canada
- Sun Life Assurance Company of Canada
- Sun Life Financial Inc.
- Sun Life Insurance (Canada) Limited
- TD Life Insurance Company
- Transamerica Life Canada

- VSP Canada Vision Care Insurance
- Wawanesa Life Insurance Company
- Western Life Assurance Company

Foreign Life Insurance Companies

- Aetna Life Insurance Company
- Allianz Life Insurance Company of North America
- American Bankers Life Assurance Coy of Florida
- American Health and Life Insurance Company
- American Income Life Insurance Company
- AXA Equitable Life Insurance Company
- CMFG Life Insurance Company
- Combined Insurance Company of America
- Connecticut General Life Insurance Company
- Employers Reassurance Corporation
- GAN Assurances Vie Compagnie française d'assurances vie mixte
- General American Life Insurance Company
- General Re Life Corporation
- Gerber Life Insurance Company
- Hartford Life Insurance Company
- Liberty Life Assurance Company of Boston
- Life Insurance Company of North America
- Metropolitan Life Insurance Company
- Munich Reinsurance Company
- New York Life Insurance Company
- Partner Reinsurance Company Ltd.
- Partner Reinsurance Europe SE
- Pavonia Life Insurance Company of Michigan
- Phoenix Life Insurance Company
- Principal Life Insurance Company
- Prudential Assurance Company Limited (UK)
- Reassure America Life Insurance Company
- ReliaStar Life Insurance Company
- SCOR Global Life
- Standard Life Assurance Company 2006
- Standard Life Assurance Limited
- State Farm International Life Insurance Co
- Swiss Reinsurance Company Ltd (Life Branch)
- United American Insurance Company

Source: OSFI

Life Insurance Industry - Market Value

Canada Life Insurance Market Value: US$ billion, 2008-2012		
Year	US$ billion	% Growth
2008	49.7	
2009	51.6	3.8%
2010	51.8	0.5%
2011	51.4	(0.7%)
2012	51.8	0.6%
Compound Annual Growth Rate (CAGR): 2008-2012		1.0%

Source: MarketLine, January 2014

Life Insurance Industry - Market Value Forecast

Canada Life Insurance Market Value Forecast: US$ billion, 2012-2017		
Year	US$ billion	% Growth
2012	51.8	0.6%
2013	55.3	6.9%
2014	56.9	2.7%
2015	58.3	2.5%
2016	60.0	3.0%
2017	61.5	2.5%
Compound Annual Growth Rate (CAGR): 2012-2017		3.5%

Source: MarketLine, January 2014

Life Insurance Industry – Category Segmentation

Canada's Life Insurance Market Category Segmentation: US$ billion, 2012		
Category	2012	%
Life Insurance	15.4	29.7%
Pension/annuity	36.4	70.3%
Total	51.8	100%

Source: MarketLine, January 2014

Life Insurance Industry – Geography Segmentation

Canada's Life Insurance Market Category Segmentation: US$ billion, 2012		
Category	2012	%
United States	567.8	82.6%
Canada	51.8	7.5%
Mexico	10.9	1.6%
Rest of the Americas	57.3	8.3%%
Total	687.8	100%

Source: MarketLine, January 2014

Life Insurance Industry – Market Share

Canada's Life Insurance Market Share: % share, by value, 2012	
Company	% Share
Munich Re. Canada (Life)	18.3%
Sun Life Financial	11.8%
The Great-West Life Assurance Company	11.7%
The Manufacturers Life Insurance Company	10.2%%
Other	48.0%
Total	100%

Source: MarketLine, January 2014

Appendix B: Case examples and typologies

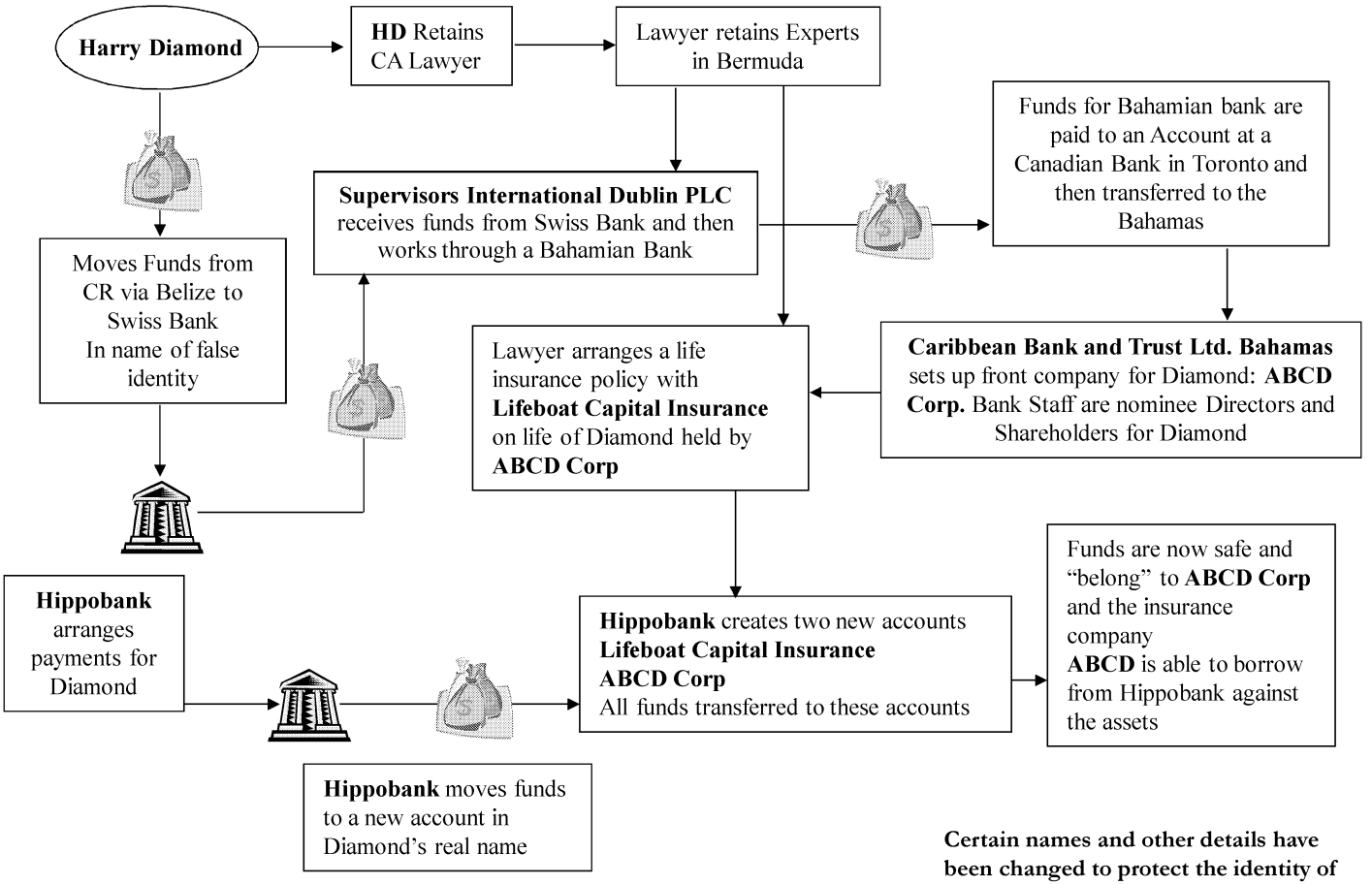
The enclosed articles have been sourced from: news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. "Life Insurance" Money Laundering Vehicle Example.
2. Through Canada's insurance loophole. The Globe and Mail, Friday December 17, 2010.
3. What your insurance broker doesn't want you to know. The Globe and Mail, December 21, 2010.
4. Money laundering in Canada: An analysis of RCMP cases. Nathanson Centre for the Study of Organized Crime and Corruption. Chapter 10 – Insurance.
5. New hiding place for drug profits: Insurance policies. The New York Times, December 6, 2002.
6. Insurance agents ordered to repay $3.7 million gained by fraud. Montreal Gazette, March 20, 2014.
7. Man charged for defrauding client out of $21,000. Toronto Star, November 28, 2013.
8. Former Texas businessman sentenced to 60 years for his role in $100M insurance fraud. Canadian Press, September 28, 2011.
9. Ex-NFL lineman charged in scheme. FoxSports.com, August 2, 2013.
10. Accused controls tax haven companies. Canberra Times. October 21, 2013.
11. Los Angeles man gets 13 years in federal prison in Texas life settlement insurance fraud case. Associated Press. December 19, 2013.
12. Former employee of National Prearranged Services Inc. and Lincoln Memorial life Insurance Company Brent Cassity pleads guilty to fraud and money laundering charges. Department of Justice Documents, July 3, 2013.
13. Seven charged in life insurance fraud scheme. Department of Justice Documents, July 25, 2012.
14. Insurance Gateway for money laundering. The Times of India. May 8, 2013.
15. Frauds blow and hole in insurance firms. Mail Today, March 5, 2012
16. Irda fines Tata AIA for violating anti-money laundering norms. Press Trust of India, February 13, 2014.

17. Staff at LIC, Birla Sunlife, Reliance Life others accused of 'helping' people avoid tax. The Times of India. May 8, 2013.

18. Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities. Narrative summaries of Reasons for Listing – Q1.A.201.05. Yasser Mohamed Ismail Abu Shaweesh. September 16, 2009.

"Life Insurance" Money Laundering Vehicle



Certain names and other details have been changed to protect the identity of involved parties.

THE GLOBE AND MAIL

Through Canada's insurance loophole

TARA PERKINS **AND** GRANT ROBERTSON
The Globe and Mail
Published Friday, Dec. 17 2010, 8:41 PM EST
Last updated Tuesday, Jul. 31 2012, 4:56 PM EDT

Lynne Rae Zlotnik had insurance in her blood.

Her father, Harold, began selling policies in 1945 and eventually she followed in his footsteps. "Insurance," Harold Zlotnik liked to say, "is the business of financing dreams."

But when insurance regulators began looking into Vancouver-based Lynne Zlotnik Wealth Management Inc. this year - a firm she created in 2006 to sell life insurance and other investment products - they were troubled by what they found.

More related to this story

- Graphic Canada's new insurance landscape
- Graphic Traditional insurance sales in Canada
- Graphic By the numbers: Insurance premiums in Canada

Several of her clients had invested a total of more than $1.4-million in her company on the promise of a lucrative return. The clients included 96-year-old Katie Sturhahn, who cashed out a $200,000 segregated fund, an investment fund that comes with insurance guarantees, and instead put her faith in the insurance agent.

It was a questionable financial strategy, since the payout on the fund - which she intended to leave her five children - was assured. Soon after the elderly woman died in March, the agent declared bankruptcy, and the money was gone.

"That was our inheritance," says her son, 71-year-old Walt Sturhahn. "We've got none of it."

But an even more disturbing discovery had yet to be made: When regulators went looking for someone responsible for overseeing such a risky financial transaction, there was no one to answer for it. The regular checks and balances that are designed to oversee an insurance agent had failed.

The insurance company that administered the policy had no direct oversight over Ms. Zlotnik. In a practice that is increasingly common throughout the industry, she dealt with a middleman company called a Managing General Agent, or MGA, which is an unregulated wholesaler of insurance products to independent agents that few consumers know about. That made it difficult for regulators to scrutinize her conduct.

The case exemplifies a problem that's emerged as the insurance industry becomes increasingly complex. As the sale of life insurance has evolved over the past decade - designed to sell more policies and maximize profits for insurers and agents in an already-mature market - it has also placed consumers at risk.

A Globe and Mail investigation has uncovered a gaping hole in Canadian insurance regulation: Cases like the Sturhahns' are not isolated events. Instead, nearly half of all individual life insurance policies in Canada are now being transacted through MGAs, which often undertake little - if any - oversight of agents in the market.

Though consumers place trust in their agents and increasingly look to them for financial advice and to explain complex policies and products, insurance regulation hasn't kept pace with the industry, and doesn't take these wholesalers into account. Across the country, MGAs operate beyond the watch of regulators - leaving consumers exposed.

Though regulators can revoke an agent's licence - Ms. Zlotnik lost hers in April - by that time it's too late for the consumer. The damage can't be undone and the money may be unrecoverable. With closer oversight, the sudden cancellation of insurance policies such as Ms. Sturhahn's or decisions resulting from poor financial advice would be detected earlier, when the moves could still be reversed in the consumer's favour if questionable circumstances were found.

"[My brother]said 'Just forget it, forget it,' " said Mr. Sturhahn, who is wheelchair-bound and suffers from asbestosis after a career as a carpenter. "And I'm trying, but it's hard to forget when you're living on a shoestring and something like that happens."

When Gerald Matier, executive director of the Insurance Council of British Columbia, which licenses agents in the province, looked into the matter, he was stunned: Since Ms. Zlotnik was working through an MGA, no one was directly responsible for overseeing the agent.

When he asked the MGA whether anyone thought to question the cashing in of an insurance product by a 96-year-old woman, he learned that no one had, because there are no regulatory requirements for MGAs to police life insurance agents.

It was a problem that no one, not even regulators like Mr. Matier, saw coming.

Twenty-five years ago, most insurance agents were contracted directly by the insurance companies whose policies they sold. Agents were in-house representatives of firms such as Manulife or Sun Life and employers were responsible for keeping tabs on their sales forces.

"When there was a problem, the regulator would know, 'Well, this is a London Life agent,' so they would contact London Life's compliance department ... because it was that company's responsibility," says Peter Lamarche, president of the Canadian Association of Independent Life Brokerage Agencies, a growing MGA industry group. "In

the new environment, the regulator doesn't know who to call."

Today, most agents are independent, and can sell policies from multiple insurers.

As a result, the new breed of managing general agents has quickly sprung up. And in the span of a decade, these agencies have quietly grown into one of the most powerful forces in Canada's life insurance industry by offering to help insurers deal with a large roster of independent agents, while helping agents obtain access to various policies sold by insurers, in exchange for a cut of the action.

According to Investor Economics, a financial industry consultancy, the MGA channel is now responsible for at least 44 per cent of the new life insurance policies sold to individuals across the country.

That means nearly half of all policies are being sold with serious gaps in regulatory oversight.

The MGA explosion has severed the chain of oversight between insurance companies and agents, but the full effect of that development is hard to quantify. Regulators are, at best, only beginning to grapple with the sector's fast rate of growth.

Those watchdogs are painfully behind the curve.

Mr. Matier tried to find a solution, but could barely find agreement on what the role of an MGA should be inside the industry - a disinterested middleman, or a key link in the supply chain that should be responsible for the agents it supplies with policies. It is an issue in all provinces. But rather than spring into action, regulators have been blindsided.

Meanwhile, there are signs the MGA industry itself is trying to stave off regulation, worried that new rules will be bad for the bottom line.

As for the insurance companies themselves, which have made Canada an exportable brand name in reliable life insurance, they also have yet to reckon with the unintended consequences of a revolution they encouraged in order to save trouble and expense.

And the stakes are getting higher for insurers as products become more complex and therefore more difficult for consumers to understand.

Facing a mature market for life policies, insurers are looking to increase business by developing a dizzying array of new offerings, from critical illness coverage to living benefits products. Insurance agents are increasingly involved in wealth management, and advise people on tax and estate planning - functions that require careful oversight.

Prices on many products are going up, largely because low interest rates have been eating away at insurers' profit margins. Insurers have also been reducing benefits on some products.

The dollar amounts spent in the insurance sector are staggering. Canadians bought $311.6-billion worth of life insurance in 2009, bringing the total value of life insurance they own to $3.47-trillion.

In total, almost 21 million Canadians own life insurance, an average of $169,000 per person. They paid $15.1-billion worth of life insurance premiums in 2009, according to the Canadian Life and Health Insurance Association. Of that, at least $1-billion comprises life insurance policies sold directly to individual consumers.

The evolution of a new model

The life insurance industry is built on trust, and consumers put their faith in the agent they deal with to navigate a series of choices about complex products.

As Ms. Zlotnik said in a promotional video: "What I'm passionate about is to make sure that each person that I advise has a level of financial literacy. I explain all the terms [in]fairly easy digestible ways."

The video featured a number of her clients, including Gabe and Greta Milton, a retired Vancouver couple. "She makes a person feel totally comfortable, and really Lynne's explanations are so clear," Ms. Milton said. She and her husband are listed as creditors in the bankruptcy, having invested $23,000 with Ms. Zlotnik's business.

Though her case exposed a serious weakness in oversight of the MGA channel, Lynne Zlotnik maintains she did nothing wrong. She says she is the victim of an overzealous regulator and intends to appeal its ruling. She also says that a serious illness that had hospitalized her prevented her from dealing with the regulator.

"I was trying to develop an agency like my successful father," she said in an e-mail denying the allegations. "I've been in business 23 years, never had a complaint against me."

But the trust that consumers place in the life insurance industry reaches beyond the independent agent they deal with. Canadians assume that regulators are also keeping an eye on those agents, and that insurers have a stake in overseeing the way their products are sold.

Canada is known for its financial regulation, and when it comes to insurance, Ottawa watches over the capital structures of underwriters, while provincial watchdogs are responsible for policing how policies are sold.

Traditionally, life insurers assumed responsibility for the agents who sold their products and gave advice to clients. The market was dominated by insurers' in-house career sales agents, whom they recruited and were responsible for training and supervising. While oversight of agents was not embodied in law, it was enshrined in corporate practice because the insurers knew their brands were at stake if customers had problems with their agents.

The directness of the chain of responsibility from insurer to agent is clear from the industry jargon for these agents: "captives."

"Everyone worked for a company," says Kevin Cott, president of a Toronto-based MGA, Qualified Financial Services, who joined the insurance business in the early

1980s. "Advisers, training, financials, paying of commissions, monitoring, mentoring - the whole nine yards - were the responsibility of the insurer."

The life insurance industry began undergoing a low-profile but massive transformation two decades ago as the independent agent distribution model, sometimes called the broker channel, started taking hold.

The channel flourished because it helped consumers shop around without having to visit an agent at each insurer. But insurers were also enthusiastic as they realized that using independent agents would be easier and cheaper than employing a captive sales force.

Insurers generally tried to do some homework on agents before signing contracts with them, and still had a vested interest in ensuring that their advice to customers and sales tactics were up to snuff.

But as the independent sales channel grew, a problem emerged that would ultimately lead to the creation of MGAs.

To learn the ins and outs of complicated products, independent brokers were forced to deal with multiple insurers. And the insurance companies had to spend time dealing with legions of independent agents to keep them up to date. This proved unwieldy. Hence, the new corporate middlemen that evolved to fill this need.

Some MGAs were started by former career agents who saw an opportunity and wanted to branch out on their own. In some cases, career agents were pushed by the insurers themselves to start up a shop.

As the insurers wound down their own internal agent systems, Mr. Cott says, "they would often tell managers, 'Listen, we're closing down your office, but what we'll do is we'll give you a direct contract, an MGA contract if you will, for you and your people.'"

The shift to outsourcing is reflected in the career agent population, which is tracked by the Canadian Life and Health Insurance Association.

The numbers show a steady decline since 1985, when there were 22,600 career agents. For the past decade, the number has been below 10,000.

Meanwhile, the number of independent agents selling life insurance has soared to 76,300. A large but unknown number of those are now working through MGAs.

The role of career agents has dwindled to the point that they represent less than one-third of the industry's sales. The bulk of sales come from independent agents, and much of that is done through MGAs.

Only a handful of life insurers, including London Life Insurance Co. and Industrial Alliance Insurance and Financial Services Inc., are still recruiting and using career agents. Sun Life has the biggest stable, with more than 3,500 people across Canada. Manulife Financial, the largest Canadian-based life insurer, conducts more business through MGAs than any other underwriter.

"Over the last several years, we've had a strategy to significantly grow our presence in the MGA channel, and that has been driving most our growth in the life insurance business," Paul Rooney, the head of Manulife's Canadian operations, told analysts in late November.

Manulife and many other major insurers declined to be interviewed on the record about the MGA issue. Some insurance executives said that criticizing the distribution channel would be detrimental to their business.

Insurers benefit by relying more on MGAs. One example: A large proportion of life insurance commissions are paid up front, when the policies are sold. If the consumer later abandons that policy, the insurer will "charge back" the unearned commission. Under the old model, the insurer had to track down agents years after the policy was sold to get its money back. Now, MGAs get hit with the chargebacks.

But perhaps the most fundamental advantage of the MGA route is that it saves insurers the costs of recruiting and training agents. These expenses are harder to justify now that it's easy to effectively "rent" distribution, says a senior executive of one Canadian life insurer, who adds, "We love the MGA channel."

Why this became a problem

No one envisioned that an entire segment of the insurance industry would spring up unregulated - it just seemed to happen.

In the old system, before MGAs evolved, it was in the best interest of insurers to keep close relationships with their agents.

This made it easier to drive sales higher, since it exposed weaknesses in sales performance, but it also helped to spot problems. An agent with excessively high sales might be needlessly selling customers too much coverage in order to boost commissions. In such cases, a company risked losing that customer.

But the disconnect under the MGA system has created several loopholes which have direct implications for consumers should problems arise. When approached by the regulators, the insurance companies who underwrite the policies can argue that they have no knowledge of the agent's actions, and that responsibility rests with the managing general agent. The MGA, on the other hand, can deflect responsibility by suggesting that its role is not to police the sales of policies, since it is merely a middleman stocking products from the large insurers for the independent agents to sell on the street.

The industry is now a patchwork of sales practices without any standard procedures. The way MGAs oversee agents' activities varies from firm to firm. Some insurers write conditions into their contracts with MGAs specifying they must police agents, but many do not. Some insurers' contracts require that MGAs screen the agents that they hire; others don't.

"From one MGA to another, there is a different level [of supervision]and different standard at play," says Terri Di Florio, the chief executive officer of Hub Financial Inc., one of the country's largest MGAs, supplying 3,000 independent agents across the country.

That means the consumer can have no expectation of a safeguard when they buy a life insurance policy that is channelled through an MGA - and the consumer is unlikely to know that an MGA is even involved.

The sales practices of agents working for MGAs are not the only worry. The vast amounts of personal and medical information consumers provide to their agents also sit outside the rules.

"One of the big issues is privacy," said one insurance executive. "They have underwriting files from brokers that sit in their file drawers. There's no regulation and they've got medical information on people and it's just sitting there. ... I really don't think the consumer has any idea about what happens to their information once they give it in this channel."

To further cloud the picture, it's not even clear who the agent answers to. Some agents will work with more than one MGA, making it harder to determine who is responsible for any given agent.

One more wrinkle is the appearance of a new category of players, generically known as associate general agents, or AGAs. Those are agencies that don't have enough sales volume to get an MGA contract. "They have this middle ground between a brokerage contract and an MGA, and so you might be an AGA of an MGA," says an executive at a major insurer who spoke only on condition of anonymity. "So that's yet another layer. And that gets even further from the regulatory environment."

The rules are so lax that even when a regulator confronts a problem agent, it's all too easy for the agent to simply find another MGA. Earlier this year, Mr. Matier of the Insurance Council of British Columbia revoked the licence of an agent he was investigating. That didn't put the broker out of action. The agent simply found an MGA in another province - Saskatchewan - that would provide a contract, so that the agent could keep on selling policies in Canada.

"It's these kinds of issues that you're starting to see," Mr. Matier says.

No one is taking responsibility

Despite the major role the agencies are playing in selling billions of dollars of insurance products to consumers, regulators have yet to grasp how unclear the picture is, and what little oversight exists.

The Canadian Council of Insurance Regulators, an umbrella group of provincial watchdogs, became aware of the MGA issue at least two years ago and assigned a group of officials to look into it. However, the group has yet to report or take any action.

The Financial Services Commission of Ontario, the largest provincial regulator, would not comment, other than to say it is now reviewing the matter of MGAs.

Highlighting the degree to which MGAs have eluded scrutiny, even just determining how many have sprung up in Canada is difficult. "Nobody in the country is really sure how many managing general agencies there are," says Mr. Lamarche, the president of the MGA industry group.

Goshka Folda, senior managing director at the consultancy Investor Economics, estimates that there are nearly 400 MGAs operating in Canada, of which about 100 would be sizable agencies, while the remainder have one or two contracts. The largest operations supply more than 1,000 brokers; the smallest have just one contract from an insurer.

In an effort to play catch-up, the life insurance industry's umbrella group, the Canadian Life and Health Insurance Association, has developed a lengthy questionnaire asking MGAs to detail the extent of their activities.

But the association's vice-president of distribution and pensions, Leslie Byrnes, declined to be interviewed on the subject, citing a need to wait for the Canadian Council of Insurance Regulators to publish its long-overdue consultation paper on the issue.

The move by the life insurance association to start gathering information on the agencies points to how little is being done to monitor the sector's activities. Of the nearly 100 life insurance companies active in Canada, only a handful, including Sun Life and Manulife, are actively conducting any sort of auditing work on the MGAs with which they have relationships.

Some MGA players acknowledge the need for better regulation. "There probably should be some oversight. That's probably true in any professional services industry where you're advising the general public," says Ms. Di Florio of Hub Financial.

But many agencies say that they don't want to pay for any more oversight - including ensuring that consumers are not being sold inappropriate products - unless they're compensated for it. The agencies make the case that their profit margins are too thin to support the oversight and paperwork involved.

The Independent Financial Brokers of Canada, which represents about 4,000 independent financial advisers, told regulators in a recent report that significant new rules for MGAs are not necessary - and moreover would prove expensive to implement.

They would much rather just let their own insurance cover any problems.

"In the event of an administrative oversight, most agencies have corporate E&O [errors and omissions insurance] which is the appropriate recourse for consumers," the brokers association argues in documents to the regulator.

That approach means consumers may be subjected to a lengthy claims process.

In the meantime, the problem has become tangible for Mr. Matier and his team in B.C.

"The level of supervision, accountability and training that was inherent in the career insurance company model has diminished and accountability for the actions of new life agents is less clear," the B.C. regulator said in a report on the MGA issue.

"Once licensed, a life agent is not subject to any mandatory industry oversight, which differs significantly from all other sectors of the financial services sector [such as]property and casualty insurance, securities, mutual funds and real estate."

An industry left to police itself

While the state of regulatory limbo persists, MGAs are left to decide for themselves how to appropriately conduct business. Some have taken steps to police themselves and their agents, but they are the exception.

At Qualified Financial Services, Mr. Cott took matters into his own hands. The Toronto-based MGA culled its ranks, cutting its contracts with more than 130 advisers, in part because the company realized it had too many agents to keep proper tabs on.

The move raised eyebrows in the MGA industry because it was so unusual. In an otherwise free-wheeling industry, there have been few clampdowns. Mr. Cott is alone in that regard. "We, like the insurers, don't want to have 10,000 people running around that we don't know who they are, where they are or what they are doing," Mr. Cott says.

THE GLOBE AND MAIL

What your insurance broker doesn't want you to know

GRANT ROBERTSON **AND** TARA PERKINS
The Globe and Mail
Published Tuesday, Dec. 21 2010, 7:32 PM EST
Last updated Thursday, Aug. 23 2012, 4:03 PM EDT

In a closed-door meeting this summer, executives at one of Canada's best-known life insurance companies gathered at its headquarters to plot the latest moves in their industry's secret war.

It's a war fought with weapons that look harmless on the surface: deluxe trips to sunny destinations, offered to the independent brokers on whom the insurers rely to sell their life policies.

More related to this story

- Deflation 'worst possible world' for life insurers
- Through Canada's insurance loophole
- Retirement a distant dream for many entrepreneurs

The executives knew they would have to spend at least $8,000 to $12,000 per broker to be competitive. And the trip had to be enticing - something on the order of a Brazilian beach getaway or a luxury trek through Asia.

At a time when low interest rates have squeezed the insurance industry's profit margins, the company knew that if the brokers weren't kept happy, they could easily shift their business to a competitor offering better compensation and perks.

Two key parameters had to be kept in mind. First, a few hours during the week-long trip had to be set aside for a seminar, so that the company could deem the excursion an educational conference. And second, the budget had to include a guest for each broker - even though this doubled the cost.

Buttering up each broker's better half was all part of the strategy. "We say, 'If you want to come here again as a guest, you better tell your guy to sell our stuff,'" said a senior executive present at the meeting.

Although the battle to win brokers' affections has become a defining characteristic of Canada's life insurance industry, it's kept well out of the sight of the consumers, businesses and corporations who are buying policies - and who, the insurers admit, are paying for the trips, too.

Regulators and the industry examined the issue six years ago, and publicly acknowledged that some practices - including how brokers are compensated - weren't in alignment with the customers' best interests. But the brokers pushed back, and little changed.

An investigation by The Globe and Mail has found that attempts to improve transparency in Canada have been thwarted by the industry's successful efforts to water down proposed reforms. Yet at the same time the industry has kept compensation details under wraps, many of its products have evolved into complex financial instruments that are hard for average consumers to comprehend.

When Canadians purchase life insurance now, their broker typically hands them an industry form letter promising that "any insurance product I recommend will be the one I deem to be best suited to meet your needs, without regard to the compensation practices of any one company."

But the promise does not reflect the reality of the business for the big underwriters, such as Manulife Financial Corp., Sun Life Financial Inc., Great-West Lifeco Inc., Standard Life Assurance Co. of Canada, and Industrial Alliance Insurance and Financial Services Inc., and the thousands of brokers across the country.

Rather than scouring the market to find the best coverage, and the best price, for the clients sitting across from them, many independent agents and brokers steer all their business to just one or two insurers, according to a number of high-ranking insurance executives interviewed by The Globe. They favour the ones that reimburse them most generously in commissions, bonuses and perks, such as those all-expenses-paid trips to break up the monotony of a long Canadian winter.

The incentives have distorted the sales process for a sophisticated product and broken the bonds of trust that the insurance industry was built on. The problem, these executives say, is becoming more acute: The industry is locked in a kind of compensation race as brokers push for ever-richer incentives and insurers know they must match or better their rivals' offerings.

Insurance broker representatives don't agree there is a problem. "I don't see consumers worried about compensation in the industry," said Greg Pollock, the head of Advocis, a Canadian association that represents advisers and agents in the financial services industry. "I don't see that there's an issue that needs to be addressed."

Authorities on compensation rules in Ontario told The Globe and Mail they have decided that consumers are better off without the details of trips, commissions and bonuses clouding their decision. And the industry has worked hard to keep it that way.

Spokespeople for major insurers including Manulife , Sun Life , Great-West Lifeco , and Standard Life declined to comment on the issue and referred the questions to the Canadian Life and Health Insurance Association. Frank Swedlove, the association's president, said in an e-mailed statement that "the issue of conflicts of interest - real or perceived - arising from compensation is one that the life and health insurance industry, and its regulators, take very seriously."

But several high-ranking executives at Canada's largest insurance companies talked to The Globe and

Mail about the lack of disclosure and the problems it has created. They only did so on condition of anonymity, because they feared that by speaking publicly they could face a backlash from the brokers who sell their products.

"We've gone out and said we want to discontinue the incentives, but essentially the brokers won't give you policies if you did that," one senior executive said.

"The incentives breed a type of behaviour that's not good for the industry."

While the industry's workings are opaque to consumers, the picture is much clearer to professionals like Jeff Schaafsma, chief risk officer for the city of Surrey, B.C. He is an expert in buying insurance, and must manage file cabinets full of complex policies to cover everything from city employees to construction sites.

"If you come in from the outside and look at the insurance industry, you think, 'How could this be so unregulated?' " Mr. Schaafsma says.

"And you think, why would people accept this - handshake deals, and millions of dollars moving around and not really understanding how it's moving? The premium goes up, the premium goes down, and nobody knows why."

Canadians pay about $15-billion in life insurance premiums each year, and another $40-billion in premiums on property and casualty (P&C) policies, primarily for home and car insurance. Last year about 757,200 individual life insurance policies were sold, averaging $271,600 each. New individual policies sold today are almost twice the size they were 10 years ago.

Billions of dollars in commissions flow every year from these sales. Canadian-based life insurers paid $7.2-billion to agents worldwide in 2009, up 26 per cent from $5.7-billion at the end of 2005. A significant proportion of that money was paid to agents in Canada. Foreign-based life companies paid nearly $600-million in commissions in this country, up slightly from $590-million in 2005. Canadian property and casualty insurers shelled out another $3.74-billion in commissions in 2009, which rose 17 per cent since 2005, according to data the companies file with the Office of the Superintendent of Financial Institutions.

Many of the incentives have little, if anything, to do with serving the customer; rather, they're paid by insurance companies to keep the brokers coming back to them.

"For claiming to be independent and working in the best interests of their clients, brokers keep their cards quite close to their chest in terms of what they're being paid and by whom," Mr. Schaafsma said. "It's the wild west."

Commissions, bonuses, perks

Until the early 1990s, major life insurers like Manulife and Sun Life sold the majority of their policies

through in-house sales agents, dubbed "captives." But in the past two decades, the industry has evolved dramatically as insurers increasingly looked to outsource sales in order to reduce overhead.

As much as 70 per cent of all life insurance policies now sold in Canada are handled by independent brokers who are compensated primarily through commissions and perks. The agents often work through intermediaries known as managing general agents, which can contract several hundred brokers at one time, giving them more clout with the insurers. The vast majority of P&C sales also occur through brokers.

A good insurance broker in Canada can earn $100,000 annually, but it is not uncommon for take-home incomes to be significantly higher.

Insurance companies use three kinds of incentives to entice agents and brokers to direct business to them. There are upfront commissions when the sale is made; back-end commissions, usually called bonuses or "contingent" commissions, which are often based on the volume of business a broker does with that insurer; and perks.

The latter two are structured with one purpose in mind: to promote loyalty and encourage brokers to bring as many customers to that insurer as possible. The more the broker consolidates his clients' business with a particular insurer, the more lucrative the deal gets.

In life insurance, the upfront commissions have traditionally been high compared with other industries, because the product has always been a tough sell compared with other consumer purchases.

If a customer buys a universal life insurance policy that requires him to pay $1,000 in premiums the first year, the agent is likely to earn a commission of about $600 up front and a further $1,200 in a bonus at the end of the year, provided certain sales levels are met. That doesn't include incentives such as trips, nor commissions for keeping the policy in force in future years.

Brokers also can get paid extra for bringing in an insurer's favourite kind of customers - the kind who stay, or who don't make claims. For example, a broker who sells five group life insurance accounts for Standard Life paying total annual premiums of $3-million could earn a bonus of $30,000 if none of the clients take their business elsewhere. P&C insurers sometimes offer bonus payments for signing policies with "good customers" who file fewer claims.

The principle that a broker's first responsibility is to the client is contained in industry codes of conduct.

Don Bailey, who stepped down last month as the head of Canadian operations for Willis Group, one of North America's largest insurance brokers for corporate and business clients, says the industry and regulators need to tackle the transparency problem.

"What you see is agencies and brokers knowing what their targets are, and knowing that if I can shift this much premium volume to another carrier before the end of the

quarter, then I can trigger a cheque," Mr. Bailey said. "These [sums]are not incidental. They are significant amounts of money.

"If I'm the buyer, that should put in doubt why somebody is recommending one carrier over another. Is it because they truly believe that carrier is better? Or is it because they have a big cheque coming?"

'White sandy beaches'

Free trips are used by the insurance companies to tell brokers about their products, but they are also tools for instilling loyalty, ensuring that brokers are not tempted to direct business to rival firms, especially in the life insurance industry. The insurance companies detailed this strategy to The Globe and Mail.

Like consumers who sign up for loyalty programs or use premium credit cards, life agents accumulate points as they sell policies for a particular firm.

"I know some agents who say, 'Okay, I'm going to do business with [another] company this year because they've got this convention somewhere, or it's too difficult to meet your criteria to go to your convention,'" said Bruno Michaud, senior vice-president of administration and sales at Industrial Alliance. "At the end of the day, we see a convention for advisers as an award for the advisers for doing business with us. And it's a good occasion to develop a stronger sense of belonging to the company."

In the standard disclosure letter given to consumers at the time of purchasing a life insurance policy, there is a line stating: "From time to time, some companies may offer other types of compensation such as travel incentives or education opportunities."

But well out of the consumer's sight, internal industry documents obtained by The Globe and Mail detailing these perks are fashioned conspicuously like vacation brochures for luxury golf outings, cruises and sightseeing trips. Industrial Alliance's pamphlet shows photographs of crashing waves and exotic flowers, and invites brokers to "enjoy sunny skies while relaxing on sweeping white sandy beaches... Soak up the rays in a world-class resort." RBC Insurance's 'California Dreamin' conference was held at a resort near San Diego.

Two of Canada's biggest life insurers found out the hard way that perks distort the market. Senior executives at both firms told The Globe and Mail they raised the price of a universal life policy, only to watch sales of their other products - including the ones whose prices hadn't changed - take a hit. The price increase made the product harder to sell. Brokers told one of the companies that the price change meant it just wasn't worth their time to stay up to date on the insurer's other products.

The competitive pressure to provide incentives comes at a time when more Canadians need impartial advice on their insurance options. For example, Ontario has just decreased the amount of medical benefit coverage that insurers must offer drivers, but consumers can now choose to buy additional coverage. That leaves drivers in the province having to make important decisions on their policies this year. When it comes to life insurance, competition for the coveted baby boomer market has

prompted life companies to release a wider array of products, adding more complexity to an industry that is already difficult for many consumers to navigate without the help of an expert.

Yet the brokers have convinced regulators that the inability of Canadian consumers to grasp complicated financial matters is exactly why they shouldn't have to provide detailed disclosure of compensation, according to discussions with insurers, regulators and brokers.

Brokers push back

Critiques of the current compensation system are seldom heard. Consumers Association of Canada says that, owing to limited resources, it is not looking into the matter. The issue is invisible in the political arena.

Proponents of the industry's compensation structure nevertheless say criticism of perks and commissions is overblown. In their view, contrary to what the public might believe, a broker's main job is to prod people to buy life insurance and to plan for their financial futures - not to shop around. "If they spend all their time trying to find the absolute lowest price, chances are they're not spending their time on what they're truly being paid to do," says the top executive at one insurer. "Which is help bring the person to action on something they wouldn't have done on their own."

Mr. Schaafsma of the City of Surrey and his fellow risk managers are a rare voice of dissent. He says that upfront commissions are acceptable, if they are disclosed. However, the hidden perks and back-end commissions are a problem.

"You get a trip to Hawaii - that's a benefit that isn't going to the consumer, it has to flow into the price," he says.

Earlier this year, his professional association, the Risk and Insurance Management Society, issued a paper calling for better disclosure.

The paper, however, has had no tangible impact on igniting a debate that insurance brokers would prefer to avoid - and one that they skillfully extinguished earlier this decade.

The Canadian Council of Insurance Regulators, the umbrella group for provincial regulators, began to probe how insurance is sold in late 2004. The move came after a crackdown was announced in the United States to deal with allegations that a small number of U.S. brokers had rigged the sale of P&C policies to boost their commissions.

The committee found that while some brokers may argue that bonuses and perks do not influence their advice to clients, they may "appear ... to result in a potential conflict of interest."

The committee made three proposals. It recommended new legislation or regulation to clarify that the client's interest was to be placed first. It proposed to limit "performance-linked benefits" to insurance brokers, including contingent commissions that are hidden from the consumer. Finally, the

committee said there should be greater disclosure of ownership and other financial ties between a broker and an insurer, including the common practice of insurers lending money to brokers to expand their businesses.

The ensuing backlash revealed a broker community unequivocally opposed to these ideas. One of many groups to argue against the changes was the Insurance Brokers Association of B.C. Citing a lack of consumer complaints on the matter, the group implied there was no difference between selling insurance policies and furniture or cars. "Name any industry and you'll find mechanisms in place for motivating the sales force," the association wrote in its response to the committee.

Advocis, the Financial Advisors Association of Canada, warned that new restrictions would bind the industry in red tape.

If brokers had to explain complex commissions, such as contingent payments, it would be unduly confusing for the consumer, the group warned. And altering the overall incentive structure could disrupt the workings of a multibillion-dollar industry.

The pushback from the broker community worked. By the time of its final report in 2008, the committee's three key recommendations had been watered down. It no longer backed the idea that "clients first" should be enshrined in regulations, or that limits should be placed on commissions or perks. But the industry would have to start disclosing to the consumer any possible conflicts of interest.

Advocis endorsed the proposals, saying the industry was in fact already adhering to them. And on Dec. 8, 2008, the council of insurance regulators declared the debate over, and thanked the committee for "a job well done."

Brokers are expected to make customers aware of actual or perceived conflicts of interest, but this disclosure takes many forms.

"As you likely already know, agents and brokers in the life insurance business in Canada are compensated by commissions, bonuses and other inducements from the companies we do business with," says a letter that one broker group makes available to clients. Customers are asked to sign the letter, which describes "incentive-based compensation" as an "industry-wide practice," but makes no mention of specific figures.

This is enough disclosure, says Greg Pollock, the head of Advocis. "For the most part, we believe that the current structure of compensation in this country works well."

When it comes to auto and home insurance, the Insurance Brokers Association of Canada, which speaks for 33,000 property and casualty brokers, said its code of conduct requires brokers to disclose compensation - if a consumer asks. "The broker is required to divulge the method by which he is being compensated," said Steve Masnyk, a spokesman for the Insurance Brokers Association of Canada.

For instance, the broker might disclose that he or she will be paid a commission of between 10 and 15 per cent of premiums. Insurers also make general disclosure statements about compensation, usually on their websites, but details are limited.

The Registered Insurance Brokers of Ontario, the self-regulatory body for property and casualty brokers in Canada's largest province, also requires members to hand out a disclosure form that discusses compensation without divulging numbers.

But RIBO still uncovers cases in which agents do not have copies of the disclosure statement they are supposed to provide, through audits it conducts every three to five years. Tim Goff, manager of complaints and investigations at RIBO, says there is "95 to 99 per cent" compliance among brokers on this form.

The Insurance Council of British Columbia, meanwhile, has encountered cases where a broker has told a consumer incorrect information after the consumer asked for details of their compensation.

Mr. Bailey, the former head of an insurance broker, suggests the current system is not enough.

"[Brokers]should declare to the buyer: 'Just so you know, I represent the insurance company and not you. And I'm making significantly more money than you think I am,' " Mr. Bailey said. "Just disclosing the conflicts, in our mind, does nothing."

The 2008 detente with regulators signalled the campaign to head off reform succeeded. The industry diluted the suggested fixes down to a small number of voluntary measures.

"If you look at the system, the compensation, the way it all works, you'd be protecting it too," said a senior executive at a major insurer. "You don't want people asking questions, you don't want to disclose it, you don't want them to know you're going on a trip - because it's pretty good."

NATHANSONCENTRE
for the STUDY *of*
ORGANIZED CRIME AND CORRUPTION

Money Laundering in Canada: An Analysis of RCMP Cases

Stephen Schneider

10 INSURANCE

Of the 149 proceeds of crime cases examined for this study, the insurance industry was implicated in 96 (64.4%). However, an important caveat should be applied to this statistic and, by extension, the use of the insurance industry to launder the proceeds of crime. Unlike those sectors of the economy that predominate as money laundering vehicles – such as deposit institutions or real estate – in most of the police cases, the insurance sector was not expressly sought out by criminals to launder their illicit revenues. Instead, insurance policies were purchased because big ticket items that require coverage – such as cars, homes, marine vessels, and businesses – were acquired (with the proceeds of crime). As such, in most cases, the insurance sector was somewhat tangential to the actual money laundering objectives and processes.

However, the police cases also show that traditional services offered by the insurance industry – such life insurance policies – have also been used expressly to launder the proceeds of crime. According to a 1998 report entitled *Money Laundering Typologies,* the Financial Action Task Force (FATF) describes how single premium insurance bonds are purchased from insurance companies and then redeemed prior to their full term at a discount. The balance of the bond is paid to the launderer in the form of a "sanitized" cheque from the insurance company, thereby creating a seemingly legitimate source for the funds.

A Manitoba drug trafficker purchased a life insurance policy with a value of $78,000. The policy was purchased through an agent of a large Canadian life insurance company using a cashier's cheque. The client made it known that the funds used to finance the policy were the proceeds of drug trafficking. Knowing this, the agent charged a higher commission. Three months following this transaction, the drug dealer cashed in his policy for its full value.

In 1997, John Huffam was arrested for cocaine trafficking (for which he was later convicted) and a proceeds of crime investigation was undertaken. During a search of his home, police seized monthly statements issued by a life insurance company pertaining to a life insurance policy registered in the name of Huffam. Police also uncovered monthly statements from another major insurance company pertaining to another life insurance policy, also registered in his name. Police found that he had been contributing to this life insurance policy since 1980, and by 1995, it had a cash value of $80,042.04.

In a smaller number of cases, the insurance sector was used much like a bank: cash is deposited into accounts or term deposits; investments – such as RRSPs and mutual funds – are purchased; and mortgage financing is received. As the barriers that separate the different financial sectors continue to tumble in Canada, insurance companies are increasingly providing the type of banking services favoured by money launderers.

A $70,000 mortgage was obtained from a major Canadian life insurance company to finance a home for a multi-kilo drug trafficker. In the course of their investigation, police also found that the drug trafficker had almost $115,000 invested in short term investments through the same company. The investments were facilitated by a co-conspirator working within the insurance company who siphoned the funds through another unwitting account to avoid suspicion.

In 1995, an insurance broker in Alberta accepted large amounts of cash from known criminals, which were then invested under his own name. He would issue his clients a life insurance policy document, which could be redeemed whenever they wanted, for a fee. In one instance, the broker took $30,000 in ($100 bills) that were purportedly generated from local cocaine sales. The insurance broker then filled out a "Whole Life Policy" with a specified cash surrender value of $25,000 plus interest. The broker stated that he could put the policy in any name and would even hide its existence if need be. He then offered to funnel the cash through the bank account of another company he operated so as not to attract suspicion.

The New York Times

December 6, 2002

New Hiding Place For Drug Profits: Insurance Policies

By ERIC LICHTBLAU

WASHINGTON, Dec. 5— Law enforcement officials said today that Colombian cocaine traffickers seeking to launder tens of millions in drug profits from the United States and Mexico had begun exploiting an unlikely haven -- life insurance policies.

Officials at the Treasury Department said they were so worried about the trend that they were pushing for tougher regulation of the insurance industry as a way of identifying suspicious insurance policies.

A central concern for the authorities is that terrorist financiers, too, may seek to exploit vulnerabilities in the insurance industry to launder money for their operations.

A federal grand jury indictment brought today in Miami highlighted the phenomenon. In it, the authorities charged that five Colombians took part in an elaborate scheme to launder millions in cocaine profits originating from street sales in New York City, Florida and elsewhere.

American law enforcement officials say Colombia has indicated that it will extradite the five suspects to the United States to stand trial.

Drug traffickers often use bank deposits, wire transfers and other financial mechanisms to disguise the source of their revenues. But officials at the Customs Service said the current case was the first in which a major trafficking ring has been known to use insurance policies to cover its financial tracks.

In interviews and court documents, law enforcement officials at the Customs Service said that in recent years, brokers connected to the Cali drug cartel in Colombia had bought insurance policies in the Isle of Man and other British islands, as well as perhaps Florida and other locations, to launder more than $80 million.

Using drug proceeds from the United States and Mexico, the suspects opened some 250 different investment-grade life insurance accounts in the Isle of Man alone, investigators said. The insurance policies, worth as much as $1.9 million each, were sometimes taken out in the names of nieces, nephews and other relatives of the traffickers, investigators said.

The traffickers would typically cash out all or part of the Isle of Man policies prematurely after a year or so, paying penalties of 25 percent or more to get access to the laundered cash more quickly, investigators said.

Customs Service officials have seized $9.5 million in Florida in connection with the case, most of it in the last three weeks, officials said. They expect to seize more assets and bring more charges against others they accuse of involvement in the operation, and they are closely scrutinizing a South Florida insurance company to determine its role.

"This has opened our eyes," said John Clark, special agent in charge of the Customs Service's Miami office, which led the investigation. "We think this is just the tip the iceberg. This is a system that seems to have been used and abused by narcotics traffickers for years."

Officials in Colombia have also seized $20 million there and in Panama in connection with the money-laundering operation. They arrested at least nine people in the case last month -- including three of the five defendants charged today in Miami. Another Colombian wanted in the case is thought to be at large in California.

Those indicted today in Miami on conspiracy and money-laundering charges were Rodrigo José Murillo and his son, Alexander Murillo, who investigators say were active on the drug-trafficking side of the operation; Jaime Eduardo Rey Albornoz and Arturo Delgado, who investigators say brokered the transactions; and their assistant, Esperanza Romero.

The indictment seeks the forfeiture of $2.1 million that the authorities say the defendants laundered through banks and insurance companies.

The case was brought in Florida because some of the money passed through companies in the state and because the laundering investigation grew out of a major drug-trafficking case there in the early 1990's.

The case led to the seizure of 47,000 kilograms of cocaine distributed by the Cali cartel and others. In the last several years it has also led investigators to develop high-level informers in the trafficking industry. These sources indicated that much of the cartel's money was winding its way to the Isle of Man, investigators said.

The Customs Service started the financial spinoff of its 1990's case in early 2001, working closely with counterparts in Colombia, Panama, Britain and the Isle of Man.

Officials in the Isle of Man, a hub for global insurance companies, were eager to cooperate, American officials said. After concerns were raised in recent years about whether the island's oversight of the industry was too lax, the officials "wanted to put that to rest by cooperating and to show that they weren't a money-laundering haven," said Anthony Arico, assistant special agent in charge in Miami for the Customs Service.

Isle of Man officials said today that they had instituted new safeguards against criminal use of their corporations to launder money. But they acknowledged that the high volume of global business in the territory made it an attractive target for launderers.

In the current case, investigators pulled together information from financial transactions as far away as Russia, using informants, wiretaps and undercover operations to trace the money trail, officials said.

In New York City, undercover Customs investigators acted as go-betweens, funneling cash from local street sales and forwarding it to the Isle of Man through checks or wire transfers to buy life insurance policies, officials said.

Undercover agents also got the word out to drug dealers that, for a fee, they would accept and launder large amounts of cash, according to a seizure warrant filed in federal court in New York in connection with the case.

Dealers would then drop off large sums of cash -- sometimes hundreds of thousands of dollars -- and direct the undercover agents to wire the money to banks and insurance companies around the world, the warrant said.

American officials said that Mr. Albornoz and Mr. Delgado, who each own financial transaction businesses in Colombia, were the "master brokers" who oversaw the insurance scheme. Colombian officials said Mr. Albornoz even organized conferences on money laundering for insurance companies and financial institutions around the world.

"The case just underscores the clever and crafty schemes that drug traffickers and terrorists, too, are capable of conceiving to move their money," said Rob Nichols, a spokesman for the Treasury Department.

The department proposed in September that insurance companies be required to adopt programs to better detect accounts opened expressly to hide illegal revenues.

Officials said the investigation in Colombia was a driving force in the still pending proposals, which have met with general support from many insurance groups.

Mr. Clark of the Customs Service said that if insurance companies were subject to the same types of rigorous reporting and monitoring requirements as banks, the authorities would have been able to detect some of the suspicious tactics used by the Colombian launderers.

Insurance companies might have reported, for instance, that policyholders were authorizing unrelated third parties to withdraw money from their accounts or were frequently cashing out their policies early, he said.

The proposed restrictions, he said, would help the authorities "spot the type of irregular flow of money that we were seeing here."

Chart: "INVESTIGATION -- Laundering Drug Profits" In recent years, Colombian cocaine traffickers have laundered as much as $80 million in drug money through life insurance policies in the British Isles and other places, American law enforcement officials said. Here are some ways the traffickers sent money through the Isle of Man, according to the Customs Service: NEW YORK Undercover Customs Service agents wire cash to the insurance policy on the Isle of Man. MEXICO Third parties wire payments to the Isle of Man through a Mexican money exchange house. LONDON British authorities working undercover transfer money to the Isle of Man policy. FLORIDA Money is transferred to the policy from an insurance broker's commission account. COLOMBIA The Isle of Man insurance policy is cashed in early and deposited into the drug traffickers' shell company. (pg. A12)

---

infomart

The Gazette

Insurance agents ordered to repay $3.7 million gained by fraud

montrealgazette.com
Thu Mar 20 2014
Section: OnLine
Byline: Paul Delean

MONTREAL - Two Sherbrooke insurance agents will have to repay more than $3 million they received from Canada Life Assurance after a Superior Court judge ruled they defrauded the company with an elaborate scheme to collect commissions.

The judgment against Stéphane Corbeil, Ian Roy and GCS Firme Conseil Inc., a company owned by Corbeil, was rendered by Judge Martin Bureau.

Court was told that between 2006 and 2011, the two men sold 160 universal **life-insurance** policies to individuals and businesses, generating commission and bonuses totalling about $3.7 million.

Canada Life alleged they'd put in place a fraudulent scheme by selling to "simulated" clients, to whom they promised free **life insurance** for 24 to 30 months. Many of the clients were acquaintances of the defendants and members of their family, the company said.

The defendants would advance them money for an initial payment, pocketing the difference between the payment and commission generated. Then the payments would stop, letting the policy lapse.

In an example cited as evidence, the initial payment for the policy was $13,900 and the commission it generated for them $23,325.

Court was told that in some cases, the same client would reapply after the original policy died, generating another commission.

Canada Life said the intention of the men was not to offer the **life-insurance** product to their clients, but only to serve their own interests.

The defendants maintained the company brought this on itself with a faulty commission schedule, but Judge Bureau disagreed.

He said they had no credibility, clearly violated the ethics of the profession by reimbursing client premiums, and the scheme was exactly as the company described it.

"Clients, for whom the strategy cost nothing, got the benefit of significant insurance coverage for a period, without ever having any real intention to maintain or conserve this protection beyond the time allowed by the payment made for them by the defendants," Judge Bureau said, noting that in one case, the insurance policy actually produced a $900,000 payout for the family of an applicant who died while covered.

To be legitimately entitled to commissions and bonuses, the agents had to act in good faith and respect their obligations toward the company and clients, he said.

"It would be illogical," Judge Bureau wrote, "to consider that the defendants, in light of their fraudulent actions, had the right to any remuneration whatsoever from the plaintiff."

He ordered them to repay the full $3.7 million in commissions and bonuses received from the company, plus interest.

Property in Sherbrooke seized pending judgment will serve to acquit the sum.

pdelean@montrealgazette.com(mailto:pdelean@montrealgazette.com)

infomart

thestar.com

Man charged for defrauding client out of $21,000

thestar.com
Thu Nov 28 2013
Section: News | Toronto Star
Byline: Paul Clarke(https://author.thestar.com/content/thestar/authors.clarke_paul.html)

A Richmond Hill man who posed as an insurance agent and defrauded a client out of thousands of dollars was arrested by Toronto Police on Thursday.

The man allegedly convinced his victim to cash out his **life-insurance** policy worth $21,000 in return for a new policy that would better suit his client's financial needs. The man took off with the money and never purchased the new policy for his client.

Laurence Honickman, 41, has been charged with **fraud** over $5,000, laundering proceeds of crime and failure to comply with probation.

Police believe there may be more victims.

Anyone with information is asked to contact police at 416-808-1300 or Crime Stoppers at 416-222-TIPS (8477).

Illustration:
• Laurence Honickman was arrested by police who say he posed as an insurance agent and defrauded a client out of $21,000.

Length: 111 words
Idnumber: 201311280116

Tone: Negative

Tone: Neutral
Ad Value: $708 Circulation: 58,839

THE CANADIAN PRESS

Former Texas businessman sentenced to 60 years for his role in $100M insurance fraud

Canadian Press
Wed Sep 28 2011
Section: Foreign general news
Byline: BY LARRY O'DELL

RICHMOND, Va. _ After hearing tearful testimony from several people whose life savings were stolen, a federal judge sentenced a former Texas businessman to 60 years in prison Wednesday for his role in a $100 million **life insurance** scam that claimed more than 800 victims in three dozen U.S. states and Canada.

A Richmond jury in June convicted Adley Abdulwahab on 15 counts of conspiracy, wire fraud, securities fraud and **money laundering**.

Abdulwahab, 36, was one of the principals of companies called A&O that used investor funds to buy **life insurance** policies from individuals at less than face value. Investors were supposed to be paid when the insured died, but A&O's partners spent the money on lavish lifestyles instead of safeguarding the investments and paying premiums. Policies lapsed, and investors lost their money.

``They were people who built their dreams by hard work _ real hard work _ and those dreams have been stripped from every one of these investors," U.S. District Judge Robert E. Payne said.

Given a chance to address the court before sentencing, Abdulwahab suggested the value of insurance policies was incorrectly calculated, said prosecutors had declined to meet with him during the investigation, and blamed a co-defendant for encouraging him to join A&O.

Among the victims was Paula Higdon Whitaker of Magnolia, Texas, whose life savings of $1 million helped finance mansions, fancy cars, expensive jewelry, resort vacations and other luxuries for A&O's leaders. Whitaker, a teacher and counsellor, said she worked as many as three full-time jobs at a time over 40 years of frugal living to build a nest egg to help her only son, who had medical problems.

``I earned money the old-fashioned way _ I worked for it," a weeping Whitaker testified. ``That's why this is such a horrendous and difficult thing for me."

After her son Ryan died, she planned to use the A&O investment to fund a charitable foundation in his memory. Then she learned that A&O was a scam, and all her money was gone.

``It's been four years, seven months and 28 days since I lost my son and I cry every day because I can't leave the legacy for him that I wanted," she said. ``It was like taking Ryan away from me again."

Other victims talked about the embarrassment of losing their life savings to a fraud and the anguish of seeing a lifelong goal of a comfortable retirement vanish.

U.S. Attorney Neil MacBride, who attended the sentencing, also said 60 years was a fair sentence.

``A case like this really puts a human face on financial crimes," he said. ``These defendants stole life savings and retirement funds from hundreds of people who worked hard and played by the rules."

He noted that some of the investors worked their entire lives to save $50,000, while A&O's officers often rang up that much in credit card purchases in a month.

Abdulwahab was sentenced a day after Payne sentenced A&O co-founder Christian Allmendinger of Houston to 45

years for his role in the scheme. Five other conspirators, including A&O co-founder Brent Oncale of Houston, previously pleaded guilty and received lighter sentences.

A federal financial crimes task force in Virginia co-ordinated the investigaton. Several victims are from Virginia, and an A&O sales agent who pleaded guilty is from Richmond.

Length: 555 w ords
Idnumber: 201109280407

Tone: Negative

Ex-NFL lineman charged in scheme

Updated Aug 2, 2013 11:19 AM ET

FoxSports.com

SAN DIEGO (AP)

A former NFL defensive lineman is among four people charged in San Diego with participating in a $50 million insurance fraud scheme.

The 2013 offseason was a rough one for NFL players and the law. Take a look back at the players arrested before camp ever opened.

U-T San Diego reports 36-year-old Byron Frisch was charged along with three others with conspiracy to commit mail and wire fraud.

Frisch and others are accused of submitting false information to obtain more than $50 million worth of life insurance policies for unqualified applicants who didn't plan to pay the policy premiums. Authorities say they received more than $1.6 million and the ability to sell the policies to investors.

The four allegedly recruited elderly individuals to apply for purported free life insurance policies with million-dollar death benefits, then submitted applications with false details.

Frisch, a self-employed financial adviser, played for the Dallas Cowboys and the New York Giants.

The Canberra Times
INDEPENDENT. ALWAYS.

Accused controls tax haven companies

Ben Butler

680 words
21 October 2013
Canberra Times
CANBTZ
B009
English

Accused controls tax haven companies

Ben Butler

Formerly secret Cayman Islands documents reveal that Sydney businessman Vanda Gould, who was charged last week with serious tax and **money laundering** offences, controls two companies in the Caribbean tax haven. The documents are evidence in a civil case in which overseas companies allegedly associated with Mr Gould and his co-accused, John Leaver and Peter Borgas, are attempting to claw back tax bills totalling about $40million. Mr Gould is the chairman of listed investment company CVC and Mr Leaver, a former director of Gold Coast developer Sunland, is also on the board. In the Federal Court case, the Tax Office alleges the offshore network brought $19.45million back into Australia, much of which went to Mr Gould and Mr Leaver. It alleges $3.4million of tax haven money went towards the purchase of four apartments by a company associated with Mr Gould and Mr Leaver, while an additional $1.9million helped fund the purchase of a property in Woollahra by Mr Leaver's daughter.

Messrs Gould, Leaver and Borgas were arrested last week and charged with conspiracy to dishonestly cause a loss to the Commonwealth and conspiracy to use $30million as an instrument of crime - offences that carry jail terms of 10 years and 25 years respectively. They have been released from custody after lodging bail money totalling $12million. Mr Gould is not registered as a director or shareholder of either Cayman Islands company, MH Investments and JA Investments. However, the court documents show he signed nominee agreements on August 31, 2005, describing him as the "appointer" of both companies. The word "appointer" has been handwritten into the documents, replacing the printed word "beneficiary". In both agreements, nominees appointed by Mr Gould declare they hold the shares on his behalf and promise to vote as directed by him "to enable the appointer to exercise all of the rights and privileges as a shareholder of the company". The nominees also promise to act as company directors and "vote as directed by the appointer

at all times when acting as a director of the company". Mr Borgas, a Belgian citizen who lives in Switzerland, is the sole director and sole shareholder of each company, and his wife Winny serves as assistant secretary. In the Federal Court case, which continues despite the arrests, several offshore companies are challenging the Tax Office's contention they are Australian residents and should pay local tax on profits from share trading. The offshore arrangements, described as "Byzantine in their complexity" by Justice Nye Perram, take in a dizzying array of companies and professionals in tax havens including Vanuatu, Singapore and the British Virgin Islands. Chemical Trustees, Derrin Brothers Properties and Bywater Investments, of the Bahamas, have told the court they are controlled by Mr Borgas from his base in Switzerland. Southgate Investment Funds claims to be controlled from London, while Hua Wang Bank Berhad, of Western Samoa, claims to be managed from the Samoan capital, Apia. The Tax Office alleges JA Investments and MH Investments own the network of

companies and Mr Gould controls all of them except Southgate, which it alleges is controlled by retired Sydney anaesthetist Joseph David Ross. It alleges Messrs Gould, Leaver and Ross funded the offshore network by buying **life insurance** policies from Fidelity Pacific **Life Insurance** Company, which operates from tax haven Vanuatu and claims on its website that although "death is inevitable taxation does not have to be". The Tax Office alleges that among the companies paying premiums was Planette Thoroughbred Trading - a company owned by Mr Gould and Mr Leaver that ran racehorses with radio shock jock Alan Jones and Racing NSW chairman John Messara. It also alleges that on the instructions of Mr Gould, Fidelity deposited funds with the Bank of Commerce (Micronesia) in Vanuatu, which then loaned it on to companies in the offshore network. Profits from share trading were then allegedly repatriated as loans, which were used to buy property and fund companies controlled by Mr Gould and Mr Leaver.

Associated Press

Los Angeles man gets 13 years in federal prison in Texas life settlement insurance fraud case

152 words
19 December 2013
07:13
Associated Press Newswires
APRS
English

HOUSTON (AP) - A Los Angeles man has been sentenced to 13 years in prison in a nearly $10 million Texas-based life settlement insurance scam.

A federal judge in Houston on Wednesday sentenced Charles Craig Jordan, who pleaded guilty to conspiracy to commit mail and wire fraud. Jordan was also ordered to pay almost $9.7 million in restitution to more than 500 victims.

Prosecutors say the scheme involved a Houston company called Secure Investment Services and American Settlement Associates. A co-defendant, Kelly Taylor Gipson of Rockwall, awaits sentencing after pleading guilty to conspiracy to **launder** proceeds from the fraud.

A life settlement is when people who are typically elderly or terminally ill sell their **life insurance** policies for a cash payment. Investigators say Jordan and Gipson misused investor money and the policies lapsed.

Former Employee of National Prearranged Services Inc. and Lincoln Memorial Life Insurance Company Brent Cassity Pleads Guilty to Fraud and Money Laundering Charges

565 words
3 July 2013
Department of Justice Documents
DOJDOC
English

Justice Department FBI Press Releases

Former Employee of National Prearranged Services Inc. and Lincoln Memorial **Life Insurance** Company Brent Cassity Pleads Guilty to Fraud and **Money Laundering** Charges

U.S. Attorney's Office July 3, 2013

Eastern District of Missouri

ST. LOUIS, MO–Brent Douglas Cassity pled guilty today before United States District Judge Jean C. Hamilton to participating in a fraudulent scheme involving the sale of prearranged funeral contracts and monetary transactions involving the proceeds of that scheme. Cassity, 46, faces up to five years in prison for his role.

In court, Cassity admitted that beginning as early as 1992 and continuing until 2008, National Prearranged Services, Inc. (NPS) sold prearranged funeral contracts in several states, including Tennessee and Ohio. During that time, insurance companies affiliated with NPS issued **life insurance** policies related to those prearranged funeral contacts. As part of the contracts, the total price for funeral services and merchandise for an individual was agreed upon, and that price would remain constant regardless of when the funeral services and merchandise would be needed. Customers entering into prearranged funeral contracts would usually pay a single sum of money up-front to NPS either directly or through a funeral home that was also a party to the contract. NPS represented to individual customers, funeral homes, and state regulators that funds paid by customers under the prearranged funeral contracts would be kept in a secure trust or insurance policy as required under state law. Cassity admitted, however, that NPS made use of funds paid by customers in ways that were inconsistent both with its prior and continuing representations and with the applicable state laws and regulations.

Cassity was employed at various times by NPS and also served as a director of Lincoln Memorial **Life Insurance** Company, for which NPS served as general agent. Cassity also held numerous titles with affiliated companies, including chief executive officer, chairman, president, and director of Forever Enterprises Inc.; and president and director of National Heritage Enterprises.

Cassity pled guilty to one count of mail fraud (count 31), one count of wire fraud (count 21), and one count of **money laundering** (count 38). Cassity also pled guilty to willfully permitting James Douglas Cassity, whom he knew to have been convicted of a felony involving fraud or dishonesty, to exercise significant control over NPS's affiliated insurance companies (count 50)

Cassity will be sentenced on November 7, 2013, at 9 a.m. Earlier this month, Cassity's co-defendant and fellow NPS executive Sharon Nekol Province pled guilty to six counts of mail fraud, wire fraud, and misappropriation of insurance premiums arising out of the same scheme. Cassity's co-defendants, James Douglas Cassity, Randall K. Sutton, Howard A. Wittner, and David R. Wulf have entered pleas of not guilty and are scheduled to

appear for trial starting on August 5, 2013. As is always the case, charges do not constitute proof of guilt, and every defendant is presumed to be innocent unless and until proven guilty.

Cassity's case was investigated by Internal Revenue Service-Criminal Investigation, the Federal Bureau of Investigation, and the Postal Inspection Service. Assistant United States Attorneys Steven Muchnick, Charles Birmingham, and Richard Finneran are handling the case for the U.S. Attorney's Office.

Seven Charged in Life Insurance Fraud Scheme

766 words
25 July 2012
Department of Justice Documents
DOJDOC
English

Justice Department FBI Press Releases

Seven Charged in **Life Insurance** Fraud Scheme

U.S. Attorney's Office July 25, 2012

Middle District of Louisiana (225) 389-0443

BATON ROUGE, LA--United States Attorney Donald J. Cazayoux, Jr. announced today that seven area residents have been charged for their role in a **life insurance** fraud scheme. The U.S. Attorney has charged Timothy R. Schlatre, 34, of Denham Springs, with mail fraud, **money laundering**, and asset forfeiture. Schlatre faces a maximum sentence of 30 years in prison and fines of up to $500,000 or twice the gross gain or loss from the offense, whichever is larger.

The U.S. Attorney has also charged Jason Paul Austin, 32, of Walker; Jodi Marie Austin, 34, of Walker; Ricky J. Austin, 49, of Denham Springs; Jimmy O. Cassels, 33, of Denham Springs; Todd D. Cummings, 34, of Walker; and Dena A. Gaudet, 33, of Denham Springs, each with conspiracy to commit mail fraud. These individuals each face a maximum sentence of five years in prison and a fine of up to $250,000.

The bills of information allege that Schlatre, using his position as a **life insurance** agent for New York Life and Lincoln Financial, devised a scheme to defraud New York Life and Lincoln Financial in order to fraudulently receive commission payments by selling **life insurance** policies based on false statements and representations. Specifically, Schlatre submitted false information to the companies regarding the applicant's net worth and annual income, thereby defrauding New York Life and Lincoln Financial into approving the policies and issuing the commission payments to Schlatre to which he was not entitled. Because the policy values were so large, the applicants could not afford to make the premium payments. In order to effectuate his scheme, Schlatre further agreed to provide the premium payments on behalf of the applicants. This process, known as "rebating," was prohibited by both company's policies as well as state law. In order to conceal that he was the source of the premiums, Schlatre deposited money directly into the individual applicant's bank account. Schlatre further misrepresented the source of the premium payments by falsely declaring that he was not paying or allowing the rebating of any premiums.

The bills of information further allege that Jason Austin, Jodi Austin, Ricky Austin, Jimmy Cassels, Todd Cummings, and Dena Gaudet each conspired with Schlatre to obtain **life insurance** policies by making false statements regarding their net worth and annual income. All are alleged to have provided false information in their written applications as well as in subsequent phone interviews as part of the underwriting process.

The bills of information allege that Schlatre defrauded New York Life and Lincoln Financial into issuing **life insurance** policies in excess of $100 million dollars. This resulted in the receipt of commissions to which he was not entitled in excess of hundreds of thousands of dollars.

United States Attorney Donald J. Cazayoux, Jr. stated, "This ongoing investigation is another example of how

close cooperation between our federal and state partners results in the effective investigation and prosecution of significant fraudulent schemes. We will continue to pursue all who seek personal benefit through deception."

"This investigation should be a clear reminder that federal law enforcement's reach into white-collar crime extends beyond traditional health care, investment, and corporate fraud to bring those responsible to justice," stated FBI Special Agent in Charge Michael J. Anderson.

"People who conspire to create elaborate insurance fraud schemes run a very high risk of prosecution," stated James C. Lee, Special Agent in Charge, IRS-Criminal Investigation. "IRS is committed to working diligently with the Department of Justice to dismantle these organizations."

Louisiana State Inspector General Stephen Street stated, "Mr. Schlatre and his cohorts engaged in a fraud scheme over a period of several years and will now be held accountable. This case is the latest example of success in OIG's ongoing partnership with the U.S. Attorney, FBI, and IRS in investigating corruption cases."

The investigation of this matter was conducted by the Federal Bureau of Investigation, the Internal Revenue Service-Criminal Investigation, and the Louisiana Office of Inspector General. The Louisiana Department of Insurance assisted in the investigation. The cases are being prosecuted by Assistant United States Attorney Rich Bourgeois who serves as Deputy Criminal Chief.

A bill of information is a determination by the U.S. Attorney that probable cause exists to believe that offenses have been committed by a defendant. The defendants are presumed innocent until and unless proven guilty at trial.

U.S. Department of Justice

THE TIMES OF INDIA

India Business

Insurance gateway for money laundering

Sidhartha

437 words
8 May 2013
The Times of India
TOI
English

NEW DELHI: Tinoo and Arvind Joshi, the suspended IAS couple from Madhya Pradesh, faced CBI raids soon after it was discovered that they had purchased **life insurance** policies from a private insurer. The high-value transaction could not have gone unnoticed.

But there are several thousand cases that go undetected. For long, **life insurance** policies have been seen as a passport to convert "black money" into "white". There are multiple ways that agents use for anyone willing to bring unaccounted cash into the financial system.

Insurance industry executives and agents said the easiest way to do it is to pass on the commission to the client. For instance, if you buy a policy for Rs 1 crore, the commission amount of, say, Rs 20 lakh is given to the agent who then passes it on to the policyholder, although sharing of commission is illegal and can lead to cancellation of the agent's permit.

In fact, that is one reason why relatives of businessmen, politicians and filmstars often become agents as the commission doesn't need to be transferred to the insured and yet remains within the family.

But can someone with Rs 1 crore cash buy a policy? "It's possible and agents are willing partners," said a prominent development officer of **Life Insurance** Corporation. The development officer, who manages a group of agents for the company, claimed that there were several instances where Rs 50,000 – the permissible level of cash deposits – was deposited in cash on a daily basis and often went undetected. After a few days, the company issues a policy and the entire amount then gets "white".

Insurance company executives said this operation was best suited for single-premium policies, or those where the entire premium was paid upfront. Therefore, the commission also comes in one go.

There is yet another common practice in the industry, which relates to lapsed policies and even managements are involved.

Typically, these operations are undertaken by dummy agents or financier-turned agent in what is commonly known as recycling in industry parlance. The agent, usually someone with loads of unaccounted cash, becomes an agent and gets a list of policies that are no longer operational as the premium has not been paid. The agent then approaches the policyholders and revives the policy by paying the pending installment. This entitles the agent to the commission and helps in converting the amount into white.

There are also allegations that micro insurance policies are the latest tool as several covers have been issued to "fake policyholders".

Frauds blow a hole in insurance firms

Mail Today Bureau | Mail Today | New Delhi, March 5, 2012 | UPDATED 10:48 IST

Indian insurance companies have collectively lost a whopping Rs.30,401 crore due to various frauds which have taken place in the life and general insurance segments during the year, according to a study. The losses work out to about nine per cent of the total estimated size of the insurance industry in 2011, the study carried out by Pune-based company Indiaforensic states said.

The total premium income of the insurance industry, comprising life, non-life and health, is around Rs.3.5 lakh crore, according to the figures by Insurance Regulatory and Development Authority (IRDA).

The company has identified collusion between employees of insurance companies and beneficiaries furnishing false documents, and manipulation in citing the cause of death as part of the modus operandi adopted by fraudsters to claim undue insurance benefits. Indiaforensic carries out regular studies in examining frauds, security, risk management and forensic accounting and claims to have assisted the Central Bureau of Investigation (CBI) in the multi-crore Satyam scam.

The life insurance segment accounted for as much as 86 per cent of the frauds while remaining 14 per cent took place in the general insurance sector, which includes false claims for cars, houses and accidents, the report showed. The study also highlighted that the frauds in the life insurance segment had more than doubled in the last five years while those related to general insurance sector increased by 70 per cent.

In 2007, insurance firms had lost as much as Rs.15,288 crore, of which life insurance accounted for `13,148 crore while the general insurance segment lost Rs.2,140 crore. The insurance sector is susceptible to various frauds in the country. There is an urgent need to have strict measures, including setting up of a dedicated unit to detect and check frauds in the companies, said anti-fraud and money laundering expert Mayur Joshi, who is a founder member of Indiaforensic. However, insurance experts

assert that while it is true that insurance companies are cheated, the quantum of losses is not as high as the study claims.

IRDA chairman J. Harinarayan brushed aside the study. He said the insurance firms are capable enough to protect their interests. However, he admitted that insurance companies were not reporting scams or other malpractices in the insurance industry. "It is just a sensational claim. I do not think so. Insurance companies have not reported to me about such frauds. Let me see the report first and what it says and how it claims that a `30,000-crore fraud was committed in 2012 in the insurance sector. Insurance companies are capable enough to protect their interest," Harinarayan told Mail Today on Sunday. LIFE Insurance Council secretary general S.B. Mathur said, "I think the figures of fraud as claimed are unrealistic. The fraud committed could be higher in non-life insurance compared to life insurance companies. However, the total figure for fraud cannot be as high as Rs.30,000 crore.

"I went through reports submitted by the respective insurance companies to their audit committees which are not open documents. But I have not come across such mind-boggling figures. It is next to impossible.

The internal laws are not so lax." The study said that clients were defrauding the insurance companies by not disclosing existing diseases. This was being done by manipulating the impanelled doctors while applying for the policy. False age certificates are also being submitted to become eligible for insurance. The forging of medical bills are the most common fraud that affect the health insurance sector. In as many as 31 per cent of the total falsified documentation, medical bills were the common target of the frauds by external parties.

Travel abroad for surgery without disclosing it, or getting a damaged vehicle insured without disclosing the accident are some of the common methods of cheating insurance companies, the report states as examples of frauds in the general insurance sector

BUSINESS

Irda fines Tata AIA for violating anti-money laundering norms

282 words
13 February 2014
Press Trust of India
PRTRIN
English

New Delhi, Feb 13 (PTI) Insurance sector regulator Irda has imposed a fine of Rs 1 lakh on Tata AIA **Life Insurance** Company for violating anti-**money laundering** (AML) norms and not putting in place effective system for cash transactions.

The Insurance Regulatory and Development Authority (Irda) in its order said that effective systems were not in place to report cash transactions and in various instances no review was carried out for reporting cash transactions.

It also observed that in certain instances, Tata AIA accepted multiple cash transactions exceeding Rs 50,000 on a single policy from same payer without PAN number.

"The violations referred ... are considered serious in nature. Therefore, in addition to the directions issued in the respective decisions, the Authority imposes a penalty of Rs 1,00,000," the order said.

Among others, Irda has dicected the insurer to strictly comply with AML guidelines as it was revealed that the company did not make KYC norms as a binding clause and asked to put in place fool proof systems to ensure compliance with the AML norms.

Irda also said that the life insurer in various instances accepted multiple DDs (demand draft) towards a single policy or multiple polices for same payer and no review was carried out.

"However, the Life Insurer is warned for the deviations noticed in the charge and advised to ensure compliance to the guidelines/circulars issued by the Authority in this regard."

Irda also said the company did not have effective systems to ensure authenticity of KYC (know your customer) documents and directed to be vigilant in complying with KYC norms. PTI KPM MR

THE TIMES OF INDIA

India Business

Staff at LIC, Birla Sunlife, Reliance Life others accused of 'helping' people avoid tax

479 words
8 May 2013
The Times of India
TOI
English

MUMBAI: That there is no limit on cash transaction while purchasing an insurance policy could be the biggest draw for those in possession of illicit money to seek insurance companies to convert their black money into accounted money. Also, the fact that long-term insurance policies are not taxed in most cases is the biggest attraction for generators of black money to buy insurance policies as the income-tax department does not open cases that are more than seven years old.

Staff at some insurance companies like state-run **Life Insurance** Corporation of India, Birla **Sunlife** Insurance, Reliance Life and Tata AIA **Life Insurance** are accused of 'helping' people avoid tax. They help them choose products that keep them below the income-tax radar. But even for insurance purchases above 50,000, PAN has to be produced. "First we will ask for observation from each of these companies on the matter and send our special team to investigate all transactions above a certain limit," said an official at the Insurance Regulatory and Development Authority who did not want to be identified.

In a second sting operation telecast in less than three months, cobrapost.com on Monday uploaded films where officials at these insurers and banks are seen suggesting ways to a prospective customer on how to overcome tax liabilities and circumvent tax obstacles. Most of the companies dismissed these saying no transaction actually took place.

"We categorically deny the baseless allegations in relation to any involvement of the company in **money-laundering** by customers of our **life insurance** business," said Reliance Capital spokesperson.

"As part of its ongoing compliance efforts, Reliance Life will continue to examine any specific instances that come to light for appropriate remedial action, if any."

KYC norms followed by insurance companies are similar to that of the banks. Individuals need to submit identity proof, residence proof and income proof and documents such as passport, PAN card, voter's card, driving licence, electricity bill, salary slips are required to process the policy.

The reason why bankers and insurance companies use **life insurance** policies to dupe the system is investment in longterm insurance products are exempted from tax. The maturity amount under investment in **life insurance** products like regular unit-linked plans and traditional money back plans are exempted from tax under the I-T Act. Also, investment in **life insurance** products, including Ulips, traditional and term, up to Rs 1 lakh under section 80C are exempted from tax.

Generally, insurance companies report suspicious transactions to Financial Intelligence Unit. For instance, if the premium paid is 50% of the annual income. Every company has a different policy for reporting suspicious transactions to FIU. The regulator mandates cash transaction above Rs 50,000 to be reported FIU.

Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities

NARRATIVE SUMMARIES OF REASONS FOR LISTING

QI.A.201.05. YASSER MOHAMED ISMAIL ABU SHAWEESH

Date on which the narrative summary became available on the Committee's website: 16.09.2009

Yasser Mohamed Ismail Abu Shaweesh was listed on **6 December 2005** pursuant to paragraphs 1 and 2 of resolution 1617 (2005) as being associated with Al-Qaida, Usama bin Laden or the Taliban for "participating in the financing, planning, facilitating, preparing or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf, or in support of" Al-Qaida (QE.A.4.01).

Additional information:

Yasser Mohamed Ismail Abu Shaweesh attempted to commit life insurance fraud by faking a fatal traffic accident in order to acquire funds to be sent to Al-Qaida (QE.A.4.01).

Yasser Abu Shaweesh's activities were conducted with the approval of Ibrahim Mohamad Khalil (QI.M.206.05). The life insurance benefits were to be paid out to the brother of Yasser Abu Shaweesh, Ismail Mohamed Ismail Abu Shaweesh (QI.A.224.06), as the designated beneficiary.

From at least the summer of 2004, Yasser Abu Shaweesh agreed to attempt to acquire fraudulently large sums of money from life insurance companies, intending to direct a great part of this money to Al-Qaida (QE.A.4.01) to fund its terrorist activities. In pursuit of this plan, Yasser Abu Shaweesh took out 9 life insurance policies totaling 1,264,092 Euros in benefits with a number of insurance companies. In cooperation with Khalil, Yasser Abu Shaweesh tried to take out 19 further insurance policies, which would have raised the total insured to 4,325,958 Euros. Yasser Abu Shaweesh was to fake a fatal traffic accident during his stay in Egypt. By obtaining a death certificate, if necessary through bribery, the life insurance benefits were to be paid out to Ismail Abu Shaweesh. Finally, the money was to be transferred abroad, and the individuals involved were to abscond. The major part of the money was to go to Al-Qaida. Khalil was primarily responsible for paying the insurance premiums.

Yasser Abu Shaweesh had contacts, particularly via Khalil, to the international network of Al-Qaida. Before the terrorist attacks in the United States on 11 September 2001 as well as from 11 October 2001 until 12 September 2002, Khalil spent time in Al-Qaida training camps in Afghanistan. There, he was in contact with the leading cadres of Al-Qaida - also after the attacks in the United States on 11 September 2001 - who gave him instructions, and he himself took command of a group which belonged to Al-Qaida during the war in Afghanistan. Yasser Abu Shaweesh knew that Khalil supported Al-Qaida and assisted him in doing so.

Yasser Abu Shaweesh was convicted in Germany in 2007 of supporting a foreign terrorist organization and on multiple counts of fraud and attempted fraud, and was sentenced to five years and six months of imprisonment. The judgement has taken final and binding effect.

Related listed individuals and entities:

Al-Qaida (QE.A.4.01), listed on 6 October 2001

Ibrahim Mohamad Khalil (QI.M.206.05), listed on 6 December 2005
Ismail Mohamed Ismail Abu Shaweesh (QI.A.224.06), listed on 2 August 2006

Grant Thornton

Reporting Entity Sector Profiles: BC Notaries Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

BC Notaries Industry NAICS Codes

Code	Description
54112	Offices of Notaries

Offices of Notaries - (NAICS 54112)
Exclusions
- offices of legal and paralegal practitioners, except offices of lawyers and notaries (54119, Other Legal Services); and
- offices of notaries public engaged in activities, such as administering oaths and taking affidavits and depositions, and witnessing and certifying signatures on documents, but not empowered to draw up and approve legal documents and contracts (54119, Other Legal Services).

Number of establishments in Canada by type and region: December 2012
Offices of Notaries (NAICS 54112)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	3	9	12	0.6%
British Columbia	127	59	186	9.3%
Manitoba	1	1	2	0.1%
New Brunswick	1	0	1	0.0%
Newfoundland and Labrador	1	0	1	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	0	0	0.0%
Nunavut	0	0	0	0.0%
Ontario	3	8	11	0.5%
Prince Edward Island	0	0	0	0.0%
Quebec	1,071	723	1,794	89.3%
Saskatchewan	0	0	0	0.0%
Yukon Territory	0	1	1	0.0%
CANADA	1,207	801	2,008	100%
Percent Distribution	60.1%	39.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Offices of Notaries (NAICS54112)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	3	0	0	0
British Columbia	90	37	0	0
Manitoba	1	0	0	0
New Brunswick	1	0	0	0
Newfoundland and Labrador	1	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	2	1	0	0
Prince Edward Island	0	0	0	0
Quebec	837	234	0	0
Saskatchewan	0	0	0	0
Yukon Territory	0	0	0	0
CANADA	935	272	0	0
Percent Distribution	77.5%	22.5%	0.0%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Appendix B Case Examples and Typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Former B.C. notary accused of $83-million Ponzi scheme. The Globe and Mail, April 4, 2012.

2. Former notary public accused of fraud. British Columbia Institute of Technology Broadcast News, January 14, 2014.

3. Law Society of BC recommendations may have significant implications. SLAW, January 24, 2014.

4. BC says yes to paralegal regulation. Paralegal Scope Magazine, December 10, 2013.

5. Law society pushes for allowing notaries, paralegals to expand legal services. Vancouver Sun, December 9, 2013.

Former B.C. notary accused of $83-million Ponzi scheme

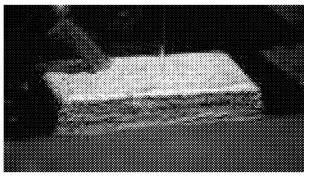
JANET MCFARLAND
The Globe and Mail
Published Wednesday, Apr. 04 2012, 3:16 PM EDT
Last updated Thursday, Sep. 06 2012, 12:59 PM EDT

A former notary public in Vancouver masterminded a Ponzi scheme that raised $83-million from 218 investors who were told their money was being invested in a financing deal with a high-end winery, the British Columbia Securities Commission alleged Wednesday.

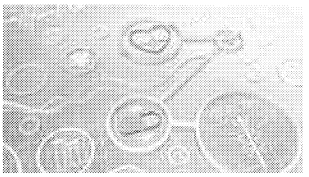
But in an unusual twist, the B.C. regulator said Mark Anthony Group Inc., which owns the Mission Hill Family Estate winery in Kelowna, did not know its name was being used in the investment scheme and had no involvement in a financing deal with Vancouver notary Rashida Samji.

MORE RELATED TO THIS STORY

- Calgary men behind $46-million fraud scheme: ASC
- 'Pre-retirees' are prey for fraudsters, study finds
- B.C. couple charged with securities fraud



MARKET VIEW
Video: How gold relates to U.S. employment



LET'S TALK INVESTING
Video: Should you rely on your employer for life insurance?

The securities regulator said Ms. Samji promised investors a "secure investment" that would provide loan collateral to wineries and would earn between 12 per cent and 30 per cent annually. She pledged their money would be held in a trust account and not paid to any party.

In reality, the BCSC alleges, Ms. Samji had no notary trust account and deposited the money into two personal bank accounts in the name of two companies she created. Much of the money has been lost, although $63-million was paid in interest to investors over the 10 years the investment scheme was operating.

The BCSC alleges that Ms. Samji told investors their money was financing a complex loan arrangement with wine-and-beer importer Mark Anthony Group, although the company says it had no business arrangement with the notary.

Mark Anthony Group spokesman Ian Galbraith said Wednesday that the

company has no idea why Ms. Samji used its name in her scheme and never had any business dealings with her.

"We were unaware of this transaction, and we were contacted by the police and are co-operating fully with them," he said.

Ms. Samji allegedly arranged with an investor to lend $300,000 to finance a house mortgage for an executive of Mark Anthony Group. The executive had no knowledge of the transaction and no mortgage actually existed, the regulator said, even though Ms. Samji purportedly "renewed" the mortgage five times between 2002 and 2011.

The BCSC said Ms. Samji took the money and created fake mortgage documents by cutting and pasting information from a real land title office document and faking the alleged borrower's signature.

Many of the investors in the Ponzi were allegedly referred to Ms. Samji by a financial planner who previously worked at Coast Capital Savings in Vancouver, the BCSC said.

The regulator said Wednesday it has reached a settlement agreement with Arvindbhai (Arvin) Patel, a former mutual fund salesman and financial planner at Coast Capital, who admitted that he encouraged 90 people – including family members, colleagues and clients – to invest $29-million with Ms. Samji.

Mr. Patel has been permanently banned from trading securities in the province, and from working in the securities or investor relations field.

The BCSC said Mr. Patel, who is unemployed, voluntarily transferred his legal interest in five properties to a court-appointed receiver, but was not assessed an additional fine because he has substantial debts and "no reasonable prospect" of being able to pay an additional amount.

The commission said Mr. Patel personally invested $600,000 with Ms. Samji, of which $350,000 was lost. His family invested $1.6-million and lost $1.4-million.

A lawyer for Mr. Patel said he could not comment while a lawyer for Ms. Samji could not be reached for comment.

Ms. Samji and Mr. Patel are also facing lawsuits, including a class-action suit, launched by investors. The class-action suit also names Coast Capital Savings.

Investor Lawrence Jer, a postal worker from Delta, B.C., and his wife Jun Jer, a piano teacher, are the lead plaintiffs on the class-action suit, claiming Mr. Patel was their financial adviser for 17 years and recommended the investment with Ms. Samji. The couple invested

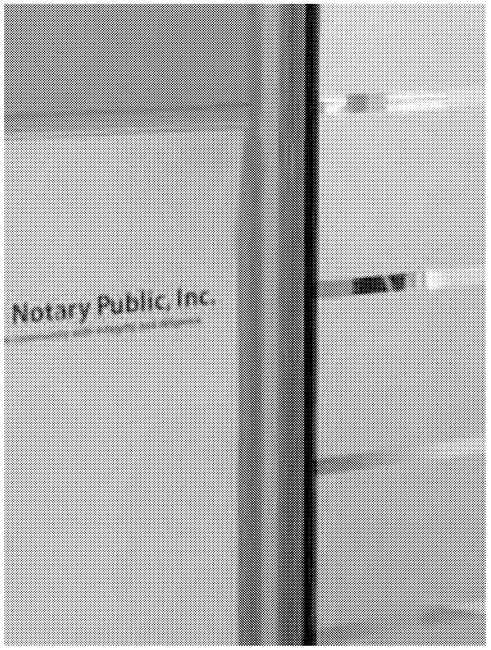
$350,000 and received interest payments totalling $156,000 from 2007 to 2011.

The couple alleges they were told their money was being invested in a "Mark Anthony Investment" product and would be held in trust. They allege their interest payments were made via a bank draft "to conceal the identity" of the accounts the money came from.

The BCSC said the Society of Notaries Public of B.C. suspended Ms. Samji on Feb. 7 and obtained a court order appointing a custodian over her practice. She resigned from the society on March 6, the regulator said.

Former notary public accused of fraud

Posted on January 14, 2014 by Alisha Randhawa



A Vancouver woman, Agatha So Chun Chung, who ran a notarial practice is accused of stealing funds from various accounts (Ty Clark)

A former notary public who ran her own practice is suspected of fraud and embezzlement.

Agatha So Chun Chung has been accused of accessing and manipulating trust accounts at various institutions while operating a notarial practice on East 49th street in Vancouver.

The Society of Notaries Public of British Columbia alleges that Agatha unlawfully removed money from many trust funds for her own means, namely to help pay overdue mortgage payments for three houses owned by her and her husband.

On three separate occasions – July 31st, 2008, January 22, 2009, and December 15, 2011 – the notary society claims Agatha deliberately transferred her legal half of each property to her husband in order to hinder, defeat, or delay her current and future creditors.

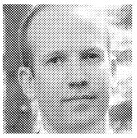
While the extent of her fraudulent scheme is not yet fully known, the notary society believes significant funds are missing.

Chung's husband, Bennie Yim Ming Chung and her daughter, Bonnie Kar Ying Chung are also accused of being co-conspirators.

No follow-up trial has been scheduled yet.

By Ty Clark

Law Society of BC Recommendations May Have Significant Implications



by Michael Litchfield

More posts by Michael »

On December 6, 2013, the Benchers of the Law Society of British Columbia unanimously approved in principle, three recommendations that, if implemented, have the potential to significantly alter the future legal services landscape in the province.

The recommendations were contained in the final report of the Legal Service Providers Task Force, a group formed by the Law Society in the fall of 2012. The mandate of the task force was to examine issues relating to the question of whether the Law Society of BC should regulate only lawyers, or whether they should regulate all legal service providers in the province. While the specific issue of regulating non lawyer legal service providers was given significant attention during the most recent Law Society Strategic Planning process, forms of this question have been considered as far back as 1989, when the Paralegalism Subcommittee recommended against the creation of a separately regulated, new paralegal profession.

The final report of the Task Force contains detailed analysis and conclusions on a number of key issues and makes the following recommendations:

1. That the Law Society and Society of Notaries Public of British Columbia seek to merge regulatory operations;
2. That a program be created by which the legal regulator provide paralegals who have met specific, prescribed education and/or training standards with a certificate that would allow them to be held out as "certified paralegals";
3. That the Law Society develop a regulatory framework by which other providers of legal services could provide credentialed and regulated legal services in the public interest;

The first recommendation will come as no surprise to anyone who has been monitoring the legal services landscape in British Columbia over the last ten years. Notaries Public in British Columbia enjoy a more expanded scope of legal service than some of their counterparts across Canada that has allowed them to handle certain real estate, commercial and wills matters. In

addition, the Society of Notaries Public of BC has long been advocating for an even greater expansion of service. Most recently in 2010, the Society of Notaries Public of British Columbia approached the Ministry of Attorney General to discuss an expansion in the scope of services permitted to include estate administration, incorporation of companies and certain family law related services. In addition to the requested expansion of services, the Notarial Profession in BC also underwent a significant change in 2009 when longstanding limitations on total number and geographically restrained notarial districts was removed in the province. In many ways then, the first recommendation is not surprising in the least and is a reaction to what I personally believe is an inevitable fundamental change in the role of notaries in the delivery of legal services in the province. A change that would likely have happened with or without the involvement of the Law Society of BC.

The second recommendation likewise is not surprising given the changing roles of paralegals in Canada. Consideration of the appropriate role of paralegals has been debated in British Columbia for many years and various working groups have been struck to consider the issue. Most recently, in January of 2013, changes to the Professional Conduct Handbook (now the Code of Professional Conduct), defined a "designated paralegal" and set out an expanded scope of service that these individuals could perform under the supervision of a lawyer. In other jurisdictions such as Ontario, paralegals are permitted an even greater scope of practice and come under the regulatory jurisdiction of the Law Society. In Ontario specifically, this regulatory change was precipitated by the existence of unregulated paralegals offering their services into the marketplace. Seen through this lens then, the second recommendation, like the first, is similarly addressing a state of affairs that is evolving with or without the Law Society of BC's involvement.

The final recommendation is the most interesting of the three and also holds the most potential for altering the landscape of legal services in British Columbia. It is not explicitly clear who "other providers of legal services" refers to. The report makes reference to various groups such as mediators and commissioners but ultimately concludes that "...consideration of the regulation of other legal service providers should be deferred for now."

The report notes that "...the Task Force consider that each of its recommendations is a first step toward an end result, and each will require further work, analysis, collaboration and consultation with other interested parties." How these recommendations may be implemented and their impact remains to be seen. As discussed above however, while the recommendations have the potential to significantly alter the legal landscape in British Columbia, they are not surprising and I would propose are a reaction to changing market forces that are already in play. This fact

will hopeful y provide the necessary pressure to ensure that action is taken by the Law Society of BC to address the shifting legal marketplace and that the work of the Legal Service Providers Task Force is not relegated to the bookshelf.

BC SAYS YES TO PARALEGAL REGULATION

December 10, 2013 · *by* Elizabeth · *in Announcements, Law & Order, Law Society/Regulatory Affairs, Regulatory Affairs* · *Leave a comment*

Photo: Vancouver Sun

Paralegals in British Columbia will come under the same regulatory umbrella as lawyers, with the approval in principle of an access-to-justice based regulatory framework for paralegals and notaries public.

At its Dec. 9 meeting, Law Society of British Columbia benchers unanimously approved in principle three recommendations:

- The Law Society and the Society of Notaries Public of British Columbia seek to merge regulatory operations
- That a program be created by which the legal regulator provide paralegals who have met specific, prescribed education and/or training standards with a certificate that would allow them to be held out as "certified paralegals"
- That the Law Society develop a regulatory framework by which other providers of legal services could provide credentialed and regulated legal services in the public interest.

The change will transform the regulation and delivery of legal services in B.C.

Bruce LeRose had chaired the Legal Service Providers Task Force for the society. Its final report was presented Dec. 6. LeRose said approving the recommendations in principle is an important move toward increasing legal services access in the province.

"Access to justice is slipping out of reach for many British Columbians," LeRose said. "It is critical that the Law Society look for ways to reverse that trend, and these ideas could be a big part of that."

Paralegal Association Involvement Continues

Carmen Marolla, Director of the B.C. Paralegal Association, said the association will work with the law society to implement the changes. "We look forward to continuing to work with the Law Society to develop the criteria for certification for paralegals, and to consider how best to create the regulatory framework to be developed for stand-alone legal service providers."

B.C. Law Society President Art Vertlieb called the benchers' unanimous support for the motion a "watershed moment in the Law Society's history."

Vertlieb attended the Law Society of Upper Canada's Welcome Reception for new licensees in November, and

spoke to Convocation the next day. He came to learn more about how paralegal licensing affected access to justice in Ontario.

"Ultimately, we will move to regulation, like Ontario," Vertlieb said in November. "We need to get on board and bring in a program of licensing that addresses access to justice issues."

Changing Face of Legal Services in Canada

Law societies in British Columbia and Quebec are looking to the Ontario licensing model, with a view to licensing the profession in their jurisdictions. The moves are seen as meeting access-to-justice principles, and protecting the public from untrained renegades.

The Law Society of British Columbia regulates the more than 11,000 lawyers in the province. It sets and enforces standards of professional conduct, to ensure the public is served by a "competent, honourable legal profession."

Ian Mulgrew: Law society pushes for allowing notaries, paralegals to expand legal services

Move would make courts more accessible to those who can't afford lawyers

BY IAN MULGREW, VANCOUVER SUN COLUMNIST DECEMBER 9, 2013

The Law Society of B.C. is proposing a sweeping change that could dramatically change the way legal services are delivered in the province.

Photograph by: Mark van Manen , Vancouver Sun files

The Law Society of B.C. is proposing a sweeping change that could dramatically change the way legal services are delivered in the province.

The society's governing directors have unanimously approved a task force report that says the legal regulator should merge with the Society for Notaries Public of B.C. and expand the use of credentialed paralegals to lower costs for the public.

"The changes are going to help access to justice tremendously," said Art Vertlieb, president of the law society.

"It's the old analogy: If you go to the hospital, you don't see the neurosurgeon right away. You see the triage nurse. Our challenge is to

get our members to buy in."

There are about 300 notaries in the province and nearly 11,000 lawyers, so the regulatory change is not a big deal.

But allowing paralegals to appear in B.C. courts under a system like Ontario's would be a major step, and many lawyers may balk at the prospect of lower-priced competition.

While lawyers can charge hundreds of dollars an hour, paralegals work for a fraction of that because they have far less legal education and handle less serious work.

Paralegals have been involved in legal aid service delivery in B.C. since the mid-'70s for minor legal tasks and by legal aid to meet criminal and civil legal information needs.

They are used for poverty law services such as welfare rights, EI appeals or landlord-tenant disputes — areas where lawyers traditionally don't practice or are too expensive to consult.

"To do a lot of legal work you don't need eight years (post secondary education)," Vertlieb explained.

"Ontario's model is basically a two-year community college course and they write a test. We may take that model or maybe there's one between two years and eight years."

In Ontario, paralegals are regulated, carry practice insurance and handle proceedings in small claims courts and Ontario courts of justice in matters under the Provincial Offences Act, Highway Traffic Act, in a summary conviction court under the Criminal Code, and before various tribunals handling landlord/tenant and workers' benefits cases.

B.C. allows paralegals to do some tasks under the supervision of a lawyer and they can appear in Family Court on some issues as part of a pilot project.

But judges have been reluctant to embrace a system that would allow more non-lawyers appearing before them when they are already dealing with a huge increase in unrepresented litigants who can't afford lawyers.

"Ontario had a long-standing tradition with paralegals going into court in that province … but B.C. has none of that tradition," Vertlieb said.

In Ontario when they brought in their licensing regime, he added, they

expected about 800 people to sign up to become paralegals — 3,000 arrived and there are some 5,600 now working seven years later.

"Think what that does to representation and access (to justice)," Vertlieb said.

In B.C., the near monopoly lawyers enjoy on providing legal services and the inefficiency and expense of the courts have meant the poor and the middle class can't afford to defend or assert their rights, creating a serious justice deficit.

The crisis is not unique to the province, though, as most common-law jurisdictions are wrestling with similar concerns.

By way of counterpoint, in Denmark anyone is permitted to practise law, even for a fee, subject to certain exceptions with respect to appearances in the superior courts. Clients therefore have a choice — obtain legal services from a qualified, regulated and insured professional, or take their chances in a buyer-beware market.

In common-law jurisdictions, the U.K. has been leading the way in addressing these issues, with mixed results. Ontario has been on the forefront of change in Canada.

The Law Society of Upper Canada followed England's lead in co-ordinating legal services provided by other professionals, not just lawyers, and introduced paralegals more than half a decade ago.

In a five-year review of the move, the society deemed the change "by any objective measure … a remarkable success."

Washington state also recently created "limited licence legal practitioners" under the authority of the Washington state Supreme Court.

The Law Society of B.C. created a task force in the fall of 2012 to examine whether it should regulate all legal service providers, in particular paralegals.

Chaired by Bruce LeRose, a law society life bencher, it included Ken Walker, a law society vice-president, Godfrey Archbold, president of the Land Title Survey Authority, Satwinder Bains, an appointed bencher, John Eastwood, president of the Society of Notaries Public, Carmen Marolla, vice-president, B.C. Paralegal Association, Kerry Simmons, president of the Canadian Bar Association — B.C. Branch, and Wayne

Robertson, executive director of the Law Foundation.

Their 41-page report was adopted by the benchers Friday.

"Access to justice is slipping out of reach for many British Columbians," said LeRose. "It is critical that the law society look for ways to reverse that trend, and these ideas could be a big part of that."

The task force said a method needed to be created to expand the scope and provide paralegals who have met prescribed standards with a certificate defining their function.

"The B.C. Paralegal Association is extremely pleased," said Marolla, of the 700-member group.

"We look forward to continuing to work with the law society to develop the criteria for certification for paralegals and to consider how best to create the regulatory framework to be developed for stand-alone legal service providers."

The task force recommendations could reduce some of the costs, eliminate the maze of multiple regulators that exists and end the hegemony of lawyers over legal services.

Still, it's not clear a single regulator of legal service providers will improve access to justice.

The task force, however, believes economies of scale can be achieved, and that's important.

"It is, simply put, more economically efficient to regulate legal service providers through one organization than it is to have to create multiple governance structures and regulatory bureaucracies, particularly when the same or similar services are being regulated," the report said.

"Not only does this duplication risk the creation of differing standards, it costs more to the system as a whole and is therefore difficult to justify."

Legal stakeholders will begin discussing the details of the societies' merger and a regulatory framework by which other existing providers of legal services, or new stand-alone groups, can provide credentialed and regulated legal services in the public interest.

Together with post-secondary institutions, they also will develop a program of specific, prescribed education or training standards for certified paralegals.

Grant Thornton

Reporting Entity Sector Profiles: Credit Unions Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entry data

FOURTH QUARTER 2013
CREDIT UNION/CAISSE POPULAIRE SYSTEM RESULTS

AFFILIATED CREDIT UNIONS & CAISSES POPULAIRES

($millions) Province	Total Savings/Deposits	Total Loans	Total Assets	Total Credit Unions	Total Locations	Total Membership
British Columbia	$52,033	$50,894	$58,958	43	371	1,877,940
Alberta	19,610	18,529	21,694	33	207	646,698
Saskatchewan	15,968	14,615	18,214	53	285	490,712
Manitoba	21,050	19,368	22,730	37	190	599,284
Ontario	27,994	28,424	33,047	90	502	1,327,438
Ontario CPs	1,172	1,107	1,349	13	26	62,005
New Brunswick	829	732	909	10	30	69,301
Nova Scotia	1,870	1,605	2,077	29	76	153,979
Prince Edward Island	783	618	858	8	15	55,224
Newfoundland	949	862	1,026	10	39	52,651
TOTAL	**$142,258**	**$136,754**	**$160,862**	**326**	**1,741**	**5,335,232**

NON-AFFILIATED CREDIT UNIONS & CAISSES POPULAIRES

Caisses Populaires						
CPs outside of Quebec (MB, ON, NB)	**$7,226**	**$7,048**	**$8,440**	**34**	**141**	**329,627**
Quebec	105,007	116,851	141,106	358	1,130	4,454,480
TOTAL (All)	**$112,233**	**$123,899**	**$149,546**	**392**	**1,271**	**4,784,107**
Credit Unions						
Ontario	$338	$248	$383	6	18	37,484
TOTAL	**$112,571**	**$124,147**	**$149,929**	**398**	**1,289**	**4,821,591**

COMBINED CANADIAN CREDIT UNION & CAISSE POPULAIRE SYSTEM RESULTS

TOTAL	**$254,829**	**$260,901**	**$310,791**	**724**	**3,030**	**10,156,823**

Above Figures do not include affiliated companies of the credit union system, such as Concentra Financial Inc., The CUMIS Group Ltd., The Co-operators Group Ltd., Credential Financial Inc., and NEI Investments.

Source: Credit Union Central of Canada - Q4 2013 - Credit Union/Caisse populaire System Results

Note: the industry data provided in the table above is understood to be more accurate, and is more recent, than the Statistics Canada data which follows.

Industry statistics and reporting data

Credit Union Industry SIC Codes

Code	Description
6061	Credit Unions

Credit Union Industry NAICS Codes

Code	Description
52213	Local Credit Unions
522321	Central Credit Unions

Using NAICs codes, searches for statistical data on the Credit Union sector were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Central Credit Unions (NAICS 522321)

Number of establishments in Canada by type and region: December 2012
Central Credit Unions (NAICS 522321)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	1	0	1	2.8%
British Columbia	2	2	4	11.1%
Manitoba	21	0	21	58.3%
New Brunswick	2	0	2	5.6%
Newfoundland and Labrador	0	0	0	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	1	0	1	2.8%
Nunavut	0	0	0	0.0%
Ontario	3	1	4	11.1%
Prince Edward Island	0	0	0	0.0%
Quebec	1	0	1	2.8%
Saskatchewan	1	1	2	5.6%
Yukon Territory	0	0	0	0.0%
CANADA	32	4	36	100%
Percent Distribution	88.9%	11.1%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Central Credit Unions (NAICS522321)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	0	0	1	0
British Columbia	0	1	1	0
Manitoba	0	20	1	0
New Brunswick	0	2	0	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	1	0	0
Nunavut	0	0	0	0
Ontario	0	3	0	0
Prince Edward Island	0	0	0	0
Quebec	0	1	0	0
Saskatchewan	0	0	0	1
Yukon Territory	0	0	0	0
CANADA	0	28	3	1
Percent Distribution	0.0%	87.5%	9.4%	3.1%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Local Credit Unions (NAICS 52213)

Number of establishments in Canada by type and region: December 2012 local Credit Unions (NAICS 52213)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	55	6	61	3.8%
British Columbia	234	2	236	14.9%
Manitoba	64	1	65	4.1%
New Brunswick	50	2	52	3.3%
Newfoundland and Labrador	10	0	10	0.6%
Northwest Territories	0	0	0	0.0%
Nova Scotia	38	2	40	2.5%
Nunavut	0	0	0	0.0%
Ontario	270	31	301	19.0%
Prince Edward Island	9	0	9	0.6%
Quebec	610	3	613	38.7%
Saskatchewan	195	4	199	12.5%
Yukon Territory	0	0	0	0.0%
CANADA	1,535	51	1,586	100%
Percent Distribution	96.8%	3.2%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 local Credit Unions (NAICS52213)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	13	40	1	1
British Columbia	8	215	10	1
Manitoba	3	54	6	1
New Brunswick	2	47	1	0
Newfoundland and Labrador	0	9	1	0
Northwest Territories	0	0	0	0
Nova Scotia	4	34	0	0
Nunavut	0	0	0	0
Ontario	43	217	8	2
Prince Edward Island	0	9	0	0
Quebec	33	543	33	1
Saskatchewan	50	139	6	0
Yukon Territory	0	0	0	0
CANADA	156	1,307	66	6
Percent Distribution	10.2%	85.1%	4.3%	0.4%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Credit Unions

Province	Number of Establishments
Alberta	168
British Columbia	377
Manitoba	219
New Brunswick	41
Newfoundland and Labrador	37
Nova Scotia	52
Ontario	527
Prince Edward Island	8
Quebec	1,220
Saskatchewan	254
Total	2,903

Source: OneSource

NAICS Code 522130 – Credit Unions

Province	Number of Establishments
Alberta	168
British Columbia	378
Manitoba	219
New Brunswick	41
Newfoundland and Labrador	37
Nova Scotia	52
Ontario	527
Prince Edward Island	8
Quebec	1,220
Saskatchewan	254
Yukon	1
Grand Total	2,905

Source: OneSource

Appendix B: Examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Credit unions lead the pack in servicing entrepreneurs: CIB survey. Financial Post, May 24, 2013.
2. Quebec man pursues bank in money laundering case. CBC News. January 29, 2011.
3. Alleged sales tax fraud may have helped finance Sikh terrorists; report. Agence France Presse, February 10, 2003.
4. Elderly trio accused of stealing $2 million from Manitoba credit union. Brandon Sun, December 15, 2007.
5. Money laundering feared at credit union; Troubled Caisse Populaire de Shippagan saw huge sums coming and going, says official. Times & Transcript, April 6, 2007.
6. Official wonders whether credit union was used for money-laundering scheme. The Daily Gleaner, April 6, 2007.
7. Potential Risks Associated with Providing Banking Services to Money Service Businesses. Operational Risk Advisory #2. Deposit Insurance Corporation of Ontario, January 2012.
8. Credit union helps new Canadians support their families. Luminus Financial, February 8, 2011.
9. In reversal, some banks value MSB account fees over AML risks. S.H.C. Consulting Group LLC, December 2, 2011.
10. Philly credit union manager charged with money laundering. Reed Elsevier Properties SA, April 1, 2013.
11. Regulators hit Miami Gardens credit union with cease and desist order. South Florida Business Journal, September 18, 2013.
12. Former credit union president sentenced to prison for fraud. Bonny Lake Courier-Herald, March 21, 2014.
13. Pimp laundered cash through credit union. Independent, December 4, 2012.

14. Former credit union executive sentenced to 24 years: Longest white-collar sentence in Massachusetts. Business Wire, September 12, 1995.

15. Former credit union president gets 5 years for money laundering. KYTX-CBS, December 1, 2010.

16. De-risking trends at big banks affect credit unions. Corporate One Federal Credit Union, November 2013.

TRENDING Housing Market | Bitcoin | Samsung Galaxy S5 | Loonie | Keystone XL Pipeline | Emerging Markets | PDAC 2014 | Apple | Pensions | Investing

Credit unions lead the pack in servicing entrepreneurs: CFIB survey

MASHOKA MAIMONA | May 24, 2013 | Last Updated: May 29 9:33 AM ET
More from Mashoka Maimona

©Bent Lewin/Bloomberg

CFIB's Battle of the Banks: Credit unions win service wars

In light of a recent Canadian Federation of Independent Business (CFIB) report, Dan Kelly, the group's chief executive, slammed big banks for being "short-sighted" when it comes to servicing smaller businesses.

The CFIB report *Battle of the Banks*, released last Wednesday, ranked banks according to how well they serve clients who own small and medium-sized businesses, with performance scores on service, financing, fees, and account manager.

Bank of Montreal and Scotiabank tied for second place with 5 (out of 10), while Alberta-based ATB Financial tumbled to the bottom of the lot with a meagre score of 2.7. Credit unions punched their way to first place, proving their commitment to the small business market.

Mr. Kelly emphasized the importance of a strong relationship between small businesses and their banks. While the latter play a critical role in business growth and development, SMBs are "intensely profitable" to banks because they bring their professional and personal business to the financial institution.

"If [banks] are not doing their job as effectively as they could, it means small businesses may be stunted. That's not helpful for taxpayers or the economy, and we're all counting on small businesses to pull us out of this erratic economy," he said.

The two surprises in the report, he said, were the plummeting fortunes of HSBC (ranked 3.6) and Alberta-based ATB Financial, from second and third place, respectively, in the last survey conducted in 2009 to nine and 10 in 2012.

While HSBC's tumble can be attributed to its shrinking share of the Canadian market, Mr. Kelly said ATB Financial's starkly low rankings, with a significant market penetration among rural-based SMBs in Alberta, are befuddling.

"I have not heard in any change in corporate strategy on ATB's part, but there seems to be a very different view of that institution by small firms compared to three short years ago," he said.

Related

How a micro-loan can turn your great idea into a business

How to talk to a bank about financing your business

ATB Financial's Wellington Holbrook said it was "gut-wrenching" to read their staggering standing report. But the executive vice-president of business and agriculture said he wasn't surprised.

"The timing of the survey made us particularly vulnerable," Mr. Holbrook said, citing the recent replacement of an end-to-end banking system, which inconvenienced customers, especially when it came to accessing online statements.

> "Our internal surveys suggest there have been improving customer satisfaction with the new system. When [our staff] was putting out fires [in the new system], it was hard for them to be doing other things for their customers."
>
> Mr. Kelly also blasted Canadian Imperial Bank of Commerce (CIBC) for a satisfaction rating that has "continued to scrape the bottom," citing their strategy to pull away from serving small-business clients. "The fact they fared badly among small and micro-sized businesses didn't surprise us so much, but even for medium-sized firms, CIBC was poorly rated," he said.
>
> Small business owner Kerry Muise joined in the chorus with 13,000 of her cross-country counterparts surveyed for the report, agreeing that credit unions outperform big banks.

With an overall score of 7.4, credit unions led in all categories, save for service, where it ranked second.

Ms. Muise and her husband, who own a gas station in Yarmouth, N.S., found an "absolutely wonderful" business match with their local credit union, Coastal Financial Credit Union. She said when they shopped around for investment openings three years ago, they approached two chartered banks.

"Right from the start, the credit union outperformed [the banks] in terms of service, interest, and enthusiasm for helping us to buy this business and enhance the community.

"At the bigger bank, we were one of many in the line-up, whereas at the credit union, I was made to feel like my business was very important to them," Ms. Muise said.

Credit unions are not-for-profit co-operatives owned by its members, rather than traded on the stock market. As a result, business profits are seen as investments toward the well-being of the community, she added. "People who work [in credit unions] are not an employee of a company — they're an employee of yours."

Steven Fitzpatrick, chief financial officer of Credit Union Central of Canada, echoed the sentiment. "Credit unions are very close to the ground in their communities. Because they are in the communities, they understand the key role small businesses play there."

Mr. Fitzpatrick, a former vice-president in CIBC commercial banking, said credit unions emphasize local decision-making, which the Big Six Banks overlook. "We have a saying that credit unions have a heart. This survey would say we also have the smarts," he said.

He dispelled the notion that credit unions are limited to small towns, pointing to their presence in Vancouver, Calgary, and Edmonton.

"We're not going to have the largest market share, but we have a disproportionately high market share for our size and our presence in the market. We clearly have an offering small businesses find attractive," Mr. Fitzpatrick said.

One out of four small business owners in the report had their accounts with a credit union.

Mr. Kelly said there is no shortage of high-budget marketing campaigns targeting small business clients. The packages the banks publicize are more marketing efforts, rather than steps toward product improvement or changing their lending practices, he said.

"We want the reality to catch up with the marketing language."

Quebec man pursues bank in money laundering case

Accountant ran money scheme at credit union, Quebec businessman says

CBC News Posted: Jan 28, 2011 7:02 PM ET Last Updated: Jan 29, 2011 4:16 PM ET

A Quebec construction firm owner has alleged his accountant cheated him out of $1 million, and says his local credit union was aware of the money-laundering scam.

The alleged money-laundering scheme, according to a Radio-Canada report, involves construction entrepreneur Robert Thomas, a caisse populaire branch in Joliette and chartered accountant Jean Siminaro, who has been linked to the Hells Angels.

What is money laundering?

Money laundering is the process by which a person or organization converts cash and assets gained through criminal activity into a form that can be used legitimately and openly without drawing the attention of the authorities.

The broad aims of money laundering are threefold: To convert proceeds of crime to a less suspicious form; to conceal the illegal ownership or origin of criminal earnings; and to create a legitimate explanation for the source of the assets.

The RCMP say it is difficult to determine the exact size and scope of money laundering in Canada but that it is a multibillion-dollar industry.

Read more about money laundering.

Thomas says his signature was forged on hundreds of cheques drawn on his business account, which was managed by Siminaro for several years.

The entrepreneur has launched legal action against the caisse populaire branch and Quebec police are investigating the allegations, according to the CBC's French-language service.

In 2001, Thomas hired Siminaro, his neighbour, to do the accounting for his company Construction Robert Thomas, based in Repentigny.

A nearby branch of the caisse populaire — Quebec's credit union network — lent the company nearly $2 million to launch its building projects.

In 2007, Thomas received notice that he owed back taxes, and the caisse notified him that it planned to seize his

condominiums for failing to repay the loan.

Thomas later discovered that 622 cheques amounting to about $1 million were written against the company's account without his knowledge.

Thomas alleges his former accountant forged his signature and used the chequing account to launder money. As well, the construction entrepreneur alleges, the caisse branch tolerated the situation by allowing the cheques without notifying him.

"There were many cheques, but we can say we tolerated it, as we do sometimes for clients who sometimes have cash flow issues. We're there to provide solutions," credit union manager Jean Dénommé said in an interview with Radio-Canada.

The branch maintains Thomas should have kept tabs on his account and reported any irregularities.

Siminaro was arrested in 2009 and charged with conspiracy and money laundering in connection with Hells Angels boss Normand Marvin (Casper) Ouimet.

Siminaro has been suspended from the Quebec order of accountants pending the legal proceedings against him.

Ouimet was arrested in November 2010 on an outstanding warrant in connection with multiple murders linked to Quebec's biker wars. He is being held in detention at an undisclosed location.

With files from Marie-Maude Denis, Radio-Canada

Alleged sales tax fraud may have helped finance Sikh terrorists: report

Agence France Presse (English)
Mon Feb 10 2003, 6:42pm ET
Section: International News

ATTENTION - CORRECTS US equivalent figure in second para to read 16.25 million US dollars ///

OTTAWA, Feb 10 (AFP) - Opposition lawmakers claimed Monday that a major sales tax fraud may have helped finance Sikh terrorists who blew up an Air India flight from **Canada** in 1985.

Some 25 million dollars (16.25 million US dollars) were bilked from the federal government with fraudulent claims for a goods and services tax (GST), **Canada**'s equivalent to Europe's value added tax, according to a CBC Television report Monday.

The scheme, according to the report, involved fictitious companies billing each other and charging the obligatory GST which was then claimed back by the company allegedly providing the goods and services for export.

In British Columbia, where there is a large Sikh community, police have charged two men -- Sikhander Singh Bath and Manjit Singh Kanghura -- with fraud. Police said the fraud involved the illegal receipt of federal government cheques every month for about three years.

A member of the prosecuting team, Barbara Veltkamp, said there were 18 volumes of documents being entered as evidence which, she claimed, involved fraudulent GST refund claims on alleged transactions between different companies.

She said some 20 fictitious lumber companies were involved.

Veltkamp, who said this was one of the biggest GST fraud cases in Canadian history, involved "very serious charges: **money laundering** and fraud charges."

CBC reported that most of the alleged phoney transactions were handled through the Khalsa **Credit Union**, a financial institution run by and for members of British Columbia's Sikh community.

One of the alleged participants in the fraud scheme was, said CBC, Rupudiman Singh Malik who is in prison facing trial in the 1985 Air India bombing that killed 329 people off the coast of Ireland.

In the House of Commons, John Reynolds, a senior frontbencher with the Canadian Alliance, said: "Terrorism could be involved."

Referring to both this and another multi-million dollar GST fraud in Ontario, Reynolds said: "The government has already admitted organized crime is defrauding Canadians through the GST fraud. Now we learn that international terrorists might have discovered that there is free money in **Canada** when the (governing) Liberals are in power."

Both CBC and Reynolds claimed that government inspectors failed to carry out the most simple of audits on the 25 million dollars alleged to have been illegally claimed.

Coincidentally, one of three militant Sikhs about to go on trial for the Air India bombing -- Inderjit Singh Reyat, 51 -- agreed on Monday to plead guilty to manslaughter in the Air India bombing.

Prosecutors said they had agreed to accept the admission of manslaughter in return from dropping murder and conspiracy charges against Reyat.

Rupudiman Singh Malik and Ajaib Singh Bagri are both due to appear on murder charges resulting from the Air India downing in court in March.

hfw/jlp

Canada-fraud

infomart

BRANDON SUN

Elderly trio accused of stealing $2 million from Manitoba credit union

Brandon Sun
Sat Dec 15 2007
Section: Provincial
Byline: Mike McIntyre

WINNIPEG - An elaborate bank fraud netted two Winnipeg families more than $2 million in a case that has led to criminal charges and a nasty ongoing civil court battle.Police arrested a 64-year-old man, his 63-year-old wife and their 76-year-old business partner this week following a year-long investigation.

Court documents obtained by FPNS show the trio allegedly scammed the Cambrian **Credit Union**'s Main Street branch between September of 2005 and September of 2006.

The money was then allegedly distributed to themselves and their adult children in Winnipeg, Saskatchewan and Alberta.

None of the allegations has been proven and the accused are presumed innocent.

Margaret Sirkis and her husband, Kenneth, declined to comment when contacted on Friday afternoon.

The other accused, John Maxey, couldn't be reached.

Maxey's wife and son, along with two of the Sirkis' children, are named in the civil case, but are not facing criminal charges.

According to the civil court filings, nearly $1 million has already been repaid to the Cambrian **Credit Union**. They are now asking a judge to order the accused to repay the remaining $1.2 million.

Maxey has filed his own claim against Sirkis and his wife, denying any involvement in the illicit operation.

Police said the scam involved manipulating bank computers systems into thinking there was a positive balance by making fictitious deposits between several companies along with dormant bank accounts.

The Sirkis' allegedly owned two different consulting companies and worked closely with Maxey and his four companies to make the frauds happen.

The companies named in the civil court case are: Seabrook Management Services Bradburn Freight Management, Designer Financial Services, Saxon Investments, Main Chance and Albian Investment Ltd.

The scam was uncovered when bank officials became suspicious about a number of "questionable" transactions involving closed accounts from their branch towards the Sirkis' account at Cambrian.

Police have now laid several charges against the accused, including fraud over $5,000, possession of goods obtained by crime over $5,000 and **money laundering**.

The three were each released on a promise to appear in court at a later date.

Length: 337 words

Times & Transcript

Money laundering feared at credit union; Troubled Caisse Populaire de Shippagan saw huge sums coming and going, says official

Times & Transcript (Moncton)
Fri Apr 6 2007
Page: A4
Section: News
Byline: By Kate Wright Times & Transcript Staff

The province's superintendent of credit unions is concerned that a **credit union** in Shippagan may have been used for **money laundering**.

Robert Penney said there are only about 5,000 people living in Shippagan, yet the local Caisse Populaire had 35,000 members at its peak.

He contacted the RCMP because there were a number of significant deposits entering and leaving the caisse populaire from outside the community.

"The main concern is when you have money entering a financial institution that doesn't seem to correspond with the business of that institution or with the community that institution operates in," he said.

Penney said large deposits were coming from outside of the province and were being made by people who didn't normally bank with the **credit union**.

He said the multi-million-dollar transactions were "significant" enough to set off red flags.

Penney says he started looking at the Shippagan caisse last year when he became superintendent of credit unions, and informed the previous Conservative government.

"As far as I'm concerned, deputy ministers and ministers are well aware of the file," he said. "We were actively working on the file."

The Liberal government has been taking heat for bailing out the troubled Shippagan **credit union** with a $60-million rescue package.

Attorney General T.J. Burke said if the caisse had gone bankrupt, taxpayers would have been on the hook for $86 million in protected deposits.

The government has announced a plan including a $31.5-million grant and $10 million in repayable "stabilization shares" to help the Shippagan caisse after years of risky lending practices.

The institution recently announced a deficit of more than $30 million and has been under supervision by **Credit Union** Central of New Brunswick since June 2004.

Burke said information has recently come to light to spur the government to call for further investigation.

The government assistance package would also include a $20 million infusion into the New Brunswick **Credit Union** Deposit Insurance Corporation, which insures credit unions and caisse populaires in the province's two federations. Meanwhile, Shippagan would be required to repay the $10 million in stabilization shares into the deposit insurance corporation by 2022.

The federations maintain their own stabilization funds, totalling about $70 million.

But that money would be left untouched as Shippagan moves from the **Credit Union** Central to the Fédération des caisses populaires acadiennes under the terms of the deal.

Burke has contacted the RCMP and the province's auditor general about possible criminal investigations into what happened at the **credit union**.

"As far as I'm concerned, deputy ministers and ministers were aware of the file," he said.

"I want to be careful somewhat what I say here, but we were before cabinet at least on a couple of occasions and board of management at least on a couple of occasions. "

Volpe, who as the former finance minister was the chairman of the board of management cabinet committee, denied any knowledge of red flags surrounding potential **money laundering**.

With files from Canadaeast New Service reporter Daniel McHardie.

Length: 476 words
Idnumber: 200704060053

Tone: Negative
Ad Value: $755 Circulation: 18,889

The Daily Gleaner

Official wonders whether credit union was used for money-laundering scheme

The Daily Gleaner (Fredericton)
Fri Apr 6 2007
Page: A4
Section: News
Byline: By CHRIS MORRIS The Canadian Press

New Brunswick's superintendent of credit unions says he is looking at whether a financially troubled **credit union** in northern New Brunswick may have been used for **money laundering**.

Robert Penney said about 5,000 people live in the fishing community of Shippagan, yet the local Caisse Populaire in the community had 35,000 members at its peak.

He said a significant number of deposits were made and withdrawn from outside the community and the province, raising questions in his mind about what was happening.

"That's a red flag," he told reporters at the legislature.

"I'm not saying it's evidence of a crime. I'm simply saying it would be responsible for me as superintendent to look further into an issue like that and get guidance from a police agency."

Penney said a number of things about the **credit union**'s operation need to be examined, including "whether or not **money laundering** took place."

New Brunswick Attorney General T.J. Burke said he has contacted the RCMP and the province's auditor general about problems at the Caisse Populaire in Shippagan, an Acadian community in northeastern New Brunswick.

The financial institution has been the focus of political debate after Premier Shawn Graham's Liberal government announced a $60-million bailout package for the debt-ridden **credit union**.

The province is also considering a public inquiry.

A spokesman for the **credit union** couldn't be reached for comment on Thursday.

Burke has raised the spectre of political tampering at the Shippagan **credit union** by the previous Conservative government, which was defeated by the Liberals in September, suggesting there were connections between board members and the Conservatives.

"As we peel the layers of this onion, the smell is getting stronger and stronger. I'll leave it at that," he said Wednesday.

Conservative Leader Jeannot Volpe said Burke appears to have prejudged any inquiry into the caisse and should step aside.

"He has prejudged and accused people of being involved," Volpe said. "He should step aside until the air is cleared."

Penney told reporters Thursday that these concerns were also raised within the highest levels of the former Conservative government, but the RCMP and Office of the Auditor General were only called into investigate this week.

The superintendent of credit unions said he has been working on the file since his appointment in April 2006.

Penney said he brought these concerns to the Conservative cabinet and top bureaucrats.

Ontario
Deposit Insurance Corporation of Ontario
Société ontarienne d'assurance-dépôts

Operational Risk Advisory #2 **January 2012**

Potential Risks Associated with Providing Banking Services to Money Service Businesses

Background

This Advisory outlines the potential risks associated with providing banking services to member-owned Money Service Businesses (MSBs). It also sets out DICO's expectations for those credit unions and caisses populaires that are providing banking and wire transfer services to member-owned MSBs or are considering entering into this line of business.

The current low interest rate environment has motivated some credit unions to improve profitability by seeking non-traditional sources of revenues. In particular, a number of credit unions have entered into arrangements to provide banking and wire transfer services to member-owned Money Service Businesses (MSBs) which are generating fee income for related cash handling, wire transfer and foreign exchange services.

MSBs are defined by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as "non-bank" entities which provide transfer and exchange mechanisms. Individuals and entities generally use MSBs to exchange or transfer value, or to purchase or redeem negotiable instruments. In Canada, an MSB is defined as an individual or an entity that is engaged in the business of any of the following activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any individual, entity or electronic funds transfer network;
- issuing or redeeming money orders, traveler's cheques or other similar negotiable instruments

FINTRAC describes MSBs as generally higher risk customers from a money laundering and /or terrorist financing perspective as criminal elements seek to exploit MSB businesses to transfer and launder funds. For further information please consult FINTRAC's report "Money Laundering and Terrorist Financing Typologies and Trends for Canadian Money Service Businesses, which is available on FINTRACs website at www.fintrac.gc.ca.

While every MSB in Canada must be registered with FINTRAC in a similar fashion to financial institutions, there are a number of MSBs operating outside of the FINTRAC framework. The number and relative size of MSBs make it challenging for regulatory authorities to monitor them effectively.

Major banks have typically refused to provide banking services for MSBs owing to the risks associated with providing them services. For this reason any credit union that has chosen to provide services to MSBs must have a comprehensive and robust compliance regime in place.

Risks to the Credit Union

Credit unions or caisses populaires entering into the servicing of MSBs are receiving significant fees for the services being provided. This level of revenues may unduly influence the credit union's rationale for entering into the MSB business by placing an inappropriately high weighting on potential returns versus the associated risks. In addition, once a financial institution begins taking on MSB clients, it is very likely that other MSBs will seek to open accounts with the credit union thus resulting in ever increasing risk.

The risks to the credit union are both financial and reputational. Financial losses (and in extreme cases, criminal penalties which may include up to 5 years imprisonment) can arise and have arisen from penalties levied by FINTRAC or law enforcement for non-compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA") or from lost recourse on deposited cheques that may potentially be so severe as to result in the failure of the institution. It should also be noted that amendments to the PCMLTFA have been proposed by the Department of Finance to include business relationships in addition to account openings and prescribed financial transactions. Reputational risk may arise from association with fraudulent activities of an MSB, its Principals, employees or its business activities.

Some credit unions have attempted to mitigate the potential risk of non-compliance with PCMLTFA legislation by contracting with third parties to screen MSB applicants and provide anti-money laundering (AML) monitoring. However, third parties do not assume the risk of non-compliance with PCMLTFA and the credit union retains both the financial and reputational risks. Where those third parties are receiving fees from MSB providers to confirm their AML Compliance Programs meet PCMLTFA requirements and monitoring ongoing AML compliance on behalf of the credit union on a fee basis, once the MSB becomes a member, a serious potential conflict of interest may arise.

DICO's Expectations

DICO has the following expectations of credit unions or caisses populaires that engage in this type of business:

- The Board of Directors should authorize entry into this line of business based on a thorough analysis by management of the potential benefits and risks.
- All MSB member accounts should be subject to Board approval.
- A comprehensive risk assessment process should be in place to identify and monitor high risk clients.
- Increased scrutiny is required over MSB accounts as they are considered extremely high risk.

- Annually, the credit union shall verify that the MSBs are in good standing with FINTRAC, provide confirmation to the credit union's Board of Directors and retain record of the verification and report to the Board for DICO examiners.

Credit unions should not accept MSBs as members unless the accounts meet the highest business standards, are professionally managed, operate in full compliance with FINTRAC requirements and are subject to robust internal and external audit procedures.

At a minimum, for each potential MSB account, credit unions are expected to:

- Conduct background checks of account principals (financial and criminal/terrorist);
- Obtain business and financial references;
- Determine the scope and size of operations, including client base and nature of material transactions;
- Review the experience and suitability of the external auditors;
- Review the qualifications of the internal auditors and the internal audit plan;
- Review the business plan and Audited Financial Statements (2 years);
- Confirm that MSB membership meets membership criteria;
- Develop and submit a business case for Board approval where MSB membership is recommended.

Any MSB membership account should have a robust membership agreement including specific operating and reporting criteria to ensure that the MSB continues to operate in full compliance with FINTRAC requirements.

Where a credit union is already involved in offering services to, or is planning to offer services to MSBs, DICO will require the credit union to provide evidence of sufficient due diligence in considering the risks in accordance with By-law #5 requirements.

DICO's examination process will include a review of all new lines of business to confirm that sufficient due diligence has been conducted and that appropriate risk management policies and controls are in place.

Examiners will also review:

- Business case and Board approvals for all MSB accounts
- MSB client information and any outsourcing arrangements or contracts
- the level and quality of internal controls
- the nature and extent of on-going monitoring and compliance practices
- the nature and extent of internal audit procedures
- the form and content of board reports

In cases where increased risk is evident, DICO may place the credit union on its Watchlist and / or require the credit union to maintain additional capital.
If you have any questions, please contact your Regional Manager. For your convenience extracts from part 5 of the PCMLTFA regarding penalties have been included as Appendix A to this document.

APPENDIX A

Extract from the Proceeds of Crime (Money Laundering) and Terrorist Financing Act

PART 5 - OFFENCES AND PUNISHMENT

General offences

74. Every person or entity that knowingly contravenes any of sections 6, 6.1 or 9.1 to 9.3, subsection 9.4(2), sections 9.5 to 9.7 or 11.1, subsection 12(1) or (4) or 36(1), section 37, subsection 55(1) or (2), section 57 or subsection 62(2), 63.1(2) or 64(3) or the regulations is guilty of an offence and liable

- (*a*) on summary conviction, to a fine of not more than $50,000 or to imprisonment for a term of not more than six months, or to both; or
- (*b*) on conviction on indictment, to a fine of not more than $500,000 or to imprisonment for a term of not more than five years, or to both.

Reporting — sections 7 and 7.1

75. (1) Every person or entity that knowingly contravenes section 7 or 7.1 is guilty of an offence and liable

- (*a*) on summary conviction,
  - (i) for a first offence, to a fine of not more than $500,000 or to imprisonment for a term of not more than six months, or to both, and
  - (ii) for a subsequent offence, to a fine of not more than $1,000,000 or to imprisonment for a term of not more than one year, or to both; or
- (*b*) on conviction on indictment, to a fine of not more than $2,000,000 or to imprisonment for a term of not more than five years, or to both.

Defence for employees

(2) No employee of a person or an entity shall be convicted of an offence under subsection (1) in respect of a transaction or proposed transaction that they reported to their superior or in respect of property whose existence they reported to their superior.

Disclosure

76. Every person or entity that contravenes section 8

- (*a*) is guilty of an offence punishable on summary conviction; or
- (*b*) is guilty of an indictable offence and liable to imprisonment for a term of not more than two years.

Reporting — section 9

77. (1) Every person or entity that contravenes subsection 9(1) or (3) is guilty of an offence and liable on summary conviction to a fine of not more than $500,000 for a first offence and of not more than $1,000,000 for each subsequent offence.

Due diligence defence

(2) No person or entity shall be convicted of an offence under subsection (1) if they exercised due diligence to prevent its commission.

Registry

77.1 Every person or entity that provides information to the Centre under section 11.12, 11.13, 11.14 or 11.3 and that knowingly makes any false or misleading statement or knowingly provides false or misleading information to a person responsible for carrying out functions under this Act is guilty of an offence and liable

- (*a*) on summary conviction, to a fine of not more than $50,000 or to imprisonment for a term of not more than six months, or to both; or
- (*b*) on conviction on indictment, to a fine of not more than $500,000 or to imprisonment for a term of not more than five years, or to both.

Liability of officers and directors

78. If a person or an entity commits an offence under this Act, any officer, director or agent of the person or entity who directed, authorized, assented to, acquiesced in or participated in its commission is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence, whether or not the person or entity has been prosecuted or convicted.

Offence by employee, agent or mandatory

79. In a prosecution for an offence under section 75, 77 or 77.1,

- (*a*) it is sufficient proof of the offence to establish that it was committed by an employee, agent or mandatory of the accused, whether or not the employee, agent or mandatory is identified or has been prosecuted for the offence; and
- (*b*) no person shall be found guilty of the offence if they establish that they exercised due diligence to prevent its commission.

February 08, 2011: Credit Union Helps New Canadians Support Their Families

Credit Union Helps New Canadians Support Their Families

Starnews Credit Union has developed new payment and treasury services for Money Services Businesses (MSBs), supported by financial services compliance experts Williams McGuire AML Inc.

Over 25% of new Canadians send money to support their families in developing countries. Typically, they send their funds through MSBs - culturally based institutions with connections to the destination country for little to no charges. However, tightened regulations and practices around compliance among big banks have made the banking relationships and services that MSBs need to operate scarce.

Starnews has teamed up with Williams McGuire to measure MSB applicants against strict standards, and to rigorously monitor their day-to-day activities for compliance with regulatory and risk standards, such as those related to trade sanctions and anti-money laundering. "Starnews is a leader among credit unions, meeting a very important need in the MSB market with a considered risk-sensitive approach, and we are delighted to be helping them with this initiative" says Matthew McGuire, director of Williams McGuire.

MSBs will hold their bank accounts at Starnews and can apply for payment services such as wire transfers, pre-authorized debits and credits, as well as treasury services, such as foreign exchange and other deposit accounts. Starnews has received applications from MSBs looking to expand the services they provide to their communities.

Starnews' CEO, George De La Rosa, has expanded the credit union's membership base from its original focus on employees of the Torstar Corporation, during his 7 years there. According to De La Rosa, "Our growth has been driven by our commitment to credit union values: a focus on relationships, innovation, ethical conduct, and caring about our members and the communities we serve. Helping MSBs serve their communities is a natural way for us to build Starnews' presence in the GTA". Starnews serves anyone living or working in Ontario, and giving their members/customers access to their accounts across Canada through its ATM network alliance with THE EXCHANGE® Network.

About Starnews Credit Union

Starnews is a credit union owned and operated by its members, with a board elected from membership during annual elections. The credit union was originally formed in 1951 to serve Toronto Star employees. Today they service anyone living or working in the province of Ontario.

Find out more at www.starnewscu.com.

About Williams McGuire AML Inc.

Williams McGuire AML's mission is to passionately protect our clients and country from the harms of money laundering, terrorist financing and other financial crime through tailored and informed risk and compliance solutions. We do this by analyzing risk, creating effective controls and assessing existing compliance regimes and controls. Our team is comprised of dedicated full-time professional subject matter experts who understand our clients regulatory and risk mitigation needs.

Find out more at www.amlcompliance.ca.

In Reversal, Some Banks Value MSB Account Fees Over AML Risks

December 2, 2011 By Brian Monroe

Dozens of small banks and credit unions have begun courting money services businesses over the past year, offering financial services to the high-risk clients in exchange for compliance-related fees.

The marketing effort is a reversal in the often fractious relationship between the companies, known as MSBs, and banks that have either turned away the businesses or charged high fees for taking on the associated anti-money laundering (AML) compliance risks. Faced with a tougher market, some small financial institutions are opening their doors to the businesses and offering lower fees to draw new clients, say MSB owners.

"An increasing number of smaller banks and credit unions are realizing MSBs can boost the bottom line as fee generators," said Jeff Sklar, managing director of SHC Consulting Group in Bellmore, NY. Over the last eight months, he has encountered more than 30 financial institutions that have either started banking MSBs or inquired about how to tweak their AML programs to do so, he said.

The opposite has been the case for the last decade, as many small MSBs have had to win over bank officials after the U.S. Treasury Department's Office of the Comptroller of the Currency (OCC) warned that the businesses were high-risk in a 2000 advisory letter. The agency repeated the warning at least twice over the next six years, further prompting banks to drop their MSB customers.

The banking troubles pushed hundreds of MSBs and thousands of agents out of the market, and contributed to industry consolidation, said Michael McDonald, an independent AML consultant based in Miami, who believes the trend is now reversing.

"I don't mind jumping through AML hoops and paying a bit more in fees if it means I get piece of mind and I don't have to be constantly juggling banking relationships," said Alan Friedman, president of La Nacional, a New York-based MSB that has more than 80 locations nationwide.

Several smaller banks across the country have "woken up to the fact that you can get a big increase in fee income banking MSBs because they are huge consumers of cash," he said, adding that in some instances banks are still restricting deposits to only $2,500 a day, which "doesn't do us any good."

How regulators will view the decision by some small financial institutions, withrelatively fewer compliance resources than large banks, to take on new AML risks remains uncertain.

While banking MSBs "can help strengthen the banks' financials, they have to realize that we may disagree with the adequacy of the controls they have in place if we believe their MSB customers are higher risk and require additional monitoring,"said a federal bank examiner in Texas, who spoke on condition of anonymity."That will be reflected in the exam."

The increase in MSB accounts at New York-based Actors Federal Credit Union (AFCU) have meant "an education for us in terms of understanding what AML risks are involved and how to mitigate them," said Chuck Brown, director of check cashing services at institution. The company has opened more than two dozen accounts for money remitters and check cashers, and plans to open its first currency exchange firm account, he said.

"We have a thriving MSB department," said Brown, adding that the credit union's examiners "are well aware of what we are doing and seem supportive."

To mitigate its risk, AFCU has employed third parties to vet related accounts and a secondary transaction monitoring system that allowed the credit union to review all of the transactions of its MSB clients, he said. AFCU has since determined that the transaction monitoring system is no longer needed, he said.

Officials at the credit union request AML program documents from MSBs and conduct annual, onsite visits to see how their clients are meeting their Bank Secrecy Act requirements, he said.

"We wanted make sure they have strong customer identification and know-your-customer programs," Brown said.

For some MSBs, bank accounts remain elusive, however, according to Friedman. Even when the companies agree to stringent AML certifications and deposit limits, banks may choose to drop the accounts with little warning, he said, adding that La Nacional lost banking services recently due to an acquisition.

The new chairman "told us we were a great account, but, sorry, they didn't want it," he said.

CustomerService@MoneyLaundering.com

Philly Credit Union Manager Charged with Money Laundering

KURT MATTSON
Published: April 1, 2013 at 04:29:50 EDT

The United States Attorney Zane David Memeger recently announced the arrest of Miqueas Santana, 43. His embezzlement and money laundering were contributing factors in the closure of the Borinquen Federal Credit Union (BFCU) in Philadelphia. According to court information, between July 2009 and June 2011, Santana, with the permission and approval of the former manager of BFCU, Ignacio Morales, withdrew money from his BFCU bank accounts without depositing sufficient money into the accounts to cover the withdrawals. The result was a deficiency of account balances in his five personal and business savings and checking accounts of more than $500,000. Santana used this money to purchase multiple pieces of real estate in the Philadelphia area.

Morales was previously convicted of multiple counts relating to embezzlement from BFCU and conspiracy to defraud the government regarding the cashing of fraudulent tax refund checks. He is serving a seven-and-a-half-year sentence for his crimes.

If convicted of all charges, Santana faces a maximum sentence of 40 years' imprisonment, 5 years' supervised release, a $1,250,000 fine (or a $1,000,000 fine plus twice the value of the criminally derived property), and a $200 special assessment. The case was investigated by the United States Postal Inspection Service, the Internal Revenue Service-Criminal Investigations, and the Federal Bureau of Investigation. The *Santana* case is being prosecuted by Assistant United States Attorney Arlene D. Fisk.

In June 2011, the National Credit Union Association took over the operation of the BFCU, but within two weeks, closed the credit union and liquidated its assets.

BSA/AML Update

Sep 18, 2013, 1:35pm EDT

Regulators hit Miami Gardens credit union with cease and desist order

Brian Bandell
Senior Reporter-
South Florida Business Journal
Email | LinkedIn | Twitter

Federal regulators issued a cease and desist order against North Dade Community Development Credit Union for violations of anti-money laundering laws.

Such enforcement actions against credit unions are rare. This is the only cease and desist order issued by the National Credit Union Administration (NCUA) so far this year.

The credit union has only $5.8 million in assets. It was "well capitalized" on June 30, an improved from its "undercapitalized" status a year ago.

The NCUA order on Aug. 29 gave it 30 days to suspend all transactions for money services businesses that aren't within its geographic area of membership. Credit unions are only allowed to deal with customers in pre-defined geographic areas. In the case of North Dade Community Development, the area is thenorth-central part of the county.

The regulatory order also told the credit union to stop all business with money service businesses until it implements adequate Bank Secrecy Act, anti-money laundering and Office of Foreign Asset Control (OFAC) compliance. This includes establishing criteria for identifying high-risk members, detecting when transactions involved prohibited countries or individuals, and timely filing suspicious activity reports and currency transaction reports.

It was given 30 days to find an employee responsible for this job, conditional upon approval by regulators.

Courier-Herald

NEWS

Former credit union president sentenced to prison for fraud and embezzlement

Mar 21, 2014 at 7:00AM

The following is a press release.

The former president of a small Pierce County, Washington credit union was sentenced today in U.S. District Court in Tacoma to 18 months in prison, three years of supervised release and more than $129,000 in restitution for two counts of wire fraud and two counts of misapplication of credit union funds, announced U.S. Attorney Jenny A. Durkan. RENEE J. THOMAS, 45, of Graham, Washington, resigned as president of Community Credit Union on September 1, 2009, just as state authorities were preparing to examine the credit union because of concern about its financial performance. Following her resignation, the investigation revealed THOMAS had used a variety of means to defraud not only the credit union but an insurance company and credit card companies associated with it. At sentencing U.S. District Judge Ronald B. Leighton said, "this crime is very serious because it is the type of crime that corrodes faith in our financial system."

According to records in the case, THOMAS committed fraud and embezzled funds in four different schemes. In 2007 THOMAS pressured an employee to falsify records related to nearly $90,000 in car loans so that she and her husband could collect disability insurance. In December 2007, THOMAS used a credit union customer's information to take money from his line of credit. THOMAS applied the $16,500 to her bills. In August of 2009, shortly before her departure from the credit union, THOMAS forged other employees' names to increase the limit on her company credit card. THOMAS used the increased borrowing authority for $22,000 in cash advances and other purchases. Finally, on one of her last days at the credit union, THOMAS used other employees' computer privileges to increase a customer's line of credit and take cash from their account. She then used some of the cash to make a payment on her credit card. The loss to the credit union for the conduct charged in the case is $126,469.

In asking for a prison sentence prosecutors wrote to the court, "As Community Credit Union's President, Thomas owed the credit union one thing – responsible stewardship. Instead, she gave it a two-year fraud "spree," targeting as her victims, the Credit Union, its customers, and its insurance carrier. Rather than watching out for the interest of her employees, moreover, Thomas abused her authority over them and involved them in her criminal schemes."

The case was investigated by the U.S. Secret Service. The case was prosecuted by Assistant United States Attorney Arlen Storm.

Pimp laundered cash through credit union

Single deposit of €854,000 was sent to account by his daughter

JEROME REILLY – Updated 04 December 2012 05:29 AM

Convicted brothel keeper and money launderer Thomas Carroll cleaned up his cash by receiving €854,000 in a single deposit to his credit union account, it can now be revealed.

The single deposit was only part of millions of euro the Carlow-born criminal amassed from his prostitution empire which stretched all over the republic, Northern Ireland and the UK.

Carroll ran his empire from a vicarage in a Welsh village. He fled Ireland after being arrested and subsequently released on bail but still kept up his Irish operation, which included young and vulnerable women from Nigeria who had been trafficked into the sex trade.

Now a written judgement by Judge Neil Bidder has shown how Carroll evaded the authorities by moving cash between accounts, some held by his daughter Toma Carroll, as well as keeping large amounts of cash on hand

Last month Judge Bidder sentenced Carroll, 48, his wife Shamiela Clark and his 26-year-old daughter Toma Carroll after they admitted money laundering.

Thomas Carroll and Clark also pleaded guilty to conspiring to control prostitutes, including women trafficked into Ireland from Portugal, Venezuela, Brazil and Nigeria. Thomas Carroll was jailed for seven years, Clark for three-and-a-half years. Toma Carroll was jailed for two years but was freed immediately because of time spent in custody awaiting trial.

Thomas Carroll ran 35 brothels in the north and the Republic. For every €27,000 in total takings from his brothels, Carroll was making more than €13,000 in clear profit.

In 2005, records showed a final balance for the year of €300,000 from Carroll's Irish brothels. In 2006 a search discovered €100,000 in cash kept in a safe and between €10,000 and €15,000 kept in notes in his house.

"The money laundering scheme was complicated, it included property investments in Wales and other countries, financed with the proceeds of the prostitution business," the judge said.

Some of the prostitutes made payments to accounts controlled by Thomas Carroll by International Money Transfers and some of this money was used to buy luxury properties in Bulgaria, South Africa and Wales.

Other monies ended up in Bank of Ireland accounts in the name of Toma Carroll. These included a sum of €111,000, which passed through the account in 2006.

But by 2007 the money going into the account had increased to €1.13m and there was another €500,000 moved through the account up to the end of September 2008.

Another lodgement showed that €854,000 deposited into Thomas Carroll's credit union account had been transferred from Toma Carroll's account.

Judge Bidder described Toma Carroll as an "intelligent and capable young woman who should have been content to follow your chosen career in the law".

"It is to a great extent your father's fault that you are in the position that you are, but you are old enough, and were old enough during the course of this conspiracy, to be able to take decisions yourself and you cannot shuttle off all responsibility so easily on to your father's shoulders," the judge said.

"I simply do not believe, and indeed it has not been pressed on your behalf, what you told the probation service, namely that at no time did you share in the proceeds of the prostitution business."

South Africa's Assets Forfeiture Unit is examining the possibility of seizing three houses in Cape Town owned by Thomas Carroll or his wife -- two in the Strand area of the city and one in Gauteng. The Strand townhouses are estimated to be worth R1.2 million, or around €150,000 each.

Sunday Independent

Former credit union executive sentenced to 24 years: Longest white-collar sentence in Massachusetts.

Date: *Sep 12, 1995*
Words: *744*
Publication: *Business Wire*

BOSTON--(BUSINESS WIRE)--Sept. 12, 1995--Richard D. Mangone, the former president of the Digital Employees Federal Credit Unioin and co-founder of the now-defunct Barnstable Community Federal Credit Union ("BCCU") has been sentenced to prison for 24 years, without parole.

This is the longest federal sentence ever given in a white collar case in Massachusetts. Mangone was also ordered to pay over $41 million in restitution, to repay the amounts lost by the two credit unions he defrauded. Mangone was a fugitive for 18 months until Aug. 29, 1995, when he surrendered to authorities.

U.S. Attorney Donald K. Stern announced that Richard D. Mangone, 51, formerly living at 273 River St., Norwell, Mass., was sentenced today on 22 counts of conspiracy, bank fraud, unlawful receipt by credit union officer and money laundering. Mangone was convicted on July 8, 1993, after a seven week trial on an indictment charging that he used his positions at the credit unions to commit massive real estate frauds, along with three other men.

In sentencing Mangone today, Judge Young referred to what he termed the "egregiousness" and "evilness" of Mangone's conduct. Judge young further commented, "Mr. Mangone, you've ruined people's lives, lots of lives, people you don't even know. Being sorry to these various financial institutions isn't the half of it."

U.S. Attorney Stern stated that Mangone's sentence is the longest federal sentence handed down for a white-collar crime in Massachusetts. Stern commented, "Richard Mangone justly deserves the long sentence meted out by the court today. Mangone's contempt for the Digital Credit Union depositors and the banking industry was reflected in his bragging that he was able to use the Barnstable Credit Union as his own personal "piggy bank." Now all four of the principals, and others who assisted their schemes, are paying the price for flagrantly disregarding the law."

Stern added, "BCCU represents one of the largest credit union frauds in history, with losses in excess of $40 million. In the course of feeding his own greed and lifestyle, Mangone placed at risk the life savings of thousands of innocent depositors and caused the collapse of BCCU."

Mangone was originally scheduled to appear for sentencing before U.S. District Judge William G. Young on Feb. 15, 1994, but fled four days before the hearing. His failure to

appear earned Mangone a place on the U.S. Marshals' Most Wanted List. The Marshals Service and the FBI aggressively pursued Mangone and were closing in when he surrendered to federal authorities in Bowling Green, Ky., on Aug. 29 and was returned to Massachusetts.

Mangone's three co-defendants were also convicted at trial. Former attorney Robert Cohen was sentenced to 10 years in prison; former Cape Cod developer James K. Smith was sentenced to 15 years; and former North Shore real estate investor Ambrose L. Devaney was sentenced to three years. All three are currently serving their sentences in federal prison.

The convictions stem from fraudulent schemes to obtain real estate loans from BCCU, previously operating at Hyannis, Mass., and the Digital Credit Union, located in Maynard, Mass. From 1985 until BCCU was declared insolvent and placed under conservatorship by the National Credit Union Administration ("NCUA") in March of 1991, Mangone and his co-conspirators created various real estate trusts with names of straw borrowers in order to obtain multi-million dollar loans for purported real estate developments on Cape Cod and in Rhode Island and Maine. They used fraudulent certificates of trust beneficial interests, phony purchase and sale agreements, and bogus financial statements to defraud the credit unions and mislead federal examiners.

Stern said that Mangone is the seventh person sentenced in connection with the collapse of BCCU. In addition to Mangone, Cohen, Smith and Devaney, three others having lesser roles in the fraudulent schemes have been convicted and sentenced. Stern also noted that his office filed charges of conspiracy and fraud against two additional former officials of BCCU on Aug. 31, and those charges are pending. The investigation is continuing.

The criminal fraud investigation was conducted by agents of the Federal Bureau of Investigation and the Internal Revenue Service. Assistance was also provided by the National Credit Union Administration. The apprehension of Mangone resulted from the coordinated efforts of the U.S. Marshal Service and the FBI. The case was prosecuted by Assistant U.S. Attorneys Paul G. Levenson and Victor A. Wild of Stern's Economic Crimes Unit.

CONTACT: U.S. Department of Justice

Former credit union president get 5 years for money laundering

BEAUMONT, Texas - The former President of the Orange County Employees Federal Credit Union was sentenced to federal prison for money laundering in the Eastern District of Texas, announced U.S. Attorney John M. Bales today.

Sandra H. Cooper, 56, of Orange, Texas, pleaded guilty on Feb. 28, 2011, to money laundering and was sentenced to 63 months in federal prison today by U.S. District Judge Marcia Crone. Cooper was also ordered to pay restitution in the amount of $1,178,340.00.

According to information presented in court, Cooper, the President and Treasurer of the Orange County Employees Federal Credit Union, embezzled approximately $1,164,340 of credit union funds over a four and half year period. Cooper was indicted by a federal grand jury on Dec. 1, 2010.

The credit union, which had just two employees, was housed in the administration building adjacent to the Orange County courthouse. The deposits of the credit union customers were insured by the National Credit Union Administration Board, a federal agency similar to the Federal Deposit Insurance Corporation, which determined in June, 2010, that the credit union was insolvent and arranged a transfer of customer accounts to the Sabine Federal Credit Union.

Cooper must surrender to the U.S. Marshals Service on July 8, 2011.

This case is being investigated by the Criminal Investigations Division, Internal Revenue Service and prosecuted by Assistant U.S. Attorney Robert L. Rawls.

De-risking trends at big banks affect credit unions

By: Jennifer Morrison, VP, Senior Risk Manager

"De-risking" was a theme at the recently held Association of Certified Anti-Money Laundering Specialists (ACAMS) 12th Annual AML & Financial Crime Conference. According to a panel of compliance and law enforcement officials at the convention, large banks are shedding their "good" customers in an effort to reduce the bank's overall risk profile (de-risking), even if the business line or customer is or was otherwise profitable. Once released from big banks, these riskier customers end up at the doors of small banks and credit unions. These riskier customers assume small banks and credit unions are unsophisticated to the regulatory burdens they bring with them.

De-risking by many major banks followed the financial crisis, as federal agencies and regulators held financial institutions accountable through the issuance of regulatory actions, penalties, and fines. Big banks took notice and over time determined it was more cost efficient to shed riskier customers than to hire the compliance staff needed to track their transactions.

There are three main BSA/AML areas where larger banks are de-risking. As such, it's important for Credit unions to be aware of the scenarios where de-risking is prevalent. The first area is Money Services Businesses or MSBs. In July 2011, FinCEN released updated definitions of MSBs (76 FR 43585-43597). As a result, larger banks are dropping MSBs from their customer base largely due to the expense associated with the level of regulatory scrutiny required when serving these customers.

Credit unions may encounter an MSB either as a "check casher" or as a "money transmitter." Be aware that an administrator or exchanger of virtual currency is also an MSB. If you have a member that is an MSB, the minimum due diligence steps per FinCEN and federal agency guidance is as follows:

- The MSB must be registered with FinCEN and in compliance with any state-based licensing.
- Opening and maintaining any account with an MSB must include new member due diligence.
- Conduct a risk assessment of the MSB. The assessment should include the products and services offered by the MSB, markets served, anticipated account activity, and purpose of the account.

If the MSB is a "higher risk" MSB (see the ***Bank Secrecy Act/Anti-Money Laundering Examination Manual***), the credit union must additionally review the MSB's AML program, review the MSB's BSA/AML independent review, conduct on-site visits, review the MSB's written procedures, review management and termination practices for the MSB, and review the written employee screening practices for the MSB. This is a lot of work and expense. It all must be documented and available for your examiner and independent review. With the additional monitoring required of the member's accounts, servicing an MSB is not a part-time job for staff performing BSA duties among other responsibilities. It is also not for credit unions with a low tolerance for risk.

Secondly, larger banks are also moving away from correspondent banking. Serving business clients who provide financial services to their customers makes it difficult for any financial institution to "know" their customers' customers or in the case of credit unions, their members' members. Money laundering is increasingly "borderless." Do not assume that money laundering is confined to the states bordering Mexico and the coastal states. While "funnel banking" or the use of third-party couriers to transport U.S. dollars from Mexico to U.S. banks and ATMs is prevalent, federal officials at the conference confirmed for the audience that couriers are now heading as far north as Chicago. Money laundering is increasingly observed by law enforcement, for example, involving such things as the purchase of distressed real estate, with anecdotal

evidence that entire city blocks in distressed areas of major metropolitan areas are being purchased for cash with drug money and funds derived from crime. Money laundering is also prevalent in the sale of fungible items, such as appliances, used cars, furniture, and other items you might see on Craigslist, for example. Given the rise in "borderless" money laundering, are you prepared and staffed to know your members' members?

Finally, larger banks are moving away from providing services to Third-Party Payment Processors (TPPPs). A TPPP is an entity that processes payments on behalf of its clients or as part of their business enterprise. TPPPs typically use remote deposit capture and/or originate ACH on behalf of their clients. Examples of TPPPs include a local CPA or payroll preparation firm that files taxes on behalf of their clients. TPPPs also include law firms who conduct title work, transmitting payments to realtors, mortgage brokers, and for mortgage payoffs. But TPPPs may include telemarketers, front companies for illegal gambling operations, and of course, front companies for drug traffickers. Again assuming smaller banks and credit unions lack the headcount or sophistication to do the expanded due diligence required, TPPPs may seek out relationships with smaller institutions. Re-visiting the "know your member" requirements fundamental to BSA, conducting due diligence just on the TPPP is not sufficient. You must conduct expanded due diligence in order to form an opinion regarding the risk embedded in your TPPP member's clients. You must determine the nature of the TPPP's clients, the purpose of the payments, set sufficient limits for the TPPP's activities, and monitor the accounts, including returns, filing a SAR whenever appropriate.

In closing, as one of the presenters at the at the ACAMS convention stressed, we need to learn from mistakes made by other financial institutions and avoid "page one risk" (i.e. keeping your credit union out of the local newspaper, as well as social media, industry journals, etc.). Learn as much as you can from Enforcement Actions as well as from actions taken by the Federal agencies and regulatory bodies. Have a compliance point of view that adds value to your credit union. Understand and reflect the risk tolerance of your credit union in your decision-making, and do not be afraid to turn away prospective members when their activities are not in alignment with risk tolerance levels, even if their business would be profitable to your credit union.

Grant Thornton

Reporting Entity Sector Profiles: Casinos Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

Casino industry SIC codes

Code	Description
7011	Hotels and Motels (which include Casino hotels)

Casino industry NAICS codes

Code	Description
71321	Casinos (except Casino Hotels)
72112	Casino Hotels

Using NAICs codes, searches for statistical data on the Casino sector were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Number of establishments in Canada by type and region: December 2012
Casinos (except Casino Hotels) (NAICS 71321)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	22	24	46	50.0%
British Columbia	16	0	16	17.4%
Manitoba	2	0	2	2.2%
New Brunswick	2	0	2	2.2%
Newfoundland and Labrador	0	0	0	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	2	0	2	2.2%
Nunavut	0	0	0	0.0%
Ontario	6	2	8	8.7%
Prince Edward Island	0	0	0	0.0%
Quebec	5	3	8	8.7%
Saskatchewan	7	0	7	7.6%
Yukon Territory	1	0	1	1.1%
CANADA	63	29	92	100%
Percent Distribution	68.5%	31.5%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Casinos (except Casino Hotels) (NAICS71321)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	1	6	14	1
British Columbia	0	3	5	8
Manitoba	0	1	1	0
New Brunswick	0	1	1	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	1	1
Nunavut	0	0	0	0
Ontario	2	0	0	4
Prince Edward Island	0	0	0	0
Quebec	0	2	1	2
Saskatchewan	0	0	6	1
Yukon Territory	0	1	0	0
CANADA	3	14	29	17
Percent Distribution	4.8%	22.2%	46.0%	27.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Casino Hotels (NAICS 72112)

Exclusions

- stand-alone casinos (71321, Casinos (except Casino Hotels)); and
- hotels and motels that provide limited gambling activities, such as slot machines, without a casino on the premises (72111, Hotels (except Casino Hotels) and Motels).

Number of employer establishments by employment size category and region: December 2012 Casino Hotels (NAICS72112)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	0	0	2	1
British Columbia	0	1	2	1
Manitoba	0	0	1	0
New Brunswick	0	0	0	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	0	1	0	0
Prince Edward Island	0	0	0	0
Quebec	0	0	0	0
Saskatchewan	0	0	0	0
Yukon Territory	0	0	0	0
CANADA	0	2	5	2
Percent Distribution	0.0%	22.2%	55.6%	22.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Canada Casinos and Gaming Sector Values: $ billion, 2008-2012

Year	US$ Billion	% Growth
2008	16.2	
2009	16.3	0.6%
2010	16.7	2.4%
2011	17.4	4.3%
2012	17.8	2.1%
CAGR: 2008-2012		2.3%

MarketLine Industry Profile – Casinos & Gaming in Canada – June 2013

Canada Casinos & Gaming Sector Category Segmentation: $ billion, 2012

Category	2012	%
Casinos	9.3	52.1%
Lotteries	4.3	24.4%
Sports betting and related	0.5	2.9%
Other	3.7	20.6%
Total	**17.8**	**100%**

MarketLine Industry Profile – Casinos & Gaming in Canada – June 2013

Canada Casinos & Gaming Sector Value Forecast: $ billion, 2012-2017

Category	2012	%
2012	17.8	2.1%
2013	18.2	2.6%
2014	18.8	3.3%
2015	19.5	3.5%
2016	20.1	3.4%
2017	20.8	3.4%
CAGR 2012-2017		3.2%

MarketLine Industry Profile – Casinos & Gaming in Canada – June 2013

Table 1. Venues

	BC	AB	SK	MB	ON	QC	NB	NS	PE	NL
Population 18+	3,728,596	2,947,425	813,919	964,162	10,654,715	6,452,582	615,007	775,897	116,555	419,523
Bingo Facilities										
Total Bingo Facilities	27	28	15	2	71	501	0	0	0	0
Casinos										
First Nation (On Reserve)	1	5	6	2	2	0	0	0	0	0
Non-First Nation	16	19	2	2	8	4	1	2	2	0
Total Casinos	17	24	8	4	10	4	1	2	2	0
Electronic Gaming Machine (EGM) Venues										
Bars, Lounges, etc. with VLTs	0	968	613	591[2]	0	1,892	260[3]	372[2]	38	397
Bingo Facilities with Slots or VLTs	17	0	0	0	0	23	0	0[3]	0	0
Casinos with Slots	17	24	8	4	10	4	1	2	2	0
Racetracks with Slots or VLTs	0[4]	3	0	1	17	0	0[5]	0	0[6]	0
Total EGM Venues	34	995	621	596	27	1,919	261	374	40	397
Electronic Keno Venues										
Total Electronic Keno Venues	3,792	88	0	904	20	2	0	0	0	0
Horse Racing Venues										
Major Racetracks	3	5	2	1	20	1	1	3	2	1
Minor Racetracks	2	2	2	6	4	5	0	0	0	1
Teletheatres	22	49	5	10	86	5	4	6	0	0
Total Horse Racing Venues	27	56	9	17	110	11	5	9	2	2
Lottery Ticket Outlets										
Total Lottery Ticket Outlets	3,853	2,611	845	901	10,073	8,559	894	1,074	179	977
Player-banked Poker Rooms or Areas										
Days Used per Month	30	30	[illegible]	30	30	30	30	26	19	0
Total Poker Rooms or Areas	12	22	[illegible]	4	9	4	1	2	2	0
Sports Betting Rooms or Areas										
Days Used per Month	0	0	0	0	30	0	0	0	0	0
Total Sports Betting Rooms or Areas	0	0	0	0	2	0	0	0	0	0
Total Venues 2011-12	**3,924**	**3,687**	**1,490**	**1,513**	**10,264**	**10,516**	**1,160**	**1,457**	**221**	**1,376**
Total Venues 2010-11	4,066	3,666	1,475	1,442	10,159	10,651	1,170	1,508	217	1,429
% Change	-3.5	0.6	1.0	4.9	1.0	-1.3	-0.9	-3.4	1.8	-3.7

Total venues 2011-12: 35,608. Total venues 2010-11: 35,783. Overall change: -0.5%. **Note:** *Total Venues 2011-12* may not equal its subtotals because some venues (e.g., keno) are contained within other venues and are therefore not counted twice. Bingo facilities are venues designated for bingo full-time (e.g., bingo association halls). Casinos are permanent, and include those termed 'Aboriginal,' 'charity,' 'commercial,' 'community,' 'destination,' 'exhibition,' 'First Nation', and 'government-run. Horse racing venues are facilities issued at least one permit by the *Canadian Pari-Mutuel Agency* (CPMA) to conduct pari-mutuel betting in fiscal 2011-12. Figures do not include facilities issued permits that did not ultimately conduct any pari-mutuel activity during the period that the permits were valid for. *Major racetracks* are those that held 15 or more live days of racing in 2011-12; *minor racetracks* are those that held fewer than 15. Player-banked poker (sports betting) rooms or areas are those in a gaming venue where player-banked poker (sports betting) took place at least once per month. The rooms or areas could have been used for player-banked poker (sports betting) only, or for player-banked poker (sports betting) and other purposes at different times (e.g., meetings, other gaming activities). *Days used per month* may be estimates only.

Table 7. Total Government-operated Gaming Revenue

(Revenue after prizes paid, before expenses deducted)

	BC	AB	SK	MB	ON	QC	NB	NS	PE	NL
Population 18+	3,728,596	2,947,425	813,919	964,162	10,654,715	6,452,582	615,007	775,897	116,555	419,523
Bingo										
Total Bingo Revenue	228,135,000	12,400,000[1]	0[2]	3,509,000	24,233,000	15,862,000	0	0	0	0
Casinos										
Total Casino Revenue	1,350,749,000	1,175,293,000[1]	372,875,000	267,055,000[3]	1,590,375,000[4]	785,931,000	Unavailable	75,304,000	12,776,000	0
Electronic Gaming Machines (EGMs)										
Slots or VLTs at Bingo Facilities	193,017,000	0	0	0	0	0[5]	0	0	0	0
Slots at Casinos	947,687,000	1,175,293,000	352,698,000	241,595,000[3]	1,139,680,000	601,311,000	Unavailable	64,025,000	11,961,000	0
Slots at Racetracks	0	45,853,000	0	0	1,734,229,000	0	0	0	0	0
VLTs at Bars, Lounges, etc.	0	593,795,000	226,425,000	321,089,000[3]	0	997,955,000	133,833,000[6]	137,200,000[6]	17,392,000	122,677,000
VLTs at Racetracks	0	0	0	6,716,000	0	0	0	0	0	0
Total EGM Revenue	1,140,704,000	1,814,941,000	579,123,000	569,400,000	2,873,909,000	1,599,230,000	133,833,000	201,225,000	29,353,000	122,677,000
Internet Gaming										
Lottery Tickets	11,386,000	0	0	0	0	0	1,047,000	1,553,000	207,000	925,000
Other	37,351,000	0	0	0	0	Unavailable	731,000	1,125,000	120,000	868,000
Total Internet Gaming Revenue	48,737,000	0	0	0	0	0	1,778,000	2,678,000	327,000	1,793,000
Lottery Tickets										
Internet	11,386,000	0	0	0	0	0	1,047,000	1,553,000	207,000	925,000
Other	431,890,000	363,360,000	91,553,000	103,239,000	1,461,547,000	858,735,000	72,280,000	87,196,000	14,274,000	86,620,000
Total Lottery Ticket Revenue	443,276,000	363,360,000	91,553,000	103,239,000	1,461,547,000	858,735,000	73,327,000	88,749,000	14,481,000	87,545,000
Total Revenue 2011-12	**2,059,511,000**	**2,190,701,000**	**690,853,000**	**701,608,000**	**4,810,384,000**[7]	**2,658,483,000**	**207,891,000**[8]	**302,378,000**	**44,769,000**	**211,090,000**
Total Revenue 2010-11	2,026,391,000	2,136,315,000	687,630,000	702,611,000	4,907,296,000	2,686,297,000	246,166,000	310,298,000	43,689,000	209,714,000
% Change	1.6	2.5	0.5	-0.1	-2.0	-1.0	N/A	-2.6	2.5	0.7

Total revenue 2011-12: $13,877,668,000. Total revenue 2010-11: $13,924,607,000 (restated to exclude casino revenue in New Brunswick so that *Total Revenue 2010-11* can be compared to *Total Revenue 2011-12*). Overall change: -0.3%. **Note:** Revenue measured as wagers less prize payouts, before operating expenses deducted. Figures rounded off to the nearest thousand. *Total Revenue 2011-12* may not equal its subtotals due to overlap between categories. For example, *Total Casino Revenue* includes revenue from casino slot machines, which also appears in *Slots at Casinos* under *Electronic Gaming Machines (EGMs)*.

Appendix B: Case examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Canada: Money laundering thrives at casinos. The Vancouver Sun, August 16, 2010.
2. British Columbia casinos violate money laundering laws. Maple Gambling, March 1, 2012.
3. When it comes to casinos, natives feel they're got game. The Globe and Mail, March 6, 2013.
4. Casino loophole lets criminals launder cash, RCMP fear. CBC News, May 20, 2008.
5. Panelists discuss the implications of Aboriginal casino gaming in Southern Alberta. Research reveals – an update on gambling research in Alberta, February/March 2006.
6. Congress needs to think twice before banning internet gaming. CQ News, February 12, 2014.
7. Why bitcoin has a firm foothold in the online gambling world. August 18, 2013.
8. Lurid testimony undermines triad chief's battle to stay in Canada. South China Morning Post, March 2, 2013.
9. Carson Yeung jailed for six years after tip-off triggered money-laundering probe. South China Morning Post, March 7, 2014.
10. How China's filthy rich use Macau to lander their money. Business Insider, November 11, 2013.
11. Junkets 'encourage money laundering': Wiki cables. Macau Daily Times, August 28, 2011.
12. Casino money laundering suspicious cases soar. http://willcocks.blogspot.ca, January 11, 2011.
13. The gambling machines helping drug dealers 'turn dirty money clean'. The Guardian, November 8, 2013.
14. Are Chinese laundries thriving in casinos? Financial Crime Asia, March 21, 2013.

August 16th, 2010

CANADA: MONEY LAUNDERING THRIVES AT CASINOS

by The Vancouver Sun

Money laundering by organized crime groups is rampant at Canadian casinos but police are essentially doing nothing to combat it, according to an internal RCMP report.

"Since 2003, FINTRAC (the Financial Transactions and Reports Analysis Centre of Canada) has sent several disclosure reports to the RCMP on suspicious transactions involving casinos throughout Canada, with amounts totalling over $40 million," the 2009 report states.

"Anecdotally, police managers have suggested that, because of other priorities and a lack of resources, at this time, nothing is being done to investigate these situations."

Sgt. Dave Gray, of the B.C. RCMP's integrated proceeds of crime unit, acknowledged Wednesday that not a single person has been charged with money laundering at B.C.'s casinos in recent memory.

"If we had more resources, then we could perhaps set broader priorities or conduct more investigations," he said in an interview.

"That goes without saying. We could definitely use more resources."

However, Gray said the lack of casino-related charges is also due to police focusing on more "target-rich" areas -- such as currency seizures at the border -- where it is easier to prove criminal intent.

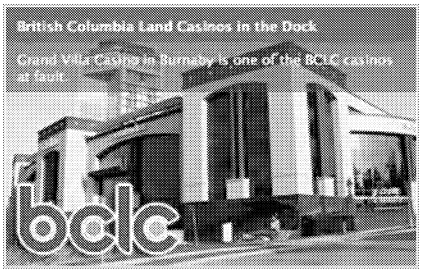
The internal RCMP report, obtained by the Vancouver Sun through the Access to Information Act, states "organized crime is prevalent in casinos at several levels," including money laundering and loansharking, and that casinos provide several opportunities for criminals to make illegally earned cash appear legitimate.

For example, criminals have been known to approach people after a big win and offer to buy their casino cheque for 105% of its face value.

The internal RCMP report notes many casinos now have self-serve kiosks where patrons can exchange winning tickets for cash, allowing launderers to operate without having to deal with a human cashier.

Article published on 1 March 2012

British Columbia Casinos Violate Money Laundering Laws



In Canada, a handful of **British Columbia land casinos** have been found to be in violation of rules and procedures aimed at vetting players who bring large amounts of cash to gamble, with the aim of preventing money laundering.

The violations are of the laws aimed at detecting money laundering, particularly money that could potentially be used to fund terrorist operations. The specific allegations are that the BC land casinos - which are operated by the British Columbia Lottery Corporation (BCLC) - failed to collect and record the information on the backgrounds of such patrons.

These violations were exposed by CBC News, which claims to have obtained uncensored and until now unseen documents from 2009 and 2010, after a year-long investigation. These were procured by CBC News through a Freedom of Information request and pertain to audits performed on three named casinos. One of the casinos is Grand Villa Casino in Burnaby.

An audit carried out by the British Columbia Gaming Policy and Enforcement Branch recorded that nine large cash transactions in a single month did not mention sufficient details of the patrons as required under the federal Proceeds of Crime Money Laundering and Terrorism Financing Act.

The backgrounds of the patrons were simply entered as "self-employed" or "business owner". The audit points out that under the Act, land casinos in British Columbia have to obtain complete details of the patron's principle business or occupation.

CBC News also reported that BCLC has been fined $700,000 by the Financial Transactions Reports Analysis Centre of Canada, for non-compliance of anti-money laundering measures. However, BCLC has appealed against the fine.

British Columbia Land Casinos Respond to Allegations

Bryon Hodgkin, the director of operation compliance at BCLC, has responded to the allegations. He claims that the casinos are required only to collect the information and file a report if they observe that the player is behaving in a suspicious manner.

> Hodgkin said that the information recording process has been tightened to take care of the audit remarks. Specific examples given by him included training of over 5,200 personnel and appointing investigators to check on the records

will be flagged if a generic entry is made.

However, the BCLC response has not satisfied former Crown prosecutor and now gambling critic, Sandy Garossino.

She says that it is a case of putting revenue ahead of national safety without understanding the serious implications of the laxness. Garossino claims that casinos in Las Vegas do not function in this irresponsible manner. "Let's get an audit of B.C. Lottery Corporation and the Gaming Policy and Enforcement Branch because this is just not good enough," she demanded.

Add Comment

Be the first to comment on this article!

THE GLOBE AND MAIL

When it comes to casinos, natives feel they've got game

WENDY STUECK
VANCOUVER — The Globe and Mail
Published Wednesday, Mar. 06 2013, 10:55 PM EST
Last updated Wednesday, Mar. 06 2013, 11:34 PM EST

Part of The Big Gamble [http://tgam.ca/biggamble], a series examining British Columbia's complicated relationship with casinos.

Given the track record of recent casino proposals in British Columbia, it might seem the appetite for such projects has run its course.

Vancouver nixed an expanded casino in 2011. Surrey voted down a $100-million casino complex in January. Despite those rebuffs, Joe Hall looks around the province and sees open arms.

More Related to this Story

- THE BIG GAMBLE B.C. crimes linked to gambling addiction
- MGM sells massive casino plan with a promise of 10, 000 jobs
- ADDICTION Seeking out the ghosts at the slot machine

That's because he's looking at the terrain from his viewpoint as chairman of the British Columbia First Nations Gaming Initiative, a group set up to push for a bigger native role in the provincial gambling sector. Having spent the past couple of years trying – and failing – to persuade the province to change its policies, the first-nations gambling committee said it's ready to act on its own, by setting up gambling operations on reserve land and risking potential consequences, including possible legal action by B.C. or Ottawa.

Unlike other provinces, including Manitoba and Alberta, B.C. has not developed policies to share gambling revenue with natives.

"The province and, to some degree, the federal government just don't seem to be interested in doing it the easy way," Mr. Hall said.

B.C. first-nation groups have been lobbying for a share of gambling revenue since at least 1993. Plans for a provincial First Nations Gaming Commission got under way in 2010. Mr. Hall expects the group to be formalized and commissioners named this year.

To date, the B.C. government has declined to change course, saying the gambling sector is already close to saturation. The only native-owned casino in B.C. is part of the St. Eugene Resort near Cranbrook.

"This is not a business where, if you build it they will come," said Rich Coleman, minister responsible for gambling. "Some people think that's the case but it really isn't; you have to have it sized to the marketplace."

First nations understand the concept of market saturation, Mr. Hall retorts. That's why they were angered by the proposed casino in Surrey – which, had it been approved, would have gone up near where the Semiahmoo First Nation was mulling a casino development of its own.

"It was on their [Semiahmoo Nation] traditional territory, they hadn't been consulted and it would have had a direct impact on them. And they had spoken about a casino years ago and really made no progress with the provincial government," Mr. Hall said.

The committee is looking at sites in areas including Vancouver Island and the Okanagan. As for capital, Mr. Hall said the group has that lined up as well, in the form of partners willing to invest.

In Canada, 15 native-owned casinos operate under various provincial regimes, ranging from Ontario's centralized model – natives share revenue from the Casino Rama operation near Orillia – to ones that feature several casinos, as in Saskatchewan.

There are pros and cons to every model but all – except B.C. – feature revenue-sharing, said Yale Belanger, an associate professor of native American studies at the University of Lethbridge who has written extensively on native gambling.

As to whether casinos have delivered the economic benefits first nations hoped for, results are mixed.

Management fees and debt-servicing costs take a big chunk of profits. So do provincial governments. Alberta, for example, takes a 30-per-cent cut of revenues generated by native casinos – a percentage that Dr. Belanger maintains should be reduced.

"Even though there are dollars now circulating in these [aboriginal] communities, there's a substantial portion that should be making it to those communities that isn't," Dr. Belanger said.

The location of B.C. first nations near or in sizable urban centres in the Lower Mainland, the Okanagan and elsewhere in the province would suggest there is potential for profitable native-owned casinos, he said. But the political terrain is less inviting.

"B.C. in terms of its lack of response is indicating that first nations don't fit into their gambling plans," Dr. Belanger said.

Mr. Hall, meanwhile, said his committee has been talking to counterparts in other provinces to learn from their experiences in finding operators, building facilities and setting up sound financial and management systems.

"We have the luxury of someone else walking through all those spiderwebs and maybe clearing a bit of a path for us."

With a report from Justine Hunter in Victoria

Casino loophole lets criminals launder cash, RCMP fear

CBC News Posted: May 20, 2008 6:05 AM ET Last Updated: May 20, 2008 6:14 AM ET

An RCMP probe into a southern Ontario drug trafficking ring has exposed a loophole in the province's casino system that police fear criminals are exploiting in a bid to launder the proceeds of crime.

Called Project Ozzi, the 2004 RCMP investigation broke up a drug trafficking ring involving cocaine and ecstasy in the Toronto and Kitchener areas.

RELATED STORY: CBC News goes inside two Ontario casinos to test how easy it is to launder money and to see who is watching.

RCMP investigator Cpl. Joe Peel says suspects linked to the ring were frequent players at Casino Rama, outside of Orillia, Ont., and Mohawk Racetrack, west of Toronto. They would play as much as twice a day, often depositing $9,000 into the slot machines each time, said Peel.

"They would go in, under the threshold of $10,000, play various machines and then, at some point, cash out, get the little stubs from the machines … and then ask for a cheque," said Peel, who is with the force's proceeds of crime section.

Peel said the players were careful to make sure most transactions fell below $10,000 — the amount that's supposed to set off alarm bells among casino staff. Under provincial and federal laws, casinos are required to report cash transactions of $10,000 or higher to the federal agency that monitors suspicious movement of money — the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Peel said members of the organization would then deposit the official casino cheques into bank accounts.

"They were trying to legitimize … trying to clean or cleanse the money … is the best way to put it," said Peel. "[Take] the dirty money from the drugs, [gamble it] through the casino … get a cheque and then put it in a bank account. That was the process."

"The process of laundering the money doesn't always rely on winning. It can be just playing it and then checking out. Actually getting a cheque from that institution," he said.

Plea deal with ringleader

Peel said he suspected an apparent casino connection after a 2005 bail hearing for Lenard Ro, the man later convicted of leading the Toronto-Kitchener drug ring. At the hearing, Ro's mother told the court much of her

family's cash came from casino winnings — more than $100,000 for one month alone. She brought along casino receipts as proof, telling the court she was a very successful gambler.

Peel said after learning of that testimony, he was struck by how simple it would be to launder money through slot machines.

"It seemed too easy, to launder money through the casino. Really, it bothered me at that point, how easy it was," said Peel. He said he suspected people linked to Ro's organization had funnelled anywhere from $3 million to $5 million through casinos to get the official cheques.

In an e-mail to CBC News, Ontario Lottery and Gaming Corporation (OLG) said their transaction records show the amount of money issued by casino cheque to people linked to Ro's organization is "far lower" than the RCMP estimation of $3 million to $5 million. The e-mail arrived late Friday, even though the organization has been aware of the story for several weeks.

RCMP later charged Ro's mother, brother and father with money laundering, but the charges were dropped against the three family members when Ro struck a plea bargain and pleaded guilty to masterminding a drug and money laundering operation.

The CBC tried to reach Ro but his lawyer did not return phone calls. Messages left for his mother were not returned.

OLG told the CBC that Ro's mother appeared to be a good customer and didn't fit the profile of money launderer.

RCMP warned to back off

Peel said when he approached OLG about possible money laundering at casinos, the organization's vice-president of security, Mike Sharland, told him to back off. Peel said he was shocked by Sharland's response.

In 2007, Sharland was the subject of a separate Toronto police investigation into allegations of obstruction into a criminal investigation at OLG concerning an Ontario man who was duped out of his winning lottery ticket. Police found no evidence to indicate Sharland interfered with the criminal probe, but did conclude the secondment of a senior OPP officer to OLG "did create a conflict of interest." Shortly after the report was issued, the OPP decided to stop seconding its officers to head security at OLG. Sharland retired from the OPP last March, and from OLG four months later.

"I didn't record our conversation, but basically, [I] was told to look somewhere else and get off his turf, that sort of thing," said Peel. "I didn't get very good vibes from him. Let's put it that way."

Sharland, who was also pulling double duty as a serving OPP chief superintendent during the time he worked as the head of OLG's security, told CBC News he couldn't recall the conversation.

"All the time that I was either at the AGCO [Alcohol and Gaming Commission of Ontario] or OLG, we always co-operated fully with any outside police agencies," he said.

Peel says he doesn't know the extent of money laundering in the province's casinos, but says the loophole shows the potential for greater problems.

"I would hope it was an isolated incident. I doubt it. I'm sure many other criminals out there know as much as Lenard Ro and are doing the same thing," said Peel.

With files from Dave Seglins

VOLUME 5 • ISSUE 3
FEBRUARY / MARCH 2006

research reveals...

an update on gambling research in ALBERTA

About The Alberta Gaming Research Institute

The Alberta Gaming Research Institute is a consortium of the Universities of Alberta, Calgary, and Lethbridge. Its primary purpose is to support and promote research into gaming and gambling in the province. The Institute's identified research domains include bio-psychological and health care, socio-cultural, economic, and government and industry policy and practice. The Institute aims to achieve international recognition in gaming-related research. It is coordinated by a Board of Directors working in collaboration with the Alberta Gaming Research Council. The Institute is funded by the Alberta government through the Alberta Lottery Fund.

OUR MISSION:

To significantly improve Albertans' knowledge of how gambling affects society

Your comments and queries are welcome either by e-mail abgaming@ualberta.ca or phone 780.492.2856.

Panelists discuss the implications of Aboriginal casino gaming in Southern Alberta

by Rhys Stevens

ON NOVEMBER 4TH, 2005, a group of academics and community representatives from Southern Alberta presented their insights regarding the development of casinos on First Nation reserves at a forum entitled *Aboriginal Casinos: Who's Cashing In? Panel Presentation and Public Discussion*. The meeting was sponsored by the Royal Society of Canada in conjunction with The University of Lethbridge and was well-attended by members of the university community, City of Lethbridge delegates, First Nations leaders, and local citizens.

Aboriginal gaming is sometimes called the "new buffalo" by casino supporters.

In his opening remarks, session moderator and Lethbridge Herald Managing Editor Doyle MacKinnon noted that there are a myriad of "complex social and economic issues" embedded in the topic. He also contextualized the issue by informing the audience that the Province of Alberta is considering casino applications from seven First Nation applicants and that there could potentially be three casinos operating by the end of 2006. After summarizing the status of Aboriginal casinos in other Canadian provinces, MacKinnon introduced panel participants Dr. Yale Belanger (Department of Native American Studies, U. of Lethbridge), Dr. Rob Williams (School of Health Sciences, U. of Lethbridge), Ms. Phyllis Daychief (Lethbridge Community College) and Mr. Chris Shade (Former Chief, Blood Tribe).

ALBERTA GAMING RESEARCH INSTITUTE

Photo credit: Bernie Wirzba, CRDC, University of Lethbridge

Examining the origins of Aboriginal gaming in Canada [Belanger]

In his remarks, Dr. Yale Belanger set the stage for the three following presentations as he described the origins of Aboriginal gaming in Canada. Belanger's scholarly interest in casino gambling relates to how First Nations communities have attempted to employ them as an economic driver for their "nation-building" efforts. The use of gaming as an economic development strategy has had a somewhat turbulent history. The full story is related in a book that he is preparing about the history of Aboriginal gaming in Canada.

The use of Aboriginal gaming as an economic development strategy has had a somewhat turbulent history.

According to Belanger, the country's introduction to Aboriginal gaming can be traced back to 1984 when a Manitoba reserve held a small lottery. This watershed event was soon followed by attempts to introduce additional forms of unregulated gambling such as high-stakes bingos on reserve lands. Perhaps inevitably, such events had a short lifespan as disapproving provincial authorities conducted raids that were designed to snuff out these unlawful activities. Despite this inauspicious debut, strong lobbying efforts by the provinces themselves in the early 1990s were ultimately successful in allowing legalized First Nations gambling to emerge. By the mid-1990s, five casinos with varying levels of Aboriginal involvement were operating and producing significant economic benefits.

River Cree Resort and Casino, Enoch Reserve west of Edmonton (Nov. 2005).

Photo provided by Alana Yinn, Woodbridge Communications

Belanger noted that plans are afoot for several more Aboriginal casinos to be introduced in both Alberta and Saskatchewan. He suggested that it may be difficult to anticipate how economically successful these casinos will be as there is presently very little research on the topic.

Research themes relating to the socio-economic cost and benefits of First Nations casinos [Williams]

Dr. Rob Williams, Professor in the School of Health Sciences and the Lethbridge research coordinator for the Alberta Gaming Research Institute, outlined in his presentation an interpretation of the socio-economic costs and benefits of First Nations casinos. He began by noting that there has been a long cultural history of First Nations gambling in North America for ceremonial, religious, and recreational purposes. There has also been "a different chronology in the evolution of casinos in Canada versus the U.S." and Williams suggested that this may mean that there will possibly be different outcomes.

Based on his review of the scholarly literature on the topic, Williams commented that most U.S.-based tribes have benefited significantly from casino gaming in terms of improved education, employment,

and decreased poverty. Social costs, however, often increased with respect to number of bankruptcies and incidence of crime. Intra-generational tribal divisions were also common regarding whether casinos were desirable to use as an economic development strategy. In Canada, though the amount of published literature has been sparser, Williams suggested that the economic benefits were still evident—most particularly to the First Nations that hosted Internet gambling web sites (e.g., Kahnawake First Nation in Quebec).

The three general themes Williams identified as having emerged from research studies are: 1) that economic benefits are often offset by social costs (e.g., high rates of problem gambling); 2) that there are clear features which differentiate successful and unsuccessful casinos (e.g., local gaming monopoly, proximity to urban centres, "destination-style casinos"), and; 3) that the commercial and micro-level benefits of casinos are evident but there are few macro-level benefits (i.e., casinos do not increase revenue on their own unless revenue is generated by gaming tourists instead of by local residents).

Community gambling survey on the Blood Reserve [Daychief]

A powerful example used by Ms. Phyllis Daychief in her presentation on problem gambling on the Blood Reserve was how residents commonly referred to the bridge leading off reserve as "Bingo Bridge." Daychief is an educator with Lethbridge Community College and an active participant in the community life of the Blood Tribe. She also recently authored a summary report that describes a research project on gambling that was conducted by a women's group from the Reserve.

The gambling project included the development of a survey that was administered to a non-representative sample of several hundred people on the Blood reserve. Based on the results obtained, individuals reported spending $2,000 / year on gambling (four times the Canadian average) and 47% of survey respondents were considered to be "high-risk gamblers" (in comparison to 5% of the general Alberta population). Daychief made a recommendation in her report that members of the reserve acknowledge the community's problem with gambling and that they "take a stand" to deal with it. She ended with the hopeful observation that a "grassroots" women's movement has developed that seeks to minimize the negative social aspects associated with problem gambling.

Determining the viability of a Blood Tribe casino [Shade]

The Blood Tribe was one of the earliest First Nations to lobby the Alberta government to establish a policy on First Nation gaming. As former Chief of the Blood Tribe, panelist Mr. Chris Shade provided his unique perspective regarding the tribal administration's experiences assessing the viability of on-reserve casino gambling. Shade noted that Premier Ralph Klein was an influential supporter of "destination-style" casino development and it was under his government in 2000 that a policy was formally developed. He also pointed to a 1997 study by

Diskin receives New Investigator Award

Kate Diskin was awarded the New Investigator Award "for outstanding research on the treatment of addictive behaviors" at the 11th International Conference on Treatment of Addictive Behaviors (ICTAB-11) in Sante Fe, New Mexico. This award is particularly prestigious as it has been bestowed upon Diskin by one of the most important conferences in the field of addictions. Her Institute-funded dissertation related to the "Effects of a single session of Motivational Intervention on Problem Gambling Behavior" and was co-authored by Dr. David Hodgins. This is the second award received by Diskin for her gambling-related research. She is currently pursuing her Ph.D. in Psychology at the University of Calgary.

2006 conference program finalized

The Institute's 5th Annual Alberta Conference on Gambling Research, "Social and economic costs and benefits of gambling" will be held on Friday, April 21st and Saturday, April 22nd, 2006 at the Banff Park Lodge, Banff, Alberta. Full details, including registration information, featured speakers, and conference program are available on the Institute's website. The conference program has been approved for 12.75 credit hours by the Canadian Problem Gambling Certification Board. <http://www.abgaminginstitute.ualberta.ca/2006_conference.cfm>

the Canadian Tourism Council that the top two Albertan attractions for European travelers were to visit the Rocky Mountains and to experience Aboriginal culture.

After a pre-feasibility study showed little promise for casino gaming on the relatively remote Blood Reserve in the southwestern corner of the province, the tribe explored options to establish a casino closer to an urban centre. A Lethbridge location was ruled out because the market potential was considered only marginal. A Calgary-area location on lands purchased specifically for casino development was also nixed due to the fact that the parcel would be non-contiguous with reserve lands. Over time, the Blood Tribe slowly lost interest in casino gaming development. Shade recalled that his role ultimately became that of advocate for a policy of profit-sharing between *gaming* and *non-gaming* First Nations communities.

Shade suggested that he felt there was currently little community interest in utilizing casino gaming as an economic development strategy. In conclusion, he contended that it would be now be difficult to secure the necessary support of the local community in any such future initiative.

The panel presentation and discussion of Aboriginal casinos was part of the The Royal Society of Canada's series of university forums on "taboo topics." According to the Society, these forums were created "to provide citizens and policy-makers with a locus where thorny issues and taboo topics of national concern can be critically examined, discussed, clarified and summarized, and become a public resource." Additional information about the panel discussion is available from the Society's web site <http://www.rsc.ca/>

Rhys Stevens — Writer
Vickii Williams — Editor
Epigrafix — Design/Layout
Media queries — 780.492.2856

e-mail: abgaming@ualberta.ca p. 780.492.2856

ISSN 1499-2639 (Print)
ISSN 1499-2647 (Online)

Congress Needs to Think Twice Before Banning Internet Gaming | Commentary

672 words
12 February 2014
CQ News
CQTDAY
English

** CQ News **

* Congress Needs to Think Twice Before Banning Internet **Gaming** | Commentary * Congress should tread extremely carefully before it even thinks about banning lawful activity on the Internet.

Congress is being pressed for a sweeping ban on Internet **gaming**. Whether you gamble or not -- and whether you participate in Internet games or not -- it is clear that the prohibition of Internet **gaming** is a bad idea for Americans.

There are many reasons why Congress should not ban Internet **gaming**, but three in particular stand out:

It would block common-sense consumer and online protections for the most vulnerable, including minors.

It would trample on state and individual rights.

It would put Congress in the position of banning technological innovations the public has already widely embraced.

First, a ban would allow an unsafe black market for Internet **gaming** to continue to thrive. By missing the opportunity to regulate a lawful market, Congress would be denying common-sense consumer protections for the estimated 1 million Americans that spend nearly $3 billion every year on illegal and unregulated **gaming** sites that lack important protections such as age verification and geolocation.

Modern technologies exist to block minors from playing, protect those with addictions and ensure games are fair. These technologies have already worked to protect consumers in Europe, **Canada** and the United States; where New Jersey, Delaware and Nevada are already implementing programs for responsible Internet **gaming**. Unlike the billion-dollar black market, these programs provide real consumer protections. A congressional ban on online **gaming** would ensure that millions of Americans are denied these very protections.

Not only do these black-market websites lack consumer protections, but the FBI and other law enforcement professionals say they present a serious risk for **money laundering**, identity theft and other criminal enterprises, including potential terrorism. Under a congressional ban, that billion-dollar black market for Internet **gaming** would continue to thrive, with no protections, no oversight and no regulation.

Furthermore, a congressional ban would prevent regulated Internet **gaming** programs from generating millions in revenue for local priorities such as schools, transportation or public health. It's no surprise that states including California, Pennsylvania and New York are considering their own programs for responsible and regulated Internet **gaming**.

In addition to the states that currently permit Internet **gaming**, there are state lotteries across the nation offering

online options in an effort to meet consumer demand. A congressional ban would stop them in their tracks, cutting off critical sources of state revenue.

Third, a ban would put Congress in the unenviable position of trying to legislate away specific activity on the Internet and popular technological advancements that the public has widely embraced.

Businesses cannot pretend the Internet and online demand do not exist. One need not look further than film, television and music to see that industries must evolve and keep pace with technological advances, or consumers will simply leave them behind. Even major retailers like Blockbuster, Tower Records and Borders learned hard lessons by not embracing online technologies, sending each into bankruptcy.

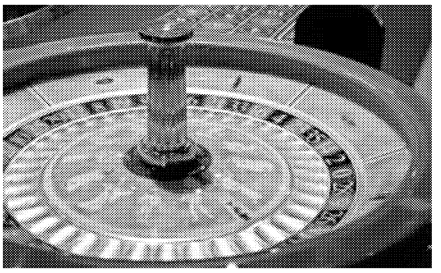
The lesson here is that it is impossible to stand in the way of the Internet; rather, we should embrace and shape these new technologies in ways that are safe for consumers. There is no question whether Americans are **gaming** online. More than a million are. Instead of trying to put the Internet back in a bottle, and ignoring technological and consumer demand, Congress should be focused on making it safe for all Americans.

The effort to ban Internet **gaming** is misguided but it also may draw attention to the real issue: How do we break up the billion-dollar black market to ensure consumer and online protections are in place for the millions of Americans who choose to play games online?

Mary Bono, a U.S. congresswoman from 1998 to 2013, was a member of the House Energy and Commerce Subcommittee on Communications and Technology.

Why bitcoin has a firm foothold in the online gambling world

Daniel Cawrey (@danielcawrey) | Published on August 18, 2013 at 13:58 GMT |Analysis, Bitcoin Gambling, Companies



When it comes to online gambling versus traditional bricks-and-mortar casinos, the internet has the upper hand. Online casinos don't have to hire a bunch of employees, build fancy edifices or wow gamblers with marketing tactics to bring them in.

On the other hand, internet gambling in the United States operates in a grey legal area. Online casino operators get away with it by hosting their sites outside of US borders in places like Costa Rica. It's a profitable business to be in: according to the American Gaming Association, online gaming is a $4-6 billion market. That's precisely why we're seeing an entire industry crop up around bitcoin gambling.

SatoshiDice

No article on gambling and bitcoins would be complete without mention of SatoshiDice. Recently sold for $11.5 million in BTC at the market price for bitcoins at the time, the site was able to avoid the ire of US regulators by blocking American IP addresses from gambling on its site. Yet anyone who was familiar with sending BTC directly to SatoshiDice's bitcoin address or using a VPN to access the site was able to circumvent this.

Unlike some online gambling sites, SatoshiDice shows a listing of gaming transactions. Source:SatoshiDice

It's still unclear who actually bought SatoshiDice. It's another mystery in a long line of bitcoin enigmas back to, well, Satoshi himself. But SatoshiDice has been a catalyst for bitcoin-based gambling it seems, with many SatoshiDice competitors having sprung up since its launch. The reality is that all it takes is some web programming skills and an understanding of bitcoin to be able to set up a BTC-denominated gambling site.

Bitcoins as chips?

When the conventional gambler walks onto a casino floor to play table games, that person has to convert their money into chips in order to play. This element of traditional casinos is a mental component that is likely constructed to make a gambler spend more since chips bear less resemblance to cash. One would think, considering the rise of bitcoin-based gambling, that the same element is in play as well.

It's possible that bitcoin is much more versatile as a method of gambling than that of a traditional casino's usage of chips.

Source: Flickr

Kevin Meehan, one of the proprietors of bitcoin gambling site BitSaloon, sees the similarities with chips. Yet he believes that bitcoins are much more versatile as a unit of wager. "Bitcoins already act like the chips/credits you see on other sites, but inherently have more value since they can immediately be taken off of a wallet on a gambling site and used at places like WordPress, Reddit or other vendors accepting BTC."

Transparency

What's interesting in bitcoin-based gambling sites is how many of them are possibly more transparent than traditional casinos or other online sites. That's because with the block chain being a public ledger, all that an inquisitive gambler would need to do is follow the transactions from a site's bitcoin address. It's no wonder, then, that sites like SatoshiDice show the latest plays being transacted on the site (see above) and claim to be "provably trustworthy". But what

does that actually mean?

Day	Secret / Hash
August 7th 2013	Secret: *For security, today's secret will not be shown until tomorrow* Hash: b3f7620446a795c49aeab6dd0c3de33258d6d7f47897556a6771a41100a0b618e
August 6th 2013	Secret: MSRHbMfKQmLxBiECYeydDUi4cqCkc1oKq28JuRzhyRiH4MEqkESMj3P2p0ygy7 Hash: c6d456e0ccee1a9e0078b06c797d5328f28f8364ec63b0622ffd7a34249466fdcb
August 5th 2013	Secret: gFN1e8k5jxjRK5Bx4obY3ZCHSgM9xMBtLRo0TVg6z1eeRAmkiAUcpOckvv4RuE Hash: f07d1be068357513f5c7a3590a25fd4d0b89e697cf776c3c6f2b693360f85cd
August 4th 2013	Secret: aDhPAVVvb8YBsN7DzesFaY6OoSd7wX9XtpYfxBqk5LxiqGBexFphcrEWXEu04T3 Hash: d8ebd9be5436bb0b183f815116d226f33ad7c730acecb72d61d531a7eb223f45
August 3rd 2013	Secret: fQab0h6CeeFg1oymtzAvDykAu5UXfTepERYdBtBuvzEh9N555PRyDNBXu681i5t Hash: 8f21f316997040d001e73dc53d2cd6e4c26a6534f386d589ca8976023fdc100

BitSaloon's random number generator uses a key combined with a hash to ensure there is no manipulation of odds.

Source: BitSaloon

In addition, some sites even publish how they implement their random number generator. BitSaloon, for example, defines itself as a "provably fair casino" meaning that the site operators cannot modify the outcome of any particular game. This is done by using a secret key for each day, which you can then hash with SHA265. This method means that the site's generator is used uniquely each time, although it's still unknown exactly how that generator calculates its numbers.

Money laundering

But money laundering has in the past found ways to use casinos to create clean money. In April of this year, 34 people and 24 companies wereindicted in connection with a company called Legends Sports. The online sports betting company was allegedly involved in "racketeering, money laundering and illegal gambling." Bitcoin is getting a good deal of scrutiny because authorities view it as a potentially good way to clean illicit money.

PREVIOUS GAMES

GAME TYPE	STARTED	FINISHED	PAY TX	BLOCK	WINNER	COMPLETE	POT
Pick 4	2013-05-09 01:20:37	2013-08-01 01:01:24	7e6d5775	249532	8469	0.0%	0.22770000
Pick 3	2013-05-23 06:33:05	2013-07-22 02:14:01	b81a2890	247851	906	0.7%	0.29700000
Pick 2	2013-04-28 10:32:37	2013-07-21 16:07:00	fc005eb9	247763	ed	2.3%	0.29700000
nelisky	2013-04-04 14:19:27	2013-06-30 06:59:31	d7b939fd	244043	dee8	0.1%	0.54450000
Pick 5	2013-02-14 16:22:06	2013-05-29 23:23:57	480c68c3	361594	77472	0.0%	415.80000000
Pick 3	2013-04-14 10:37:14	2013-05-23 06:33:05	586acad2	237472	783	0.7%	0.29700000
Pick 4	2013-03-12 21:00:22	2013-05-09 01:20:37	ad34dfc6	235234	7101	0.2%	1.09890000
Pick 2	2013-04-14 11:24:33	2013-04-28 10:32:36	8f667d1e	233556	8a	6.6%	0.84150000
Pick 2	2013-03-21 04:37:33	2013-04-14 11:24:33	ed53f2e3	231294	49	5.9%	0.74250000
Pick 3	2013-03-21 06:28:32	2013-04-14 10:37:13	3a641781	231286	a06	2.7%	1.08900000

The Amazing Anonymous Bitcoin Lottery publishes the results of previous games, but the operators of the site wish to remain unknown. Source: TAABL

Similar to the Liberty Reserve case, criminals can put fiat into the system. Then they can trade it around and split it up between bitcoin addresses in a method known as "mixing" to hide the original source. It's possible to trace, but this method makes it harder to follow. Bitcoin gambling could be another layer on top of this, which means regulators will look at bitcoin gambling

operators with a good deal of scrutiny. This is especially true for any bitcoin gambling sites that are operating anonymously, such as the Amazing Anonymous Bitcoin Lottery.

The future of bitcoin gambling

BitBet offers wagers related to all sorts of events, including the future of bitcoin. Source: Bitbet

The concept of bitcoins is still new. The idea of bitcoins and gambling is even newer. "My personal take on it is that people don't view it as real money yet", says Justin Pincar, from BitSaloon. But people seem to enjoy gambling it away. "We have seen people raise their bets based on the amount of time they've spent on the site, which makes sense, as they're building trust that we're legit."

As people find bitcoin more appealing as a currency, they will inevitably find ways to utilize it just like fiat. Gambling is just another aspect of bitcoin legitimizing itself as a real unit of value. Yet this aspect of it will bring more scrutiny to bitcoin from regulators. Online gambling, at least in the US, is something that a lot of people do. It appears that some BTC gambling sites are trying to be fair and focus on their legitimacy. If these sites are located outside of the reach of US regulators, what can really be done? The internet itself is decentralized. So is bitcoin.

What do you think about gambling with bitcoins? Does it need transparency, or is it alright for bitcoin gambling sites to operate anonymously? Let us know in the comments.

South China Morning Post 南華早報

Lurid testimony undermines triad chief's battle to stay in Canada

Saturday, 02 March, 2013, 12:00am
News › World CANADA

Ian Young in Vancouver

Immigration hearing hears Lai Tong Sang ordered murder of Macau's 'Broken Tooth'

Triad leader Lai Tong Sang faces an uphill battle to retain Canadian residency after three days of incriminating testimony at an immigration hearing this week.

It included claims that he ordered the murder of arch-rival "Broken Tooth" Wan Kuok-koi and a top lieutenant.

Immigration officer Jean-Paul Delisle told the hearing in Vancouver that Macau police had told him in 1997 that Lai ordered the killings. The order to kill Wan was not carried out but the hit against senior 14K gangster Shek Wing-cheong was, on May 4, 1997.

Shek and two underlings died when their moving car was surrounded by men on mopeds who riddled it with bullets in broad daylight.

The killing of Shek, a corrupt former Hong Kong policeman and Wan's bodyguard, triggered a dramatic escalation in the 1996-1998 war between Wan's 14K triad and the Wo On Lok gang, said to have been headed by Lai, as they battled for control of the casino junket market.

Wan was released from prison in December after nearly 14 years behind bars.

Delisle's testimony at the deportation hearing is believed to be the first sworn account of Lai's alleged involvement in Shek's killing.

Delisle, the Canadian visa officer in Hong Kong who handled Lai's initial application for permanent Canadian residency in 1994, referred to Shek by his nom de guerre, "Man Cheong".

Delisle was challenged by Lai's lawyer, Peter Chapman, that he was "overstating" the account Macau police had provided of his client's involvement in ordering the killings.

"I do stand by the comment I made about Lai Tong Sang personally ordering the contract," Delisle said, according to the Canadian Press. Delisle said Lai also ordered the murder of another 14K gangster whose identity was not clear.

The immigration review also heard testimony from gang expert Detective James Fisher that the triads were a "blight on society". On Tuesday, the hearing heard from Superintendent Patrick Fogarty, who headed a Canadian wiretapping operation that revealed how Wan's 14K plotted to kill Lai in Vancouver.

> I do stand by the comment I made about Lai Tong Sang personally ordering the contract

The Canadian government is seeking to have Lai's permanent residency revoked on the grounds that he had concealed his membership of a criminal organisation. It is seeking to have his wife, and adult son and two daughters, expelled on the grounds that they had achieved permanent residency on the basis of misrepresentation.

A ruling by immigration board member Geoff Rempel is not expected until July.

Delisle said he handled Lai's initial application for Canadian residency via the Hong Kong consulate under a foreign investment scheme.

Lai withdrew the application amid Delisle's suspicion that he was a triad.

But two years later Lai successfully reapplied through the Los Angeles consulate.

Delisle, who had special responsibility in Hong Kong for dealing with the visa applications of suspected triads, was not informed, and Lai and his family assumed Canadian residency in October 1996.

The blunder was soon revealed in dramatic fashion, when gunmen sprayed Lai's luxury Vancouver home with bullets in July 1997.

Delisle testified that he quickly faxed his bosses an affidavit describing a Macau police unit's account of Lai's involvement in ordering contract killings.

According to the news agency Canadian Press, Delisle said had he been asked by the Los Angeles consulate, he would have told them they were dealing with "a major triad head". It was not clear why it took 16 years for the case to reach a hearing.

Lai, who has not been photographed in public for 15 years, was granted permission join in the hearing via teleconference from Macau, where he is understood to divide his time.

South China Morning Post 南華早報

Carson Yeung jailed for six years after tip-off triggered money-laundering probe

Friday, 07 March, 2014, 12:09pm
News › Hong Kong COURTS

Austin Chiu austin.chiu@scmp.com

A tip-off to police started chain of inquiry that ends in six-year jail term for former hairdresser

An anonymous letter of complaint written in English triggered the investigation that ended with one-time high-flyer Carson Yeung Ka-sing behind bars yesterday.

Police disclosed this as the hairdresser-turned-businessman and owner of English soccer club Birmingham City started a six-year jail term for money-laundering.

Speaking outside District Court, Superintendent Gloria Yu said the letter was received in 2008 - some time after Yeung acquired a 29.9 per cent stake in the club but before he took full control of it in 2009.

JUDGE DOUGLAS YAU

"The law will come down on them with full force"

"We did not start the investigation because Mr Yeung bought the football club," Yu said. "Whether or not the complainant made the report because Mr Yeung bought the shares, you have to ask the complainant."

A source close to the defence team said there would "almost certainly" be an appeal.

Yeung was convicted on Monday of five charges of laundering HK$721 million using five bank accounts at Wing Lung Bank and HSBC between 2001 and 2007. He has 28 days to file an appeal.

The court heard earlier that from 2001, various parties made deposits into the accounts, many for no apparent reason. Some were made by securities firms and a Macau casino, while others were made by unknown parties. Some 437 deposits, totalling more than HK$97 million, were made in cash.

"I find that without his considerable skill in share dealings and connections to the Macau casinos, the laundering could not have gone on for such a long time and on such a large scale," Judge Douglas Yau Tak-hong said in sentencing Yeung. "Maintaining the integrity of the banking system is

of paramount importance if Hong Kong is to remain an international finance centre."

The judge said the six-year prison term was meant to serve as a deterrent and signal to those who exploited the system that "the law will come down on them with full force".

The judge also remarked that deposits made by apparently innocent individuals into Yeung's accounts were "all somewhat connected" to Lin Cheuk-fung and Cheung Chi-tai, who were said by Yeung to be two bosses of casino junket company Neptune Group. The court heard that Cheung was reported by the media to be a local triad gang leader.

Yu said police would examine the judge's remarks carefully to decide whether there was a need to investigate the "possibilities" he had raised.

The prosecution will apply on April 3 to confiscate some of Yeung's assets, about HK$400 million of which have been frozen by a court injunction.

Yeung took over Birmingham City for HK$731 million in 2009 and was arrested in June 2011. He quit all his posts in the club's holding company last month.

How China's Filthy Rich Use Macau To Launder Their Money

Mamta Badkar
Nov. 11, 2013, 2:51 PM

REUTERS/Bobby Yip

A stunning $202 billion in "ill-gotten funds are channeled through Macau each year," according to The Congressional-Executive Commission on China Annual Report 2013.

Diplomatic cables released by Wikileaks claimed that the casino and hospitality sector accounted for over 50% of Macau's GDP but that, "its phenomenal success is based on a formula that facilitates if not encourages money laundering."

And a lot of that money comes from China.

Macau casinos pulled in a record 36.5 billion patacas ($4.57 billion) in revenue in October, largely driven by Chinese visitors.

In 1999, Macau saw 800,000 mainland Chinese tourists. That figure exploded to about 12 million in 2008 and then 17 million in 2012*. In 2012, another 11 million visitors came from Hong Kong and Taiwan.

How exactly does it work?

China only allows 20,000 yuan ($3,200) to be moved out of the Mainland at a time and $50,000 a year. To circumvent that, Chinese high rollers can do one of two things. They can deposit money with junkets in the mainland and use that money in Macau, or they can borrow from junket agents.

If they choose to deposit the money, the junkets, who are basically gaming promoters, ferry money across borders. The gamblers can then use that money in Macau. Once they're done gambling they can take their winnings in U.S. funds or Hong Kong dollars and invest it in property or offshore tax havens.

These junket agents vary from sole proprietorships to publicly listed companies. They help arrange for visas and accommodations, including VIP rooms. They also collect gambling debts.

Frequently, the money that ends up here has come through illegal means, through bribes or embezzlement.

A paper from Jorge A. F. Godinho, at the University of Macau — Faculty of Law explains how junkets play a role in money laundering in Macau.

> "According to the FATF and Asia/Pacific Group on Money Laundering (APG), there are several vulnerabilities regarding promoters, including the fact that their intervention enables the creation of an additional layer which may not contribute to knowing the identity of the players and the source of funds, in addition to the fact that not all jurisdictions regulate gaming promoters and/or their representative offices.
>
> "...Gaming promoters may assist in the transfer of funds to the casinos of Macau. In the case of VIP Baccarat, the amounts involved can be very significant. Moreover, in many cases, there will be no actual transfer of funds, but rather a simple balancing of accounts between credits in mainland China and debits in Macau. This is one of the reasons why the gaming promoter sector is rather developed.
>
> "There is no doubt that this channel can also serve for the movement of funds of an illicit origin, whether coming from corruption, embezzlement of public or private entities, or any other sources. Hence the particular need for rules and procedures for the detection of illegal transfers."

REUTERS/Bobby Yip

A Grease themed slot machine in Macau

Triads

Triads, or Chinese organized crime units, "dominate the junket industry," according to Benjamin Carlson at Foreign Policy.

Since Chinese courts don't recognize or enforce payments on casino debts and since gambling is illegal in China, junkets often rely on triads to collect their debt.

Triads that operate in Macau and around the world, partake in everything from money laundering to drug and human trafficking.

Diplomatic cables released by Wikileaks that date back to 2009 explain how unregulated junkets are:

> "Although they must register and are subject to nominal regulation in Macau, these facilitator organizations allegedly work closely with organized crime groups in mainland China to identify customers and collect debts. Junket operators work directly with Macau casinos to buy gaming chips at discounted rates, allowing players to avoid identification.
>
> "Know-your-customer (KYC) and record-keeping requirements are significantly looser than in other international gaming venues. Government efforts to regulate junket operators in Macau have been aimed at limiting competition, rather than combating illicit activities.
>
> "Oversight of both casinos and junket operators is limited and remains a serious weakness in Macau's AML regime. Periodic tightening of Chinese Individual Visitor Scheme

permit requirements may reflect Chinese government concern about corrupt officials laundering money in Macau."

Another way illicit money finds its way to Macau's casinos is through pawn shops. Visitors buy goods from a pawn shops with a debit card and then sell it back for cash.

Cracking Down

Since the Chinese handover late last year, Beijing has been cracking down on corruption which has included efforts to regulate the gambling industry. In December, some junket operators were arrested.

Last year, Senator John McCain raised concerns about illicit money from Macau making its way into the American political sphere by pointing out that CEO of Las Vegas Sands Corporation, Sheldon Adelson, got his profits from Macau.

Macau is considering implementing a cross-border cash declaration system to restrict money laundering, though no specifics were unveiled.

A real crackdown on money laundering seems to still be a ways away.

**The article was corrected to show that mainland Chinese tourists increased to 17 million in 2012, not 17 billion.*

Junkets 'encourage money laundering': Wiki cables

29/08/2011 21:11:00 Vítor Quintã

'Oversight of both casinos and junket operators is limited and remains a serious weakness,' according to leaked US diplomatic cables

The local gaming sector's dependence on VIP gaming operators, known as junkets, is "a formula that facilitates if not encourages money laundering," according to leaked US diplomatic cables.

A cable titled 'The Macau SAR economy at 10: Even jackpots have consequences' says "oversights of both casinos and junket operators is limited and remains a serious weakness in Macau's AML [Anti-Money Laundering] regime".

Junkets work with local casinos and independently run VIP rooms that accounts for more than half of Macau's gaming revenue, "allowing players to avoid identification," says the document released last week by whistle-blower website WikiLeaks.

"Know-your-customer and record-keeping requirements are significantly looser than in other international gaming venues," the document signed December 2009 states.

The cable was sent from the Consulate General of the US in Hong Kong to the US Department of State. It acknowledges that junkets "must register and are subject to nominal regulation in Macau".

But "Government efforts to regulate junket operators in Macau have been aimed at limiting competition, rather than combating illicit activities," the document stresses.

Junkets "allegedly work closely with organised crime groups in mainland China to identify customers and collect debts," the consulate added.

In 2009 Beijing's tighter policy on visas for Macau slowed visitor arrivals, in what was seen as an attempt to cool down gaming growth.

But the cable claims "periodic tightening of Chinese Individual Visitor Scheme permit requirements may reflect Chinese government concern about corrupt officials laundering money in Macau".

The MSAR Government spokesperson office declined to make any comments.

Corruption woes

"The dream to get rich quick, the huge flows of cash, and the attraction of high-paying jobs in the growing casino sector continues to challenge the

'Periodic tightening of Chinese Individual Visitor Scheme permit requirements may reflect Chinese government concern about

MSAR's ability to combat corruption and illicit financial activity," the document warns.

corrupt officials laundering money in Macau'

Under the subtitle 'Macau Laundry Service' the cable says "massive flows of money and relatively weak controls over financial transactions make Macau a target for those seeking to launder illicit funds".

"Despite rapid progress, particularly with regard to regulation and oversight of Macau's financial sector, weaknesses remain," the US Consulate wrote.

The cable mentions the case of Banco Delta Asia, which was "a useful tool for the North Korean regime to transfer funds related to illicit trade".

The bank is forbidden from doing business with US financial institutions, which effectively prevented it from conducting any foreign currency transaction.

The 2009 cable also recalls the conviction of former secretary for Transport and Public Works, Ao Man Long, to a 28-year prison sentence for corruption and money laundering.

"While applauding the investigation and conviction of Ao, critic's charge that he could not have engaged in corrupt practices for so long without the knowledge of other senior Macau officials," the US Consulate stressed.

The document adds that, following Ao's arrest, "approvals for new construction projects stalled as Macau officials took extra care to avoid the appearance of impropriety" – a view shared by local businessmen, executives and lawmakers.

"Macau's explosive economic growth, a public outreach campaign to encourage reporting, and increased CCAC [Commission against Corruption] resources have led to significant increases of corruption cases in recent years," another cable signed January 2010 says.

Labour tensions

The gaming boom has "fundamentally altered the nature of Macau's economy, bringing increased prosperity but also (...) increasing social tensions," the cable says.

'Many industry observers believe one or more foreign producers of copyrighted content must file lawsuits in Macau to force the antenna companies out of business'

On the one hand the strict quota system that forces companies to hire local workers has increased wages.

"Rising demand for casino workers, however, has led to criticism that Macau's youth are forgoing higher education and training to make easy money as card dealers and croupiers," the US Consulate wrote.

On the other hand "the influx of foreign labour since 2004 has increased social tensions and protests against illegal and foreign workers," the document adds.

"Concerns that foreign labour will supplant local Macanese workers makes labour and immigration policy a sensitive political issue," another cable signed January 2010 says.

The Law for the Employment of Non-Resident Workers, which came into effect on April 2010, requires imported labour to leave the territory for six months before applying for a new work permit with a different employer.

This law would "severely restrict workers' ability to change employers," an October 2009 cable warned.

But four lawmakers said the bill would not sufficiently protect Macau resident worker rights and called for specific caps on imported labour.

"They also stated that real estate developers should receive stiffer punishment for the illegal workers employed by local contractors," the document adds.
"If enacted, such a provision would impact US gaming companies that might occasionally employ local contractors and thousands of migrant workers to complete the various construction projects around Macau," the US Consulate warned.
A December 2009 cable also pans the government's strategy for economic diversification.
"Macau interlocutors note that with limited land, a small labour force, and huge returns on property and gaming investments, there is little incentive for investors to look at more difficult and less lucrative investments in other industries," the document says.
The development of Hengqin Island should "lessen pressure on Macau to diversify its economy within its own borders," the US Consulate wrote.

Antenna piracy

The leaked US diplomatic cables also mention the long-lasting conflict between public antenna companies and Macau Cable TV.
"Piracy of television signals (and much US-origin program content) is rampant," a January 2010 cable says. "The Consulate General continues to raise these issues with Macau officials."
A March 2009 cable had already criticised authorities' "inability to resolve this issue," despite acknowledging that "Macau's outdated copyright law makes it difficult for law enforcement to act against software piracy and control digital/internet IPR infringement".

A new copyright law has remained frozen at the Legislative Assembly since February with lawmakers still waiting for a new version of the draft law.
Last month the Court of Second Instance rejected an injunction filed by Macau Cable TV, even though it acknowledged that "the illegal activity" of public antenna companies was causing financial losses to the concessionaire.
"Many industry observers believe one or more foreign producers of copyrighted content must file lawsuits in Macau to force the antenna companies out of business - or at least disable their ability to sell pirated signals to Macau's households," the cable says.

'Rising demand for casino workers, however, has led to criticism that Macau's youth are forgoing higher education and training to make easy money as card dealers and croupiers'

Water acting

Water conservation initiatives were launched mainly to counter criticism from Zhuhai officials and "perceptions of waste," according to a January 2010 cable, quoting MSAR officials.
While the Guangdong province was experiencing a major drought and Zhuhai was rationing water usage in 2009, the territory launched conservation initiatives such as a water fee rebate programme.
"Macau officials shared that their conservation efforts were in large part politically driven, given that Zhuhai would perceive downstream Macau as 'wasting water' if it did not implement measures," the US Consulate wrote.
Local water conservation initiatives, "although environmentally sound, were mainly announced in reaction to

complaints from Zhuhai officials," the cable emphasises.

"Officials told us these measures were primarily 'for show, to counter perceptions of waste' and that there was no urgent concern over the water supply," the document adds. The conservation efforts could "counter the perception of a wasteful and extravagant Macau".

Despite assurances from mainland China that the territory would not suffer from water supply shortages the US Consulate said the city must reduce its dependence.

"Macau still needs to invest in sea water desalination facilities to secure its long-term water supply. However, because Macau's sea water quality is 'muddy' and therefore harder to treat, the water intake port will have to be further offshore, making the project more expensive," the cable explains.

"Nonetheless, Macau officials say they are investigating it [sea water desalination] as part of a long-term option," the documents reveals.

Paying attention

Paul Willcocks on ending life in Victoria and heading to Copan Ruinas, Honduras, for a year or two, and who knows where after that. Observations on the country, the town, the people and anything else that strikes me. Click here to send me an email. willcocks@gmail.com

TUESDAY, JANUARY 11, 2011

Casino money laundering suspicious cases soar

Criminals love casinos. They're great places for loan sharking and passing counterfeit money.

And even more important for the serious crooks, casinos are the easiest place to launder money.

The CBC used freedom of information requests to learn that millions of dollars in suspicious transactions flowed through two B.C. casinos in three months last year. The casino companies told B.C. Lotteries, but no one passed the information on to police immediately.

These aren't slightly suspicious transactions. In one case, a man entered a New Westminster casino with $1.2 million worth of chips. He didn't place a bet. He just turned them in and took the money in cash.

He told staff he was boarding a flight and was concerned the money might look suspicious. So the casino gave him a letter confirming the money was a casino payout.

It's a classic money-laundering scenario. Crime - drug dealing, robbery, whatever - can produce lots of cash. Banks have to report deposits of more than $10,000 to FINTRAC, a federal agency that fights money laundering and organized crime. Even if money is broken into smaller deposits to come under the limit, a criminal might end up having to explain where all the money came from.

Instead, criminals can buy chips in casinos, cash them in and get a cheque or, in this case, cash with a letter suggesting they were winnings. The money is clean.

In another case uncovered by the CBC, a man entered a Richmond casino with a bag stuffed with $460,000 in $20 bills and bought chips. The casino reported that there was nothing suspicious in the transaction.

All told, there were 90 large transactions worth $8 million in three months.

The RCMP only learned about this after the fact. Insp. Barry Baxter, with the unit that tracks the proceeds of crime, said the police suspect money laundering. "The common person would say this stinks," he said.

Casinos also have to report large transactions to FINTRAC, the federal Financial Transactions and Reports Analysis Centre, and also report to police and the province's Gaming Policy Enforcement Branch. But the reports aren't required for 30 days; a quick first step would be to require immediate reporting to police.

Rich Coleman, the minister responsible for gambling, initially downplayed the reports. He later promised an investigation.

But none of this is surprising.

The government's Gaming Policy and Enforcement Branch 2006 annual report, for example, warned of a crime explosion at casinos, with investigations into offences like loan sharking and money laundering more than doubling in a year.

Last year, it was revealed B.C. Lotteries had been fined $670,000 under federal laws aimed at combating money laundering and terrorism financing. There were more than 1,000 infractions; in eight cases, the most basic information wasn't collected when people walked out of casinos with more than $10,000.

FINTRAC said fines are only imposed for a "persistent, chronic failure to comply with the law."

Despite the warnings, enforcement has been minimal. In 2009, the government shut down the five-year-old specialized police unit created to target gambling-related crime.

And the enforcement branch's just-released annual report for the 2009-10 fiscal year reveals that it opened 635 investigations into money laundering, loan sharking and counterfeit offences in casinos, without laying a single charge.

Again, none of this is surprising. Casinos want to make money. Coleman and B.C. Lotteries are responsible for increasing the number of gamblers in the province, the average amount each one loses and the province's take.

Cracking down on transactions that could be linked to money laundering is a threat to those goals. Casinos fear that asking for information from big gamblers could drive away some of their best customers.

The obvious, and long overdue, first step is end the inherent conflict in having one minister responsible both for promoting gambling losses and fighting crime in casinos.

Footnote: The CBC reported that reports to FINTRAC showed that while the dollar value of suspicious transactions at casinos in other provinces stayed the same or went down in the past year, they tripled in B.C.

theguardian

The gambling machines helping drug dealers 'turn dirty money clean'

Dealers talk to the Guardian about laundering drug money through fixed odds betting terminals in bookies across Britain

Randeep Ramesh, social affairs editor
theguardian.com, Friday 8 November 2013 18.03 GMT

The Gambling Commission admitted in September what has long been privately acknowledged: FOBTs present a 'high inherent money laundering risk'. Photograph: Alamy

Dressed in a grey hoodie and jeans, James, 24, looks like just another lost soul in the high street, shuttling between the six betting shops in an east coast seaside town. It's a weekday morning and if you catch up with him inside a bookmaker, you'll find him peering intently into the green glowing screen of an electronic gambling machine – feeding in £200, "a score at a time".

But this is not a young gambler blowing his meagre wages. James is a drug dealer and his interest in the bookmakers – and the fixed-odds betting terminals (FOBTs) in each shop – is all about laundering money. "That's what turns dirty money clean," he says. Dealers feed their drug money through the machines, losing a little and then cashing out with the

vast majority of their stake, James says. They can then collect a printed ticket showing they have gambled that day – meaning that if stopped by police, they can answer questions about why an apparently unemployed young man carries hundreds of pounds in rolled-up cash.

The FOBTs are probably the single most profitable pieces of property in the town centre's shabby pedestrian precinct. Each machine, according to industry figures, grosses about £900 a week. The 24 FOBTs within a few minutes' walk are worth an estimated £1m a year in profits to the betting industry.

The terminals arrived in Britain in 2001 and were lightly regulated from the outset. Punters in bookmakers found that they could bet £100 every 20 seconds on roulette. The temptation of high-speed, high-stake casino games in the high street proved irresistible: there are now 33,345 FOBTs in the UK.

However, several high-profile cases have exposed a seamier side to the rise of the machines. Earlier this month the Gambling Commission, the industry regulator, fined Coral bookmakers £90,000 in profits it made from one drug dealer who had laundered almost £1m in its shops. Last month the industry regulator also publicly admitted what has long been privately acknowledged: FOBTs present a "high inherent money-laundering risk". In a letter to the industry trade association, the commission warned about "a retail betting model that includes high volumes of cash transactions, particularly where this includes low individual spend and a high level of anonymity... especially where that model also offers (FOBTs)."

What the machines provide is the chance for criminals to convert quickly large sums of money from the real world into virtual cash that can later be converted back into the real thing. There is little official research into the scale and extent of such operations. The 2005 Gambling Act, which regulates the terminals, says one of its primary objectives is "preventing gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime".

However, it has long been obvious to the public that criminals can convert their loot into a clean win on an electronic roulette table. Surveys for the commission show that 40% of the public regularly identify gambling with criminal activity. The industry regulator found one in 14 respondents associated money laundering with gambling.

The Guardian persuaded a number of drug dealers to talk about their criminal pursuits. What was remarkable was that they saw FOBTs as both a nuisance and necessary, trapping "weaker" people into addiction while allowing the "strong" to prosper. All

exchanged tips with fellow dealers on the best ways to launder money; all were surprisingly frank about their methods.

James's strategy is simple: £20 on black, £20 on red and £2 on zero. A press of a button and the wheel spins before the ball lands on red. That's a loss of £2. The money placed on the zero is the only risk James is taking with his cash. If the ball does land on zero, he wins £72.

With no horses to run or dealer to shuffle and just the 20-second spin of an electronic roulette wheel to wait for, it takes a little over a minute for this drug dealer to cash out. James says he knows that unless he gambles at least 40% of the float money he has put in the machine, an alert will pop up on the staff computer warning them of suspicious activity. So he methodically places the same bet to make sure that he has wagered enough.

To ensure that his winnings are not an unlikely round number, he loses some more money on the one-armed bandit. Leaving the tea brought over by the shop manager to go cold, James wanders over to the counter to collect his winnings in the form of a receipt – transforming the money he made from cocaine into apparent gambling winnings. He has lost a little more than £10. "You have to make it realistic," he says. "Bookies get nervous if you come in and just lose the same amount every day. So I vary it a little."

Drug dealers say the reason fixed-odds betting terminals are used is precisely because they are so lightly policed. James is careful not to visit the same shops in a pattern. Handily there are 15 betting shops in the town within walking distance of the main bus routes that snake through the suburbs and along the Thames estuary. "Smart dealers don't drive around here. You are more likely to be stopped by police driving around late at night doing deliveries than if you are taking a bus somewhere into town."

Then there are favoured bookies. Ladbrokes, says James, is useful because you can transfer winnings in the shop to an online gaming account. In William Hill's you can ask for your winnings to be credited directly to your debit card, with the cash landing up in your bank the same day. "Look at my account and I am a very successful punter," he says.

The economics of drug dealing make it cost-effective to pay 5% to 10% to betting shops to launder the illicit profits. James claims to have "about 100K" in his bank account. He sells about 56g (2oz) of ordinary cocaine a week and another 28g of a purer, more expensive version. "Normal customers like teachers, doctors they get the ordinary stuff.

The cleaner gear is for the City boys."

Selling cocaine in 0.8g wraps, James, a dealer, says he turns over about £5,500 of drugs – of which half is profit. Photograph: Andy Rain/EPA

James left school at 16 and worked in shops and restaurants before ending up in the City of London. "That's where I saw people using coke and I was asked if I could get some. I knew some people and I did. Never looked back. How long would it have taken to save £100,000 if I just continued doing admin in a bank?"

Selling cocaine in 0.8g wraps, in a week James turns over about £5,500 of drugs, of which half is profit. "I buy it on tick so you end up carrying a lot of money around. The trade is run by Albanians around here, so it's best to have cash ready if you need to pay it back in a hurry."

Almost all his money is laundered via FOBTs. James calculates he is worth £15,000 a year to the betting industry. "Valued customer," he grins. "I'd say there were about half a dozen of us [dealers] around here using machines. We swap tips – where to go, least crowded, staff not bothered, that sort of thing. You don't want to be recognised too many times."

In opening up to the Guardian, James says there is a risk that bookmakers in the coastal town will tighten up on who enters and who leaves. "Sure, they could stop us, but in the end they want the money.We can hang back for a bit and go somewhere else. Pretty soon they will relax and welcome us all back."

Bookmakers essentially regulate themselves: deciding whether to bar problem gamblers, cal he police over violent behaviour or report crime. As the machines contributed £1.4bn to its bottom line last year, there have been suspicions that the

industry has played down the shadier side of the terminals.

Adrian Parkinson, a former regional machines manager at the Tote, now with the Campaign for Fairer Gambling, said: "Money laundering on FOBTs has been a problem since their introduction. Whether it's cleaning notes from the proceeds of crime or drug dealers legitimising profits, it is well known in the industry that it goes on.

"I raised the issue some years ago at the Tote after being swamped with incidents of money laundering following a series of armed robberies but it's still going on."

Even worse, Parkinson says, the technology is outpacing the law. He says by the end of the year, customers in Coral will be able to transfer any FOBT winnings to their online account. "The staff won't be able to intervene, whatever their suspicions. The industry is riding rough shod over the licensing objectives. Keeping crime out of gambling has to take precedent over profit."

The Association of British Bookmakers said the industry complied fully with the law. William Hill said it had "robust systems" to meet its regulatory obligations. In a statement, Ladbrokes said: "Any criminals attempting to launder large sums are placing themselves at high risk of detection as they will be on CCTV and staff are trained to spot suspicious behaviour. Given most stakes in shops are small, any large transactions are easily recognisable. Any attempt to transfer money to online accounts will require identity verification at account opening or first transactions which in conjunction with CCTV would be an excel ent source of evidence for the police."

The media have helped to cement the place of gambling in the national psyche. Advertising during televised football matches exhorts audiences to have a flutter. Electronic gambling has found a younger audience through online role-playing games such as World of Warcraft, in which players have been able to set up virtual casinos. This year the United Nations Office on Drugs and Crime warned that such games were being used by organised crime to launder cash.

Also helping to rehabilitate gambling is a new range of interactive TV programming. Late-night shows such as ITV's Jackpot247 – in which television viewers place bets online or over the phone, playing along to a live presenter-hosted roulette show – repolish gambling's image by treating electronic betting as a form of mainstream entertainment.

This shift in the marketing of electronic gambling has taken place as suspicions emerge that the industry has been targeting poor people. Last December, in a paper for the Journal of Gambling Studies, Heather Wardle, a former project director of the British

Gambling Prevalence Survey, warned that gambling machines were more likely to be found in areas of high socioeconomic deprivation. Earlier this year, the Guardian revealed that in the 50 parliamentary constituencies with the highest numbers of unemployed people, punters visited 1,251 betting shops and wagered an astonishing £5.6bn through 4,454 fixed-odds betting terminals.

Salford has 72 people chasing each vacancy. It was the only part of Greater Manchester which last year recorded a rise in numbers on jobseeker's allowance. Photograph: Christopher Thomond for the Guardian

The presence of these machines appears to have a distorting effect on these moribund local economies. In a pub near Salford's Duchy estate, close to where rioting took place in 2011, two young men nursed pints of soft drink and explained how a vortex of soft drug sales, payday lenders and betting shops kept the local economy afloat. Salford has 72 people chasing each vacancy. It was the only part of Greater Manchester which last year recorded a rise in numbers on jobseeker's allowance (JSA).

Unemployed Jake, 28, sells marijuana on the local streets and smokes some of the profit. He recoups any losses by gambling and taking out loans at payday lenders. He points out the brown shopping arcade in Salford lined with bookmakers and loan companies. "It's the only thriving industry around here," he says.

"There are six bookmakers, one more is on its way, and five loan shops. Even if you are on JSA you can borrow money from Speedy Cash. It's the main business around here.Take dole, turn it into weed, sell them, take your profits and put them into the machines. If you win, you are quids in. If you lose, you get cash from the money shops to cover your losses. Back to dole and buying drugs. There's nothing else around here to do."

The drug dealer admits that he is "a bit" addicted to gambling, comparing the thrill of betting on the electronic spin of a roulette wheel to the rapid highs and lows of drugs. "You get a buzz. Which is why you might lose £16 or £1,600 and not notice until it's too late. I've done both."

The spread of betting shops in this part of the north-west is astonishing. Manchester city centre has 26. A few miles away in deprived Cheetham Hill, dubbed the "Bronx of Britain" for gang violence, there are four bookies in the high street, with another scheduled.Such bunching could be linked to the fact that bookmakers are limited to four machines a shop. As the machines are hugely lucrative the betting industry has bypassed the restriction by opening branches in high streets – "clustering" in poorer areas.

A betting shop manager in Greater Manchester, who agreed to be interviewed anonymously, said the FOBTs in Cheetham Hill easily earned £10,000 a week, four times the over-the-counter trade, and that local mobsters gambled heavily. "We get punters who lose big time on the FOBTs, punch them, chuck them to the ground. Smash them. We tell staff to play it cool. Don't cal police. We don't want to arouse suspicions. It's madness. We employ young mothers in those shops.

"You have people laundering money every day with cash from robberies and drugs. Do you know that dyed notes from bank robberies can be submitted to the Bank of England and the company gets reimbursed? Staff know what pays their wages. They stay quiet."

Some names have been changed.

Financial Crime Asia

compliance, regulation, blatant abuses, dirty dealings and innovations

POSTED BY

HELENOGORMAN
POSTED ON

MARCH 21, 2013
POSTED UNDER

UNCATEGORIZED
COMMENTS

2 COMMENTS

Are Chinese laundries thriving in casinos?

According to a story (http://compliancex.com/how-chinese-company-laundered-millions-using-las-vegas-slot-machines/) in the Compliance Exchange, Chinese launderers are making use of Las Vegas casinos (http://en.wikipedia.org/wiki/Casino), in particular slot machines, to clean the proceeds of crime. The filthy lucre in question is US (http://maps.google.com/maps?ll=38.8833333333,-77.0166666667&spn=10.0,10.0&q=38.8833333333,-77.0166666667(United%20States)&t=h)$670m in funds missing from the IPO (http://en.wikipedia.org/wiki/Initial_public_offering) of a former NASDAQ (http://www.nasdaq.com/) listed Chinese (http://en.wikipedia.org/wiki/Chinese_language) company.

Details on this alleged laundry are scant, so far, but laundering through casinos is a familiar cycle to the anyone with a pile of cash to clean.

Casino clearance

As cash rich enterprises, casinos are highly attractive to organised criminals or tax evaders who want to tie their funds to a legitimate source. The Mob built Las Vegas in the 1940s expressly to clean and hide the proceeds of crime. Although global anti-money laundering standards have concentrated efforts in the past five years on stemming the flow of dirty money through casinos, the gambling business remains high risk. Raising staff and company awareness, generating a culture of compliance business and implementing a minimum level of training for casino staff can help to eradicate – or at least reduce – the impact of some of the tried and tested money laundering methods.

In 2009 the Asia-Pacific Group on Money Laundering published a report on money laundering via casinos. The common methods used below can be identified easily if the casino staff are encouraged and trained to identify suspicious transactions.

The cheque method - A casino client exchanges cash for chips gambles away a small amount and returns the chips to the cashier. The cashier provides him with a cheque from the casino for the value of the chips. The client then presents the cheque to a bank.

Enhanced due diligence processes in place at both casinos and banks should mean both large sums of money and cheques (http://en.wikipedia.org/wiki/Cheque) for large amounts from casinos should be the subject of enhanced scrutiny. However, the gambling business is geared towards attracting 'high-rollers' who play with vast sums in casinos. Spending levels that may constitute unusual or suspicious in most businesses is 'normal' behaviour in casinos.

Value tampering – the purchase of chips from 'clean' players at a higher price – Money launderers (http://en.wikipedia.org/wiki/Money_laundering) may purchase chips from other money launderers or un-associated casino patrons with 'clean' backgrounds. This is done at a price greater than the chips' face value.

Combining winnings and cash into casino cheques – although few jurisdictions allow this, money launderers seek to add cash to casino winnings and then exchange the combined cash and winnings for a single cheque.

As any anti-money laundering veteran will attest, the criminally minded are always one step ahead of the law enforcers and standard setters. *Financial Crime Asia* would like to hear from AML (http://en.wikipedia.org/wiki/Acute_myeloid_leukemia) officers in casinos who have identified suspected money laundering. All stories and reports will be treated confidentially.

Grant Thornton

Reporting Entity Sector Profiles: Finanical Entities Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

Industry statistics and reporting data

Financial institutions industry SIC codes

Code	Description
6021	National commercial banks
6022	State commercial banks
6029	Commercial banks, not elsewhere classified
6081	Branches and agencies of foreign banks
6082	Foreign trade and international banking institutions
6091	Non-depository trust facilities
6099	Functions related to depository banking, not elsewhere classified
6712	Offices of bank holding companies

Financial institutions industry NAICS codes

Code	Description
52111	Monetary authorities - central bank
5221	Depository credit intermediation
52211	Banking
522111	Personal and commercial banking industry
522112	Corporate and institutional banking industry
52213	Local credit unions
52219	Other depository credit intermediation
5222	Non-depository credit intermediation
52221	Credit card issuing
52222	Sales financing
52229	Other non-depository credit intermediation
522291	Consumer lending
522299	All other non-depository credit intermediation
5223	Activities related to credit intermediation
52231	Mortgage and non-mortgage loan brokers
52232	Financial transactions processing, reserve and clearing house activities

Code	Description
522321	Central credit unions
522329	Other financial transactions processing and clearing house activities
52239	Other activities related to credit intermediation

Using NAICs codes, searches for statistical data on the Financial Entities sector were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Monetary authorities - Central Bank (NAICS 52111)

Number of establishments in Canada by type and region: December 2012
Monetary Authorities - Central Bank (NAICS 52111)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	1	0	1	11.1%
British Columbia	1	0	1	11.1%
Manitoba	1	0	1	11.1%
New Brunswick	1	0	1	11.1%
Newfoundland and Labrador	0	0	0	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	1	0	1	11.1%
Nunavut	0	0	0	0.0%
Ontario	1	1	2	22.2%
Prince Edward Island	0	0	0	0.0%
Quebec	1	0	1	11.1%
Saskatchewan	1	0	1	11.1%
Yukon Territory	0	0	0	0.0%
CANADA	8	1	9	100%
Percent Distribution	88.9%	11.1%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Monetary Authorities - Central Bank (NAICS52111)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	0	1	0	0
British Columbia	0	1	0	0
Manitoba	0	1	0	0
New Brunswick	0	1	0	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	1	0	0
Nunavut	0	0	0	0
Ontario	0	0	0	1
Prince Edward Island	0	0	0	0
Quebec	0	0	1	0
Saskatchewan	0	1	0	0
Yukon Territory	0	0	0	0
CANADA	0	6	1	1
Percent Distribution	0.0%	75.0%	12.5%	12.5%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Banking (NAICS 52211)

Number of establishments in Canada by type and region: December 2012 Banking (NAICS 52211)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	315	10	325	9.0%
British Columbia	354	5	359	10.0%
Manitoba	119	0	119	3.3%
New Brunswick	104	1	105	2.9%
Newfoundland and Labrador	80	0	80	2.2%
Northwest Territories	5	0	5	0.1%
Nova Scotia	112	0	112	3.1%
Nunavut	0	0	0	0.0%
Ontario	1,351	37	1,388	38.6%
Prince Edward Island	14	1	15	0.4%
Quebec	946	14	960	26.7%
Saskatchewan	128	0	128	3.6%
Yukon Territory	4	0	4	0.1%
CANADA	3,532	68	3,600	100%
Percent Distribution	98.1%	1.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Banking (NAICS52211)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	22	289	1	3
British Columbia	21	324	5	4
Manitoba	3	113	0	3
New Brunswick	1	100	0	3
Newfoundland and Labrador	0	78	1	1
Northwest Territories	0	4	1	0
Nova Scotia	2	108	0	2
Nunavut	0	0	0	0
Ontario	56	1,259	21	15
Prince Edward Island	0	13	1	0
Quebec	39	892	5	10
Saskatchewan	8	115	2	3
Yukon Territory	0	4	0	0
CANADA	152	3,299	37	44
Percent Distribution	4.3%	93.4%	1.0%	1.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Personal and commercial banking industry (NAICS 522111)

Number of establishments in Canada by type and region: December 2012 Personal and Commercial Banking Industry (NAICS 522111)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	312	9	321	9.1%
British Columbia	346	5	351	9.9%
Manitoba	119	0	119	3.4%
New Brunswick	104	1	105	3.0%
Newfoundland and Labrador	80	0	80	2.3%
Northwest Territories	5	0	5	0.1%
Nova Scotia	112	0	112	3.2%
Nunavut	0	0	0	0.0%
Ontario	1,330	27	1,357	38.3%
Prince Edward Island	14	1	15	0.4%
Quebec	936	10	946	26.7%
Saskatchewan	127	0	127	3.6%
Yukon Territory	4	0	4	0.1%
CANADA	3,489	53	3,542	100%
Percent Distribution	98.5%	1.5%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Personal and Commercial Banking Industry (NAICS522111)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	22	286	1	3
British Columbia	18	320	4	4
Manitoba	3	113	0	3
New Brunswick	1	100	0	3
Newfoundland and Labrador	0	78	1	1
Northwest Territories	0	4	1	0
Nova Scotia	2	108	0	2
Nunavut	0	0	0	0
Ontario	50	1,248	17	15
Prince Edward Island	0	13	1	0
Quebec	36	886	5	9
Saskatchewan	8	114	2	3
Yukon Territory	0	4	0	0
CANADA	140	3,274	32	43
Percent Distribution	4.0%	93.8%	0.9%	1.2%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Corporate and institutional banking industry (NAICS 522112)

Number of establishments in Canada by type and region: December 2012 Corporate and Institutional Banking Industry (NAICS 522112)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	3	1	4	6.9%
British Columbia	8	0	8	13.8%
Manitoba	0	0	0	0.0%
New Brunswick	0	0	0	0.0%
Newfoundland and Labrador	0	0	0	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	0	0	0.0%
Nunavut	0	0	0	0.0%
Ontario	21	10	31	53.4%
Prince Edward Island	0	0	0	0.0%
Quebec	10	4	14	24.1%
Saskatchewan	1	0	1	1.7%
Yukon Territory	0	0	0	0.0%
CANADA	43	15	58	100%
Percent Distribution	74.1%	25.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Corporate and Institutional Banking Industry (NAICS522112)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	0	3	0	0
British Columbia	3	4	1	0
Manitoba	0	0	0	0
New Brunswick	0	0	0	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	6	11	4	0
Prince Edward Island	0	0	0	0
Quebec	3	6	0	1
Saskatchewan	0	1	0	0
Yukon Territory	0	0	0	0
CANADA	12	25	5	1
Percent Distribution	27.9%	58.1%	11.6%	2.3%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Non-depository credit intermediation (NAICS 5222)

Number of establishments in Canada by type and region: December 2012 Non-Depository Credit Intermediation (NAICS 5222)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	270	639	909	13.0%
British Columbia	320	707	1,027	14.7%
Manitoba	74	140	214	3.1%
New Brunswick	50	45	95	1.4%
Newfoundland and Labrador	31	19	50	0.7%
Northwest Territories	6	5	11	0.2%
Nova Scotia	49	83	132	1.9%
Nunavut	2	2	4	0.1%
Ontario	816	2,393	3,209	45.9%
Prince Edward Island	9	10	19	0.3%
Quebec	315	844	1,159	16.6%
Saskatchewan	62	97	159	2.3%
Yukon Territory	4	4	8	0.1%
CANADA	2,008	4,988	6,996	100%
Percent Distribution	28.7%	71.3%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Non-Depository Credit Intermediation (NAICS5222)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	149	117	3	1
British Columbia	180	134	6	0
Manitoba	48	24	2	0
New Brunswick	21	29	0	0
Newfoundland and Labrador	14	17	0	0
Northwest Territories	3	3	0	0
Nova Scotia	17	31	1	0
Nunavut	1	1	0	0
Ontario	442	345	17	12
Prince Edward Island	4	5	0	0
Quebec	152	156	6	1
Saskatchewan	35	25	2	0
Yukon Territory	2	1	1	0
CANADA	1,068	888	38	14
Percent Distribution	53.2%	44.2%	1.9%	0.7%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Credit card issuing (NAICS 52221)

Number of establishments in Canada by type and region: December 2012 Credit Card Issuing (NAICS 52221)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	0	2	2	5.9%
British Columbia	2	1	3	8.8%
Manitoba	0	0	0	0.0%
New Brunswick	0	1	1	2.9%
Newfoundland and Labrador	0	1	1	2.9%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	1	1	2.9%
Nunavut	0	0	0	0.0%
Ontario	10	10	20	58.8%
Prince Edward Island	0	0	0	0.0%
Quebec	4	2	6	17.6%
Saskatchewan	0	0	0	0.0%
Yukon Territory	0	0	0	0.0%
CANADA	16	18	34	100%
Percent Distribution	47.1%	52.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Credit Card Issuing (NAICS52221)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	0	0	0	0
British Columbia	0	1	1	0
Manitoba	0	0	0	0
New Brunswick	0	0	0	0
Newfoundland and Labrador	0	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	2	5	0	3
Prince Edward Island	0	0	0	0
Quebec	2	1	1	0
Saskatchewan	0	0	0	0
Yukon Territory	0	0	0	0
CANADA	4	7	2	3
Percent Distribution	25.0%	43.8%	12.5%	18.8%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Canada bank sector values: $ billion, 2008-2012

Year	US$ Billion	% Growth
2008	3,181.4	
2009	2,853.7	(10.3%)
2010	3,082.4	8.0%
2011	3,660.2	18.7%
2012	3,847.5	5.1%
CAGR: 2008-2012		4.9%

MarketLine Industry Profile – Banks in Canada – June 2013

Canada bank sector category segmentation: $ billion, 2012

Category	2012	%
Bank credit	1,669.4	43.4%
Other assets	1,657.1	43.1%
Trading assets	331.7	8.6%
Cash assets	153.4	4.0%
Interbank Loans	35.8	0.9%
Total	3,847.4	100%

MarketLine Industry Profile – Banks in Canada – June 2013

Canada bank sector value forecast: $ billion, 2012

Category	2012	%
2012	3,847.5	5.1%
2013	4,152.1	7.9%
2014	4,522.3	8.9%
2015	4,933.7	9.1%
2016	5,350.3	8.4%
2017	5,772.1	7.9%

MarketLine Industry Profile – Banks in Canada – June 2013

Breakdown of financial entities

Financial entities	Number of entities
Banks	
- Domestic Banks	29
- Foreign Banks	24
- Foreign Bank Branches - Full Service	25
- Foreign Bank Branches - Lending	4
Credit Unions	319
Credit Union Centrals	10
Caisse Populaires	426
Financial Service cooperatives	11
Trust companies	45
Loan companies	19
Agents of the crown that accept deposit liabilities	

Sources

- OSFI (Banks, Trust companies, Loan companies)
- Credit Union Central of Canada - Q3 2013 - Credit Union/Caisse populaire System Results (Credit Unions and Caisse Populaires)
- Coops Canada - http://www.coopscanada.coop/en/about_co-operative/provincialprofiles
- Canadian Cooperative Association,Annual Report 2012-13 List of Members - March 2013, Central1 - List of Provincial Centrals & related affiliations
- Financial Services Coops - CCA -

Appendix B: Case examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Twenty-five people face charges in alleged fraud, money-laundering scheme. The Globe and Mail, July 15, 2013
2. Citigroup affiliate's troubles multiply as money-laundering subpoenas follow fraud. The New York Times, March 3, 2014
3. Awash in cash, drug cartels rely on big banks to launder profits. NPR, March 20, 2014.
4. Guatemala's ex-President pleads guilty to Miami money-laundering, March 18, 2014.
5. In hours, thieves took $45 million in A.T.M. scheme. The New York Times, May 9, 2013.
6. U.S. documents allege lapses in HSBC money laundering controls, The Vancouver Sun, May 4, 2014.
7. Bank scandals hint at problems. Kamloops Daily News, December 29, 2012.
8. Banks hide dirty laundry. Winnipeg Free Press, December 27, 2012
9. U.S. seizes $150M from Hezbollah-linked Canadian bank. The Kirkland Lake Northern News. August 24, 2012.
10. Latest example of banksterism shows why faith in capitalism is fading. Financial Post, July 13, 2012.
11. Punishment not enough to prevent banks from committing fraud. The Sudbury Star, November 2, 2013.
12. Whistleblower: HSBC still laundering money for terrorists, drug cartels. TruthstreamMedia.com. September 20, 2013.
13. Money Laundering: SSS detains staff of 13 banks over Lamido's son. This Day Live, November 16, 2013
14. NY appeals court rules to apply Israeli law in Bank of China terror financing case. The Jerusalem Post, September 20, 2013.

15. How a Canadian was charged with money laundering in sale of bitcoins. The Globe and Mail, February 12, 2014.

16. U.S. Fed warns Bank of Montreal on anti-money laundering controls. National Post. May 17, 2013.

17. 'HSBC arranged for opening of accounts abroad and withdrawal from Delhi itself. The Hindu. November 2012.

18. Tax crackdown broadens: HSBC pushed on secret bank accounts in India unit. The Wall Street Journal, April 8, 2011.

19. U.S. Banks steer clear of sensitive customers. The Wall Street Journal, January 29, 2014.

Twenty-five people face charges in alleged fraud, money-laundering scheme

Vidya Kauri
The Globe and Mail
Published Monday, Jul. 15 2013, 5:47 PM EDT
Last updated Monday, Jul. 15 2013, 5:53 PM EDT

Twenty-five people face charges in an alleged multimillion-dollar fraud and money-laundering scheme that targeted major financial institutions across the GTA.

Toronto police announced the arrest of these individuals Monday and said they are still looking for about six more suspects. The accused face a variety of charges including fraud, laundering, forging documents and obtaining credit under false pretenses.

More Related to this Story

- OSC revives case against Conrad Black
- SNC-Lavalin files suit against former executive, consultant
- Case against former Laval mayor put off until October

"Between March, 2011, and October, 2012, several people participated in an organized scheme to defraud banks, money lenders and other financial institutions in the Greater Toronto Area and launder the proceeds,"Detective Constable Sarath Thayalan said. "The scheme involved the creation of several shell companies which were then used to apply for credit from a targeted lender."

The accused are residents of Toronto, Brampton, Mississauga, Cambridge, Markham, Vaughan, Bradford, Woodbridge and Ajax. They all have different last names and range in age from 26 to 75. Det. Constable Thayalan said that some of them are friends, some are family members and some have had business dealings with each other in the past. Not all the accused know each other, he said.

"This is not the type of plan that can be done overnight. Some of the set-up times were in the order of months for some of these frauds to be tried and then tried repeatedly," he said. "There is the motivation purely for monetary gain in which someone could perceivably see a scheme like this being worthwhile."

Three of the 25 arrested – Daniel Kebbe, 33, from Bradford, Elias Rassi, 33, from Vaughan, and Michael Shawn Majeed, 33, of Markham – are alleged to have orchestrated the fraud scheme, Det. Constable Thayalan said.

The operation involved individuals impersonating accountants claiming to have connections to a shell company looking to borrow money, the constable explained. The fraudster would produce forged financial documents to a bank. A bank representative would visit the location of the business, which often had equipment and staff working. If the representative was satisfied that the deal appeared legitimate, a line of credit was granted.

"The information I have supports the belief that certain businesses participated in the scheme by allowing their business, their equipment to be misrepresented as belonging to the shell company," he said. "However, during the course of a fraud, some or all of the items that would normally be in that business would be either taken away or moved aside or replaced with items to facilitate the fraud."

The largest loan amount requested was $1.7-million. The total amount of credit requested is $8-million. Not all the money was granted, and while police have recovered some of the money, millions remain lost. The money was transferred to various places in Ontario, the United States, Hong Kong and Switzerland.

Toronto police will not reveal the names of the banks that were targeted, saying only that they are "companies we all deal with on a regular basis." The businesses that are alleged to be involved in the scam include Omnium Financial Group, Yorkshire Capital, Global Granite and Shankar Woodcrafts. Some other businesses that went by a few different names include a crown moulding company, a printing company, and a cabinetry business.

Canadian taxpayers often end up footing the bill for these crimes, Det. Contable Thayalan said. Banks often pass on the costs associated with these frauds to their customers, he said. As well, government programs subsidize some of these loans.

"Some of the money that is given out under loans of this type is often subsidized in part by government programs designed to help businesses and promote the economy. When funds are misappropriated in this way, the cost of that is transferred directly to the Canadian government who created these programs and that in turn is funded by the Canadian taxpayer."

The New York Times

March 3, 2014, 9:35 am

Citigroup Affiliate's Troubles Multiply as Money-Laundering Subpoenas Follow Fraud

By MICHAEL CORKERY and JESSICA SILVER-GREENBERG

Updated, 9:16 p.m. | A headache is growing for Citigroup as a banking affiliate involved in money transfers across the Mexican border has become ensnared in a criminal investigation.

Friday that it had been defrauded of $400 million in a scheme involving a financially shaky oil services company in Mexico.

A Citigroup affiliate based in Los Angeles received a grand jury subpoena from federal prosecutors in Massachusetts related to anti-money-laundering compliance, the bank said in a securities filing on Monday. The focus of the subpoenas is unclear. The affiliate has also received a subpoena from the Federal Deposit Insurance Corporation related to its anti-money-laundering program and the Bank Secrecy Act.

The affiliate, Banamex USA, provides banking services to individuals and small businesses in the United States and Mexico. Until recently, it was a large player in transferring money across the border between family members, industry experts say.

Mexico, Citigroup's chief executive, Michael L. Corbat, did not mention the inquiries involving the Banamex affiliate in the United States.

marketplace

Awash In Cash, Drug Cartels Rely On Big Banks To Launder Profits

by **JOHN BURNETT**

March 20, 2014 3:39 PM

Listen to the Story

All Things Considered **5 min 32 sec**

Enric Marti/AP

The Sinaloa Cartel, headquartered on Mexico's northern Pacific Coast, is constantly exploring new ways to launder its gargantuan profits. The State Department reports that Mexican trafficking organizations earn between $19 and $29 billion every year from selling marijuana, cocaine, heroin and methamphetamines on the streets of American cities.

And Sinaloa is reportedly the richest, most powerful of them all, according to the Drug Enforcement Administration. The capture last month of the Mexican druglord Joaquin "Chapo" Guzman has cast a spotlight on the smuggling empire he built.

One key to the Sinaloa Cartel's success has been to use the global banking system to launder all this cash.

"It's very important for them to get that money into the banking system and do so with as little scrutiny as possible," says Jim Hayes, special agent in charge of Homeland Security Investigations for the New York office of Immigration and Customs Enforcement, or ICE. He was lead agent in the 2012 case that revealed how Sinaloa money men used HSBC, one of the world's largest banks, as their private vault.

ICE says in 2007 and 2008, the Sinaloa Cartel and a Colombian cartel wire-transferred $881 million in illegal drug proceeds into U.S. accounts.

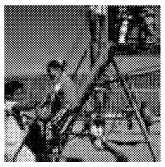
Huge Daily Deposits

According to a subsequent investigation by the U.S. Senate Permanent Subcommittee on Investigations, cartel operatives would sometimes deposit hundreds of thousands of dollars in cash in a single day using boxes designed to fit the exact dimensions of the teller's window at HSBC branches in Mexico.

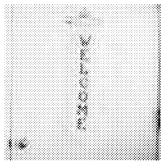
More In The Borderland Series

Parallels

At The Border, The Drugs Go North And The Cash Goes South



Borderland: Dispatches From The U.S.-Mexico Boundary



Parallels

A U.S. Border Shelter That Attracts Asylum Seekers Far And Wide

The bank ignored basic anti-money laundering controls, as the investigation found. In 2007 and 2008, the bank's personnel in Mexico wired $7 billion dollars to corresponding U.S. dollar accounts in New York. These were more dollars than even larger Mexican banks wired to U.S. accounts. ICE says some of it was drug proceeds.

Yet no red flags were raised because of what a bank official later described as, a "lack of a compliance culture" in the Mexico affiliate, according to the Senate report.

Moreover, the dollar transfers earned HSBC hefty fees. The Senate investigation quoted an HSBC email lamenting how the bank would lose $2.6 billion in revenue from U.S. dollar accounts that it was forced to close because of the Mexico fiasco.

"When I was told that there could be in the billions of dollars being moved through these accounts, it was very difficult to believe," says senior ICE agent Jim Hayes. "A lot of people have asked, 'Was this

complicit?' We don't believe that they (HSBC personnel) knew for certain that the money being moved was drug money, but they should have known."

A Simple Plan

In Culiacán, the prosperous capital of Sinaloa, where people live cheek by jowl with the cartel, even they were shocked that narco-dollars could be laundered so brazenly.

"You see the building, the office, the cars, the papers, the men in suits. Everything looks legal. That's what frightens us," says Javier Valdez, an author and journalist in Culiacan who writes about narcotrafficking.

"The DEA loves to sell the idea that these guys are super sophisticated criminal masterminds," says Alejandro Hope, a security analyst in Mexico City and a former federal intelligence agent. "It's so simple. It's so unsophisticated. That is what to me is the most disturbing part of this. These guys are not even trying that hard."

The consequences for ignoring the torrent of dirty money flowing into its Mexico bank vaults were severe for HSBC.

The Department of Justice levied penalties and forfeitures of $1.9 billion on the bank. Of course, with $2.6 trillion in assets, for HSBC this represented a man with a hundred dollars in his pocket paying a fine of seven cents. HSBC was also faulted for hiding prohibited transactions with nations like Iran and Cuba.

The bank emailed a statement to NPR:

> "HSBC has made progress in remediating anti-money laundering sanctions compliance deficiencies. But we recognize that protecting against financial crime is an ongoing journey and we have much more to do. Since 2011, we have implemented reforms and new controls, enhanced our monitoring systems, and strengthened and expanded our global financial crime and compliance organization. For example, the number of fulltime employees in financial crime and regulatory compliance is up 54 percent between 2012 and 2013."

ICE agent Jim Hayes says fallout from the HSBC case continues.

"We think this forfeiture is significant enough to make other banks to look and make sure they're in compliance," he says.

Banks Still Vulnerable

In the wake of HSBC, other banks boosted their anti-money laundering budgets, increased know-your-customer rules, and in some cases dumped high-risk clients.

Which might make you think, well, now they've got money laundering under control.

"Despite all of the efforts, banks are still vulnerable to money laundering and it's kind of an age-old thing," says Kieran Beer, editor of the news website of the Association of Certified Anti-Money Laundering Specialists.

"The drug trade is overwhelming in terms of how that money finds paths—like water — to come into the global financial system," Beer continues.

HSBC wasn't the first or last bank money-laundering scandal.

In 2010, prosecutors detailed how Wachovia Bank had been used by Mexican currency exchange houses to launder at least $110 million in drug profits.

In 2012, The Wall Street Journal reported on an FBI affidavit that laid out how the Zetas Cartel used Bank of America to launder cash through a racehorse operation in Texas.

And last month, Western Union agreed to do more to beef up vulnerabilities in its money transfer business along the southwest border.

Back in Culiacán, and throughout Mexico, currency exchange houses operate under strict new rules that are supposed to limit the size of dollar transactions, investigators are watching to see what the narcos next money-laundering ploy will be.

u.s.-mexico

Guatemala's Ex-President Pleads Guilty to Miami Money Laundering

By Kyle Munzenrieder Tue., Mar. 18 2014 at 3:45 PM
Categories: Around the World

1 Comment

What started in Guatemala and took a financial detour to Miami has now ended in New York. Former Guatemalan president Alfonso Portillo pleaded guilty in a New York courtroom today to a charge of money laundering designed to hide bribes he had taken from Taiwan.

Portillo was voted into office in 2000 as a member of the country's right-wing Republican Front party and promised to reduce corruption in the country. Instead, he got caught up in a heap of corruption of his own, and at the end of his term in 2004, he fled to Mexico. He was ultimately extradited to Guatemala in 2008, but charges were dropped. However, in an unprecedented move, a court ruled he would be extradited to America in 2011 to face charges here.

Today, he pleaded guilty to accepting $2.5 million from the Taiwanese government in exchange for continuing to recognize the Asian country diplomatically. That's a particularly tricky proposition in Latin America, where many countries have strong ties to mainland China.

Portillo accepted five checks totaling $2.5 million. The first three ended up being deposited in a Miami bank and were personally endorsed by Portillo. Two other checks were made out to Oxxy Financial Corp. and deposited into the International Bank of Miami. Much of the money was then transferred to a Paris bank account under the name of Portillo's then-wife and continued along a string of transfers across the world.

Today in a Manhattan federal court, Portillo pleaded guilty to the single charge of money laundering. It is the first time he has been convicted anywhere related to his corruption in office.

"Former president Alfonso Portillo may have thought his position of power prevented him from having to answer for accepting multimillion-dollar bribes to shape his country's foreign policy, for embezzling money intended to benefit the Guatemalan people, and for using U.S. banks to launder the ill-gotten funds. But he was wrong" U.S. Attorney Preet Bharara said in a statement. "With his guilty plea today, Portillo now stands convicted in an American court for his criminal conduct. This office will aggressively pursue and prosecute individuals, irrespective of their position or title, if they engage in violations of U.S. laws."

Portillo will be sentenced in June and faces up to 20 years in prison.

The New York Times

May 9, 2013

In Hours, Thieves Took $45 Million in A.T.M. Scheme

By MARC SANTORA

It was a brazen bank heist, but a 21st-century version in which the criminals never wore ski masks, threatened a teller or set foot in a vault.

In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.'s in a matter of hours.

In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

The operation included sophisticated computer experts operating in the shadowy world of Internet hacking, manipulating financial information with the stroke of a few keys, as well as common street criminals, who used that information to loot the automated teller machines.

The first to be caught was a street crew operating in New York, their pictures captured as, prosecutors said, they traveled the city withdrawing money and stuffing backpacks with cash.

On Thursday, federal prosecutors in Brooklyn unsealed an indictment charging eight men — including their suspected ringleader, who was found dead in the Dominican Republic last month. The indictment and criminal complaints in the case offer a glimpse into what the authorities said was one of the most sophisticated and effective cybercrime attacks ever uncovered.

It was, prosecutors said, one of the largest heists in New York City history, rivaling the 1978 Lufthansa robbery, which inspired a scene in the movie "Goodfellas."

Beyond the sheer amount of money involved, law enforcement officials said, the thefts underscored the vulnerability of financial institutions around the world to clever criminals working to stay a step ahead of the latest technologies designed to thwart them.

"In the place of guns and masks, this cybercrime organization used laptops and
said Loretta E. Lynch, the United States attorney in Brooklyn. "Moving as swif
the Internet, the organization worked its way from the computer systems of in
corporations to the streets of New York City, with the defendants fanning out a

to steal millions of dollars from hundreds of A.T.M.'s in a matter of hours."

The indictment outlined how the criminals were able to steal data from banks, relay that information to a far-flung network of so-called cashing crews, and then have the stolen money laundered in purchases of luxury items like Rolex watches and expensive cars.

In the first operation, hackers infiltrated the system of an unnamed Indian credit-card processing company that handles Visa and MasterCard prepaid debit cards. Such companies are attractive to cybercriminals because they are considered less secure than financial institutions, computer security experts say.

The hackers, who are not named in the indictment, then raised the withdrawal limits on prepaid MasterCard debit accounts issued by the National Bank of Ras Al-Khaimah, also known as RakBank, which is in United Arab Emirates.

Once the withdrawal limits have been eliminated, "even a few compromised bank account numbers can result in tremendous financial loss to the victim financial institution," the indictment states. And by using prepaid cards, the thieves were able to take money without draining the bank accounts of individuals, which might have set off alarms more quickly.

With five account numbers in hand, the hackers distributed the information to individuals in 20 countries who then encoded the information on magnetic-stripe cards. On Dec. 21, the cashing crews made 4,500 A.T.M. transactions worldwide, stealing $5 million, according to the indictment.

While the street crews were taking money out of bank machines, the computer experts were watching the financial transactions from afar, ensuring that they would not be shortchanged on their cut, according to court documents.

MasterCard alerted the Secret Service to the activity soon after the transactions were completed, said a law enforcement official, who declined to be identified discussing a continuing investigation.

Robert D. Rodriguez, a special agent with the Secret Service for 22 years and now the chairman of Security Innovation Network, said that in some ways the crime was as old as money itself: bad guys trying to find weaknesses in a system and exploiting that weakness.

"The difference today is that the dynamics of the Internet and cyberspace are so fast that we have a hard time staying ahead of the adversary," he said. And because these crimes are global, he said, even when the authorities figure out who is behind them they might not be able to arrest them or persuade another law enforcement agency to take action.

After pulling off the December theft, the organization grew more bold, and two months later it struck again — this time nabbing $40 million.

On Feb. 19, cashing crews were in place at A.T.M.'s across Manhattan and in two dozen other countries waiting for word to spring into action.

This time, the hackers had infiltrated a credit-card processing company based in the United States that also handles Visa and MasterCard prepaid debit cards. Prosecutors did not disclose the company's name.

After securing 12 account numbers for cards issued by the Bank of Muscat in Oman and raising the withdrawal limits, the cashing crews were set in motion. Starting at 3 p.m., the crews made 36,000 transactions and withdrew about $40 million from machines in the various countries in about 10 hours. In New York City, a team of eight people made 2,904 withdrawals, stealing $2.4 million.

Surveillance photos of one suspect at various A.T.M.'s showed the man's backpack getting heavier and heavier, Ms. Lynch said, comparing the series of thefts to the caper at the center of the movie "Ocean's Eleven."

While the New York crew had a productive spree, the crews in Japan seem to have been the most successful, stealing around $10 million, probably because some banks in Japan allow withdrawals of as much as $10,000 from a single bank machine.

"The significance here is they are manipulating the financial system to be able to change these balance limits and withdrawal limits," said Kim Peretti, a former prosecutor in the computer crime division of the Justice Department who is now a partner in the law firm Alston & Bird. "When you have a scheme like this, where the system can be manipulated to quickly get access to millions of dollars that in some sense did not exist before, it could be a systemic risk to our financial system."

It was unclear to whom the hacked accounts belonged, and who might ultimately be responsible for the losses.

The indictment suggests a far-reaching operation, but there were few details about the people responsible for conducting the hacking or who might be leading the global operation. Law enforcement agencies in more than a dozen countries are still investigating, according to federal prosecutors. The authorities said the leader of the New York cashing crew was Alberto Lajud-Peña, 23, whose body was found in the Dominican Republic late last month. Seven other people were charged with conspiracy to commit "access device fraud" and money laundering.

The prosecutors said they were all American citizens and were based in Yonkers. The age of one defendant was given as 35; the others were all said to be 22 to 24. Mr. Lajud-Peña fled the United States just as the authorities were starting to make arrests of members of his crew, the law enforcement official said.

On April 27, according to news reports from the Dominican Republic, two hooded gunmen stormed a house where he was playing dominoes and began shooting. A manila envelope containing about $100,000 in cash remained untouched.

Nicole Perlroth, Frances Robles and Mosi Secret contributed reporting.

This article has been revised to reflect the following correction:

Correction: May 11, 2013

An article on Friday about a sophisticated hacking crime in which $45 million was stolen from bank A.T.M.'s within hours misspelled, in some editions, the surname of a former prosecutor in the computer crime division of the Justice Department who commented on the case. She is Kim Peretti, not Paretti. The article also overstated the connection between the movie "Goodfellas" and the Lufthansa robbery in 1978, to which the A.T.M. case was compared. The Lufthansa robbery was only a plotline in the film; the movie itself was based on the book "Wise Guy," written by Nicholas Pileggi, about the mobster Henry Hill.

infomart

THE VANCOUVER SUN

Special report: U.S. documents allege lapses in HSBC money laundering controls

vancouversun.com
Fri May 4 2012
Section: OnLine
Byline: Carrick Mollenkamp, Brett Wolf and Brian Grow

In April 2003, the Federal Reserve **Bank** of New York and New York state **bank** regulators cracked the whip on HSBC **Bank** USA, ordering it to do a better job of policing itself for suspicious money flows. Staff in the **bank**'s anti-**money laundering** division, according to a person who worked there at the time, flew into a "panic."

The U.S. unit of London-based HSBC Holdings Plc quickly rallied. It hired a tough federal prosecutor to oversee anti-**money laundering** efforts. It installed monitoring systems for operations that had grown unwieldy during the **bank**'s U.S. expansion. The aim, as HSBC said in an agreement with regulators at the time, was to "ensure that the **bank** fully addresses all deficiencies in the **bank**'s anti-**money laundering** policies and procedures."

Nearly a decade later, the effort has failed to satisfy law-enforcement officials.

The extent of that failure is laid out in confidential documents reviewed by Reuters that originate from investigations of HSBC's U.S. operations by two U.S. Attorneys' offices.

These documents allege that from 2005, the **bank** violated the **Bank** Secrecy Act and other anti-**money laundering** laws on a massive scale. HSBC did so, they say, by not adequately reviewing hundreds of billions of dollars in transactions for any that might have links to drug trafficking, terrorist financing and other criminal activity.

In some of the documents, prosecutors allege that HSBC intentionally flouted the law. The **bank** created an operation that was a "systemically flawed sham paper-product designed solely to make it appear that the **Bank** has complied" with the **Bank** Secrecy Act and is able to detect **money laundering**, wrote William J. Ihlenfeld **II**, U.S. Attorney for the Northern District of West Virginia, in a draft of a 2010 letter addressed to Justice Department officials.

In that letter, Ihlenfeld compared HSBC unfavorably to Riggs **Bank**. In 2004 and 2005, that scandal-plagued Washington **bank** was fined a total of $41 million after it was found to have violated anti-**money laundering** laws, and it was acquired by PNC Financial Services.

"HSBC is to Riggs, as a nuclear waste dump is to a municipal land fill," Ihlenfeld wrote.

The allegations laid out in the Ihlenfeld letter and other documents couldn't be confirmed. It is possible that subsequent inquiries have led investigators to alter their views of what went on inside HSBC's compliance operation.

As they are, the documents reviewed by Reuters, combined with regulatory filings, court documents and interviews with current and former HSBC employees, paint a damning portrait of a **bank** allegedly unable, and unwilling, to police itself or its clients.

HSBC's U.S. anti-**money laundering** division - the people charged with ensuring that the **bank** toes the line of regulators and law enforcement - has experienced high turnover among executives. Since 2005, at least half a dozen overseers have come and gone. Compliance staff also encountered pushback from bankers eager to maintain relationships with lucrative clients whose dealings raised red flags.

In the Miami office - an important center for HSBC's private-banking and retail operations - a longtime private banker was fired for alleged sexual harassment after he warned compliance officers that clients were engaged in shady

dealings.

In one email exchange submitted as evidence in that case, employees debated whether the **bank** should help a Miami client get around U.S. sanctions by moving the client's business to HSBC's Hong Kong office. "I believe that the best outcome would be for the customer to open a relationship with Hong Kong just for leters (sic) of credit purposes. He travels there all the time," private banker Antonio Suarez wrote in a 2008 email. Suarez has since left the **bank** and couldn't be reached for comment.

UNDER THE RADAR

The revelations come as HSBC confronts multiple investigations into its internal policing abilities. The Justice Department, the Federal Reserve, the Office of the Comptroller of the Currency, the Manhattan district attorney, the Office of Foreign Assets Control and the Senate Permanent Subcommittee on Investigations are scrutinizing client activities such as cross-border movements of bulk cash, and transactions linked to Iran and other parties under U.S. economic sanctions, the **bank** said in a February regulatory filing.

"We continue to cooperate with officials in a number of ongoing investigations," HSBC spokesman Robert Sherman said. "The details of those investigations are confidential, and therefore we will not comment on specific allegations." HSBC said in its February filing that it was likely to face criminal or civil charges related to the probes.

A successful case against HSBC could result in an onerous fine and represent one of the most significant **money laundering** cases ever brought against an international **bank**. It also would draw unaccustomed attention to the challenges governments -- and financial institutions -- face in monitoring the trillions of dollars flowing through banks' back-office operations, flows essential to the daily functioning of the global financial system.

"Disguised in the trillions of dollars that is transferred between banks each day, banks in the U.S. are used to funnel massive amounts of illicit funds," Jennifer Shasky Calvery, head of the Justice Department's Asset Forfeiture and **Money Laundering** Section, said in congressional testimony on organized crime in February.

In response to Reuters inquiries about the investigations, Gary Peterson, chief compliance officer of HSBC's U.S. **bank** operations, said: "Since joining HSBC in 2010, I've been proud to lead an AML (anti-**money laundering**) team that has vastly increased investments in people, systems and expertise. We are continuously seeking to strengthen our core AML mission: to detect and deter **money laundering** and terrorist financing - and our efforts are showing results."

To date, the only enforcement action detailing any anti-**money laundering** shortcomings at HSBC was a 2010 consent order from the Office of the Comptroller of the Currency, the Treasury agency that is HSBC's chief regulator. The OCC, calling HSBC's compliance program "ineffective," told the **bank** to conduct a review to identify suspicious activity. This "look-back" was expected to yield a report to HSBC and regulators. The status of the report isn't known. A spokesman for the OCC declined to comment.

The West Virginia U.S. Attorney's probe of HSBC, which ran from 2008 until at least 2010, originated in a case against a local pain doctor who allegedly used HSBC accounts to launder ill-gotten gains from Medicare fraud. Over time, the U.S. Attorney's office began to discern that, as Ihlenfeld wrote in his letter, the doctor's case was just "the tip of the iceberg" in terms of the volume of suspicious money sluicing through HSBC.

The U.S. attorney for the Eastern District of New York in Brooklyn - one of the most powerful prosecutors outside of Justice Department headquarters in Washington - has conducted a parallel investigation, in collaboration with the Justice Department's **money laundering** section.

Specifics on the investigations have until now been cloaked in secrecy. The documents reviewed by Reuters for the first time fill in some of the details. Taken together, they depict apparent anti-**money laundering** lapses of extraordinary breadth. Among them, according to the documents:

* The **bank** understaffed its anti-**money laundering** compliance division and hired "gullible, poorly trained, and otherwise incompetent personnel." In 2009, the OCC deemed a senior compliance official at HSBC to be incompetent - the same executive in charge of implementing a new anti-**money laundering** system.

* HSBC failed to review thousands of internal anti-**money laundering** alerts and generate legally required suspicious

activity reports, or SARs, on transactions picked up by the **bank**'s internal monitoring system. SARs are important because they are sent to U.S. law enforcement and scrutinized for leads to criminal activity. In May 2010, the **bank**'s backlog of alerts was nearly 50,000 and "growing exponentially each month," according to one of the documents.

* Hundreds of billions of dollars moved unchecked each year through various **bank** operations because of lax due diligence and monitoring of accounts with foreign correspondent banks, which are financial institutions that rely on U.S. banks for processing services. The **bank** maintained accounts with "high risk" affiliates such as "casas de cambios" - Mexican foreign-exchange dealers - widely suspected of laundering drug-trafficking proceeds, and some Mexican and South American banks.

* In some instances, "management intentionally decided" not to review alerts of suspicious activity. An investigation summary also says, "There appear to be instances where **Bank** employees are misrepresenting" data sent to senior managers, and where management altered risk ratings on certain clients so that suspect transactions didn't set off alarms.

Sherman, the HSBC spokesman, said the **bank** cleared the backlog of alerts and has remained current. Sherman also said the **bank** "regularly reviews risk ratings. We have revised and strengthened our country risk rating review policies."

Spokesmen for the U.S. Attorney in Wheeling, West Virginia, and for the U.S. Attorney in Brooklyn declined to comment. The Justice Department in Washington also declined to comment, citing "an ongoing investigation into this matter."

THE MIAMI CONNECTION

HSBC was born in 1865 as the Hongkong and Shanghai Banking Corp in the then-British colony of Hong Kong. It had little presence in the U.S. market until its purchase in the 1980s of Marine Midland Banks Inc based in Buffalo, New York.

Now the fifth-largest **bank** in the world in terms of market value, HSBC had $2.6 trillion in assets at the end of 2011 and operations in 85 countries and territories. Its North American business, which includes HSBC **Bank** USA and a consumer finance unit, accounts for about 5 percent of HSBC's profit.

In 1999, HSBC's U.S. unit paid $10 billion to buy Republic New York Corp and a European affiliate, banks controlled by Lebanese financier Edmond Safra. The deal doubled HSBC's private **bank** to 55,000 clients with $120 billion in assets and broadened business in New York, Florida, Latin America and Europe.

The purchase also yielded one of the world's biggest banknote businesses, an operation that handles bulk cash exchanges between central banks and large commercial banks. In 2003, HSBC plunged into the U.S. market for subprime lending, paying $14 billion for Household International Inc.

By then, all banks faced U.S. regulatory pressure aimed at stopping shady money flows. In the wake of the September 11, 2001, attacks, the Patriot Act took effect, attempting, among other things, to choke off terrorist financing by strengthening requirements that banks look for and report suspicious activity. In recent years, U.S. law enforcement added an emphasis on money tied to the illegal drug trade.

When the 2003 order came down from regulators for HSBC to improve its anti-**money laundering** efforts, the **bank** had no centrally organized means of monitoring the movement of money across borders. That's when it hired Teresa Pesce. Pesce came from the high-profile U.S. Attorney's office in Manhattan, where she made a name for herself as a tough prosecutor overseeing **money laundering** prosecutions.

Pesce "knew the ropes," according to a person who worked in compliance at the time, and the sense among many staffers was that a "savior was here." One of her first initiatives was to order the installation of the Customer Account Monitoring Program, or CAMP, a technology system designed to filter suspicious retail transactions across HSBC's U.S. operations.

In 2006, regulators lifted their 2003 order, according to people familiar with the situation.

Pesce left the **bank** in 2007 to run KPMG LLP's anti-**money laundering** consulting business. A lawyer for Pesce declined to comment.

Despite Pesce's efforts, problems with HSBC's program persisted. In 2009, the OCC determined that Lesley Midzain, a compliance executive with little direct experience running anti-**money laundering** programs, was incompetent. She was in charge of the installation of a monitoring program to replace Pesce's CAMP system, which the OCC had determined was "inadequate to support the volume, scope and nature of international money transfer transactions," according to the documents reviewed by Reuters. Efforts to locate and obtain comment from Midzain were unsuccessful.

The former compliance-division staffer said that in the Miami office in particular, with millions of dollars from Mexico, Brazil, Argentina and other countries flowing through the Premier private-banking business for wealthy clients, "it was a nightmare to figure out what was going on down there."

Those observations mesh with allegations in a 2010 lawsuit against HSBC brought by Tomas Benitez, a longtime private banker in South Florida who had worked at Republic **Bank**. Benitez alleged that HSBC fired him in January 2009 after he warned colleagues that clients had violated U.S. restrictions on trade with Iran and Cuba.

HSBC said in a court filing that it fired Benitez for alleged sexual harassment - allegations Benitez denied.

In court documents, Benitez alleged that during an audit meeting in 2008, an unidentified federal **bank** examiner told HSBC employees that a client referred to only as "CM" "had multiple affiliations whose ties to Iran and Cuba were part of their ordinary course of business."

At a follow-up meeting, the account was discussed because of indications its owner "was funneling large amounts of funds in and out, with no apparent business purpose," Benitez alleged. He told Clara Hurtado, director of anti-**money laundering** compliance at HSBC's private **bank** in Miami, that the account had ties to Iran and Cuba and "as a result, it should not be maintained," according to the lawsuit.

After the meeting, Benitez alleged, another banker said "he would not allow Benitez's word and suspicions to defeat a million-dollar-plus account relationship." The account wasn't terminated, Benitez alleged.

Hurtado declined to comment. She left HSBC in 2009, according to her LinkedIn account.

In an email exchange submitted as an exhibit in the lawsuit, Hurtado and other HSBC employees discussed whether the **bank** could help a Miami client avoid violating U.S. sanctions by issuing letters of credit for the client from the **bank**'s Hong Kong offices, according to Benitez's lawsuit. "Clara, we are persuing (sic) another solutions..... (anything but losing the account!!!)," Suarez, the private banker, wrote in an email. The banker suggested issuing the letters of credit through Hong Kong.

In January 2009, HSBC fired Benitez. In late 2010, a federal judge dismissed his case and demand for pay, saying there was no evidence of a connection between Benitez's concerns about the accounts and the firing. The judge didn't address Benitez's allegations about illicit transactions.

Benitez's Miami lawyer, Mark Raymond, declined to comment on his client's behalf.

HSBC spokesman Sherman declined to comment on Benitez's case. "It's inappropriate to comment on unsubstantiated allegations in termination of employment cases," he said.

OBVIOUS TO STOOGES

Around the time Benitez was sounding warnings in Miami, authorities were accelerating an investigation in West Virginia of Barton Adams, a pain clinic operator in the Ohio River town of Vienna. In 2008, the U.S. Attorney in Wheeling indicted Adams on 157 counts of alleged healthcare fraud and other crimes. They allege that Adams moved hundreds of thousands of dollars in Medicare fraud proceeds between a U.S. HSBC account and HSBC accounts in **Canada**, Hong Kong and the Philippines.

Adams has pleaded not guilty.

In building their case against him, the West Virginia prosecutors determined that HSBC's compliance problems were systemic. As Ihlenfeld wrote in his letter to the Justice Department: "The Adams **money laundering** practices - which Moe, Larry, and Curly would dismiss as too transparent - would not be detected by HSBC regardless of who the customer was, or where any transaction occurred." HSBC, he said, "systematically and egregiously" violated the

Bank Secrecy Act.

One document reviewed by Reuters says HSBC developed a "large appetite for risk" after snapping up business with Mexican foreign-exchange houses formerly handled by Wachovia Corp. In 2010, Wachovia agreed to pay $160 million as part of a Justice Department probe that examined how drug traffickers had moved money through the **bank**.

West Virginia prosecutors focused much of their attention, according to the documents, on HSBC's failure to report suspicious activity on hundreds of billions of dollars in business from "high-risk" sources.

For instance, 73 percent of accounts with foreign correspondent banks were rated "standard" or "medium" risk and thus weren't monitored at all, the documents say, noting that oversight of such accounts was "extremely limited despite indications of possible terror financing." In one example, the **bank** "summarily cleared as many as 5,000" internal alerts of suspicious activity from correspondent customers in Argentina after lowering the country's risk rating.

Investigators cited a litany of failings in the **bank**'s back-office operations -- the vast but mundane business of clearing transactions by moving big sums of money around the globe. In the **bank**'s "remote deposit capture" business - an operation that electronically zaps checks around the world -- HSBC "failed to detect, review and report large volumes of sequentially numbered traveler's checks" from non-U.S. sources. Such checks are a red flag signaling possible **money laundering**, regulators have said.

HSBC also repatriated more than $106.5 billion in banknote deposits through foreign correspondent accounts, many of them in Mexico and South America, in a three-year period. And yet, "since 2005, the **bank** has filed only 19 suspicious activity reports relative to the receipt of bulk cash and banknote activities."

People familiar with HSBC and the reports said 19 is a low number given the risk of the clients. Between 2005 and 2010, banks and other depository institutions filed more than 3.8 million SARs, according to the Financial Crimes Enforcement Network, a bureau of the Treasury Department.

Similarly, investigators found that HSBC didn't report any suspicious activity after Drug Enforcement Administration agents posing as drug dealers deposited millions of dollars in Paraguayan banks and then transferred the money to accounts in the U.S. through HSBC. They have also been examining connections between one of the Paraguayan banks and Hezbollah, the Lebanon-based Islamist group classified by the U.S. as a terrorist organization. HSBC has since ended its relationship with the Paraguayan **bank**, according to government documents.

Ultimately, the U.S. Attorney's office in West Virginia entered into plea negotiations with HSBC, the documents show. A person familiar with the investigation said a deal could have resulted in one of the largest settlements ever in a **bank money laundering** case.

For reasons that aren't clear, prosecutors in West Virginia were told to stand down while the Eastern District of New York and other Justice Department divisions continued to investigate, according to a Justice Department document and an HSBC regulatory filing. The West Virginia probe could ultimately prove to be a narrow slice of a broader case if criminal or civil charges emerge.

KAMLOOPS Daily News

Bank scandals hint at problems

The Daily News (Kamloops)
Sat Dec 29 2012
Page: C1
Section: Opinion
Source: Winnipeg Free Press

American and British banks, one after another, have been engulfed by scandal this year, leaving Canadians to admire the probity of this country's banks, where nothing is ever found amiss.

HSBC, the venerable Hongkong and Shanghai Banking Corp., admitted this month it helped Mexican drug lords launder $881 million in drug-trade profits. The **bank** agreed to pay $1.92 billion in fines and improve its internal controls in relation to drug-**money laundering**, sanctions busting and other shady dealings.

Meanwhile in London, three people, including a former trader at Union des Banques Suisses (UBS) and Citigroup, were arrested Dec. 13 in connection with an official investigation of interest-rate manipulation.

Leading banks have for years been abusing the daily settings of the London Interbank Offered Rate (Libor) by submitting fake estimates of the rates they would have to pay to borrow funds from other banks. By nudging the posted rate up or down, they can raise or lower their interest costs or the value of contracts they have issued. Barclays paid a hefty fine in June and its chief executive resigned over Libor manipulation. Investigators then turned their attention to the roles of Royal **Bank** of Scotland and UBS, which pleaded guilty to fraud last week and agreed to pay $1.5 billion in fines to Swiss, British and U.S. authorities.

In **Canada**, the slate is surprisingly clean – so clean that it is hard to know what to make of it. **Canada**'s banks have never liked washing their dirty linen in public for fear of undermining confidence. But the public is keenly aware that banks' linen occasionally is soiled. It would be heartening to see some washing done – not laundering of drug profits but enforcement of integrity within the banking world.

THE CANADIAN PRESS

Editorial Exchange: Banks hide dirty laundry; Editorial Exchange: Banks hide dirty laundry

Canadian Press
Thu Dec 27 2012
Section: National
Byline: Winnipeg Free Press

An editorial from the Winnipeg Free Press, published Dec. 26:

American and British banks, one after another, have been engulfed by scandal this year, leaving Canadians to admire the probity of this country's banks -- where nothing is ever found amiss.

HSBC, the venerable Hongkong and Shanghai Banking Corp., admitted this month to U.S. authorities that it helped Mexican drug lords launder $881 million in drug-trade profits. The **bank** agreed to pay $1.92 billion in fines and improve its internal controls in relation to drug-**money laundering**, sanctions busting and other shady dealings.

"We accept responsibility for our past mistakes. We have said we are profoundly sorry for them, and we do so again. The HSBC of today is a fundamentally different organization from the one that made those mistakes," HSBC chief executive Stuart Gulliver said.

Meanwhile in London, three people, including a former trader at Union des Banques Suisses (UBS) and Citigroup, were arrested Dec. 13 in connection with an official investigation of interest-rate manipulation.

Leading banks have for years been abusing the daily settings of the London Interbank Offered Rate (Libor) by submitting fake estimates of the rates they would have to pay to borrow funds from other banks. By nudging the posted rate up or down, they can raise or lower their interest costs or the value of contracts they have issued. Barclays paid a hefty fine in June and its chief executive resigned over Libor manipulation. Investigators then turned their attention to the roles of Royal **Bank** of Scotland and UBS, which pleaded guilty to fraud last week and agreed to pay $1.5 billion in fines to Swiss, British and U.S. authorities on account of its Libor manipulation shenanigans.

The investigations, the fines, and the resignations help to reassure the public that regulatory agencies are hard at work, keeping the bankers honest. But regulators and investigators can only deal with what they know about. The vast laundering operations of HSBC came to light only because a federal prosecutor in Wheeling, West Virginia, received a tip that HSBC was helping a local doctor launder the proceeds of Medicare fraud. The prosecutor started digging and eventually a great many abuses came to light.

HSBC management admits it did terrible things back in the old days -- 2008 and before -- but contends it has reformed itself. The public has to decide how far to believe that. Why would executives of the leading banks be more trustworthy today than they were a few years ago?

In November, HSBC reported "underlying profit before taxes" (disregarding change in the value of its own debt) of $5 billion for the third quarter of 2012, up 125 per cent compared to the third quarter of 2011. This was after a U.S. Senate report had drawn attention to HSBC's large role in **money laundering**. Dishonesty and the reputation for dishonesty, it appears, are not necessarily bad for business and might even be helpful.

Confidence in banks might be encouraged if the public saw that banks are enforcing standards of integrity on their employees. Personal saintliness is probably no more common among Canadian **bank** officers than it is in the rest of mankind or at the top levels of Barclays, HSBC and UBS. But the Canadian banking tradition of quietly covering up scandals prevents the public from knowing what happens to dishonest bankers in **Canada**. We know something of

the scope of the problem in the U.S. and the U.K. because the authorities there took a close look and announced what they found. We also know what corrective steps have been taken.

In **Canada**, the slate is surprisingly clean – so clean that it is hard to know what to make of it. **Canada**'s banks have never liked washing their dirty linen in public for fear of undermining public confidence. But the public is keenly aware, from U.S. and U.K. experience, that banks' linen occasionally is soiled. It would be heartening to see some washing being done – not laundering of drug profits but enforcement of integrity within the banking world.

infomart

NORTHERN DAILY NEWS

U.S. seizes $150M from Hezbollah-linked Lebanese Canadian Bank

The Kirkland Lake Northern News
Fri Aug 24 2012
Page: B1
Section: News
Byline: JESSICA HUME, QMI AGENCY

OTTAWA --The $150 million seized by American authorities in an international Hezbollah-linked **money-laundering** scheme that involved the now-defunct Lebanese Canadian **Bank** has "no Canadian connection," the U.S. Drug Enforcement Administration says.

The U.S. treasury department and DEA said the Lebanese Canadian **Bank** (LCB) acted as a conduit funnelling funds through numerous countries into the hands of Hezbollah, a Shia militant group and political party in Lebanon.

The DEA said at least $329 million was wire transferred from the **bank** and others to the U.S. for used cars that were shipped to West Africa. Cash from the car sales was sent to Lebanon through Hezbollah-controlled channels. "As we alleged last year, the Lebanese Canadian **Bank** played a key role in facilitating **money laundering** for Hezbollah-controlled organizations across the globe," Michele M. Leonhart, administrator of the DEA, said in a statement Monday.

The LCB has a Montreal office, but the institution is based in Beirut. However, the **bank** had a "representative office" in **Canada**, meaning they were barred from receiving deposits and making transfers. LCB was only allowed to promote the services it provided in Lebanon. Its license was revoked last year by Finance **Canada** after a complaint was filed in the U.S. about the LCB's activities. Rusty Payne of the DEA's public affairs office said none of the money transferred through the LCB was sourced in **Canada**.

"There is no Canadian connection," Payne told QMI Agency. But that doesn't mean Hezbollah isn't active in **Canada**. Matthew Levitt of the Washington Institute for Near East Policy, says the group has an extensive network in **Canada** and it conducts primarily procurement work - purchasing dual-use technologies, for example, and redistributing them back to Hezbollah. In December 2011, Hezbollah's secretary general Hassan Nasrallah was asked about the group's presence in **Canada**.

"Yes," Nasrallah responded and Levitt reported in a paper. "Hezbollah has members in Montreal, Ottawa, Toronto; in all of **Canada**."

In one of Levitt's reports, he says in addition to fundraising and espionage, Hezbollah has activated sleeper cells in **Canada**.

"But they're primarily using North America as a cash cow," Levitt said. In a statement, U.S. Attorney for the southern district of New York Preet Bharara said the investigation and seizure of money on Tuesday is a big step in fighting terrorism.

"Money is the lifeblood of terrorist and narcotics organizations, and while banks which launder money for terrorists and narco-traffickers may be located abroad, today's announcement demonstrates that those banks and their assets are not beyond our reach," Bharara said.

Both the Canadian and U.S. government designate the radical Islamist group Hezbollah a terrorist organization.

Edition: Final

NATIONAL POST

Latest example of banksterism shows why faith in capitalism is fading

Financial Post | Opinion
Fri Jul 13 2012
Section: Diane Francis
Byline: Diane Francis

Another sordid example of banksterism - **money laundering** - surfaced this week accompanied, not surprisingly, by a blistering global poll that shows faith in capitalism is shrinking.

HSBC (Hong Kong and Shanghai **Bank** Corp.), the largest financial institution in Europe, revealed "major internal-control problems" and plans to apologize for its lapses next week to a U.S. Senate subcommittee into **money-laundering** and terrorist-financing activities. The **bank** could pay up to US$1-billion in fines, according to news stories.

Related

Barclays Diamond denies lying to Libor inquiry

U.S. Fed knew of Libor problems in 2007

Fallout from Libor scandal likely to hit **Canada**'s financial industry

HSBC is also embroiled with more than a dozen others in the gigantic Libor interest rate rigging scandal, along with Barclays, that has been in the headlines. Banks could pay fines of up to US$22-billion worldwide, say some analysts.

The **bank** issued a candid statement in advance of the Senate hearing: "Our anti-**money laundering** controls should have been stronger and more effective, and we failed to spot and deal with unacceptable behavior," Stuart T. Gulliver, the chief executive of HSBC, wrote in a memo to employees on Wednesday.

The period when the **money laundering** occurred was between 2004 and 2010, before its current management took over.

This scandal plus the LIBOR price fixing has sparked another large-scale Parliamentary probe into British banking in general, similar to one that probed Rupert Murdoch's media empire recently. Just as then, there are calls for an overhaul across the entire "banking culture."

What's also parallel, in political terms, is that HSBC's former chairman, Stephen Green, (in office from 2006 to 2010 when the **money-laundering** detection problems occurred) is currently trade minister in British Prime Minister David Cameron's government. Likewise, Cameron's former director of communications, Andrew Coulson, had left problems behind at the Murdoch empire then was forced to leave 10 Downing Street this spring because of the inquiry. He was recently arrested for perjury.

HSBC shares have tumbled as the market was notified on the Senate's website as to its agenda for Tuesday: "a hearing on the **money laundering** and terrorist financing vulnerabilities created when a global **bank** uses its U.S. affiliate to provide U.S. dollars, U.S. dollar services, and access to the U.S. financial system to high risk affiliates, high risk correspondent banks, and high risk clients, using HSBC as a case study."

But bad banking is only one issue. Another has been the continuing proliferation - and lack of action by governments or banks - against secrecy havens. The Organization for Economic Co-operation and Development has crusaded against this for years, the G-7 and G20 have issued countless manifestos against the practice, but absolutely nothing changes. Without prohibiting dirty money havens, the world's capitalist system can never been reformed because they hold billions of dollars worth of deposits on behalf of corrupt dictators or cunning political and business leaders.

This could easily be solved if the world's nations banned travel and trade with these places. The list was published this month by the OECD and contains some surprising countries: The "blacklist" includes Costa Rica, Philippines and Malaysia. Under the heading of "non cooperative countries" are Austria, Belgium, Brunei, Chile, Guatemala, Luxembourg, Singapore and Switzerland.

Then there is the so-called "grey list" of countries that have committed to change, whatever that means, but as yet haven't. These include the usual suspects: Andorra, Anguilla, Antigua and Barbuda, Aruba, Bahamas, Bahrain, Belize, Bermuda, British Virgin Islands, Cayman Islands, Cook Islands, Cyprus, Dominica, Gibraltar, Grenada, Guernsey, Isle of Man, Jersey, Liberia, Liechtenstein, Malta, Marshall Islands, Mauritius, Monaco, Monserrat, Nauru, Netherlands Antilles, Niue, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and Grenadines, Samoa, San Marino, Seychelles, Turks and Caicos Islands, US Virgin Islands, Vanuatu and Uruguay was recently added to this list.

Such malpractice, and accompanying immorality, are demoralizing enough to ardent free enterprisers like myself, but it has created a global backlash against

capitalism itself.

This week, the Pew Research Center released the results of its 21-country survey of 26,210 people. They have become increasingly pessimistic and disenchanted with capitalism since 2008.

To no one's surprise, respondents in fast-growing emerging economies untouched by the financial crimes of 2008 onward, have rosier outlooks and positive opinions toward capitalism. These include countries such as Brazil, China and Turkey.

But formerly rich basket cases such as most of the EU (Germany excepted), Japan and even the recovering U.S. or **Canada**, have increasing numbers of people who have been, or will be, left behind. They are dissatisfied with the status quo.

Of the 21 countries surveyed, only in China, Germany and Egypt do more than half of respondents say they are content with their nation's direction. Those who are angry about their national situation and direction mostly blame banks and financial institutions. As for belief in capitalism, only half of the respondents in 11 countries agreed that free markets were the best system.

Canadian opinions were not measured separately, but an April poll showed that the majority of Canadians living in booming Manitoba, Saskatchewan and Alberta were happy and confident, but Canadians living elsewhere were not. They worried about the future and a large proportion, with 30% claiming they had become incapable of making ends meet.

Frankly, banks, as poorly as they have performed, are not the only culprits that have caused the demoralization of rich nations. This is what the Great Markdown looks like after decades of spendthrift governments and a declining work ethic contrasted with thrift and hard work in emerging economies. It will only worsen.

Length: 919 words
Idnumber: 201207130139
Permalink: opinion.financialpost.com...»

The Sudbury Star

Punishment not enough to prevent banks from commit ing fraud

The Sudbury Star
Sat Nov 2 2013
Page: A10
Section: Editorial/Opinion
Byline: ALAN SHANOFF

Why are banks so susceptible to fraud? I don't mean fraud committed against banks, but rather fraud perpetrated by banks or fraud facilitated by **bank** conduct.

In September, the Toronto- Dominion **Bank**'s U.S. branch was fined $52.5 million by U.S. regulators for its role in a $1.2 billion Ponzi scheme operated by a lawyer, Scott Rothstein.

According to the U.S. Department of the Treasury, the **bank** ignored customer account activity which "repeatedly triggered alerts in the **Bank**'s anti-**money laundering** monitoring system." According to the SEC, the **bank** "defrauded investors by producing a series of misleading documents and making false statements about accounts that Rothstein held at the **bank** and used to perpetuate his scheme."

Last year the Royal **Bank** of **Canada** agreed to pay $17 million to settle a class-action lawsuit with victims of a Quebec Ponzi scheme operated by Earl Jones. Of course, it didn't admit liability. RBC Dominion Securities and two brokers were also fined $700,000 for "failing in their duty to protect the financial markets" from the Ponzi scheme.

According to the book, Thieves of Bay Street : How Banks, Brokerages and the Wealthy Steal Billions From Canadians, by investigative journalist Bruce Livesey, RBC "overlooked glaring clues that Jones was running a scam."

Bernie Madoff has implicated banks in his massive Ponzi scheme, stating various banks and hedge funds engaged in "willful blindness", adding "they had to know".

Of course, we can't forget the CIBC's role in the Enron fraud, which resulted in creditors' losses of $38 billion. The **bank** settled civil claims of $2.4 billion (US) and paid an additional $80 million (US) in fines to the Securities and Exchange Commission.

Plus, we can't overlook the role of the banks, including Canadian banks, in the financial crisis of 2008 related to the sale of subprime mortgages and other forms of bad debt converted into investment products and sold to an unsuspecting public. Nor can we overlook the manipulation of interest rates in the Libor scandal. According to Bloomberg Businessweek banks deliberately reported false borrowing costs which affected the "value of trillions of dollars of derivatives contracts, mortgages and consumer loans."

These are but a few recent examples of **bank** misconduct. It's almost as if there is a virus that has affected banks worldwide. Our supposedly staid, conservative Canadian banks haven't proven immune. We can't blame this on rogue employees.

They are too many incidents taking place over long periods of time to believe that.

Which leads me to ask what is it about banks and their culture that makes them susceptible to bad behaviour?

The answer is multi-faceted, but surely we must focus on the fact many banks have become above the law.

Sure, banks are sued and fined. Sometimes their employees are even prosecuted. But we never adequately punish banks.

If we impose fines that would actually hurt, we risk a **bank** failure, or harming shareholders.

In **Canada**, where we have a **bank** oligopoly with a limited number of chartered banks, each one is almost too big to fail.

If we were to levy appropriate penalties, we'd risk another financial crisis and further government intervention into the financial system.

Thus banks appear to have little incentive to perform their roles as "gatekeepers to the capital markets", to comply with laws set up to weed out money launderers, Ponzi schemers or fraudsters, or not to sell us ill-conceived products they know are doomed to fail.

Since banks and bankers seem to love money, perhaps the only way to modify their behaviour is collective punishment. Perhaps we could prohibit **bank** executives from collecting bonuses in any year in which their banks engaged in or allowed others to engage in fraud.

Perhaps we could prohibit **bank** directors from receiving fat directors' fees in such years.

That and criminal prosecutions, putting people in jail, might just work.

Whistleblower: HSBC Still Laundering Money for Terrorists, Drug Cartels

(Truthstream Media.com)

Big banks are apparently too big to jail, even when they bankroll terrorists and drug cartels, while regular people fill the prisons in the world's largest drug population for mostly non-violent drug offenses.

As a former Anti-Money Laundering Officer at HSBC, Everett Stern was arguably never actually supposed to catch money laundering activity. Instead, with little training but an inclination to make a difference, Stern caught massive levels of fraud, and contacted CIA and FBI officials in the summer of 2010 to alert them of systematic financing for terrorist organization, drug cartels and other shady entities.

HSBC was eventually fined $1.9 billion dollars by the U.S. Treasury, but Stern recently joined Occupy Wall Streets' Alt Banking protest (See video) – despite being a self-described conservative Republican – to call for criminal charges and accountability over what he says is continued money laundering on the part of HSBC officials.

Luke Rudkowski, of We Are Change, spoke with Everett Stern about his whistleblowing activities, and how he says the bank deliberately set itself up to fail at catching laundering transactions:

Certain companies and individuals flagged for illicit and criminal behavior are officially flagged in the system, and prohibited from authorized trade. But according to Stern, executives inside the system learned how to simply reclassify the coding to allow payments to go through to these entities.

Hundreds of millions of dollars were funneled to terrorist organizations including Hamas and Hezbollah – via the firm Tajco, operated by the Tajideen brothers – as well as drug cartels like Sinaloa and Los Zetas and Russian mobsters.

At the center of Everett Stern's (@Twitter) whistleblowing allegations is an account of how HSBC gave the appearance of putting into place a serious anti-money laundering unit, while in actuality it hired low level debt collectors with little to no experience, after it sold off its card card division to Capitol One.

Rolling Stone's February 2013 article 'Gangster Bankers: Too Big to Jail' helped but Everett Stern's case in the spotlight. In it, Matt Taibbi explained the circumstances that led to Stern catching the illegal activity:

> From the outset, Stern knew there was something weird about his job. "I had to go to the library to take out books on money-laundering," Stern says now, laughing. "That's how bad it was." There were no training courses or seminars on money-laundering – what it was, how to detect it. His work mainly consisted of looking up the names of unsavory characters on the Internet and then running them through the bank's internal systems to see if they popped up on any account names anywhere.
>
> Even weirder, nobody seemed to care if anybody was doing any actual work.

Later, Stern took it upon himself to look up suspicious names, research their connections on the Internet, and try to find them in the financial transactions database:

> Soon enough, though, out of boredom and also maybe a little bit of patriotism, Stern started to sift through some of the backlogged alerts and tried to make sense of them. Almost immediately, he found a series of deeply concerning transactions. There was an exchange company wiring large sums of money to untraceable destinations in the Middle East. **A Saudi fruit company was sending millions, Stern found with a simple Internet search, to a high-ranking figure in the Yemeni wing of the Muslim Brotherhood. Stern even learned that HSBC was allowing millions of dollars to**

> **be moved from the Karaiba chain of supermarkets in Africa to a firm called Tajco, run by the Tajideen brothers, who had been singled out by the Treasury Department as major financiers of Hezbollah.** [emphasis added]

Stern, who wanted to become a clandestine CIA agent to fight terrorism, says he's now under threat of legal action from HSBC, but shrugged it off, telling Luke Rudkowski that he considers blowing the whistle about these activities to be a "national security issue." Stern previously testified as a federal witness in the U.S. Government's probe into HSBC money laundering, but unsatisfied, he continues his efforts through the grassroots to demand justice for officials involved and an end to their activities.

As Taibbi wrote, "the U.S. Justice Department granted a total walk to executives of the British-based bank HSBC for the largest drug-and-terrorism money-laundering case ever. Yes, they issued a fine – $1.9 billion, or about five weeks' profit – but they didn't extract so much as one dollar or one day in jail from any individual, despite a decade of stupefying abuses."

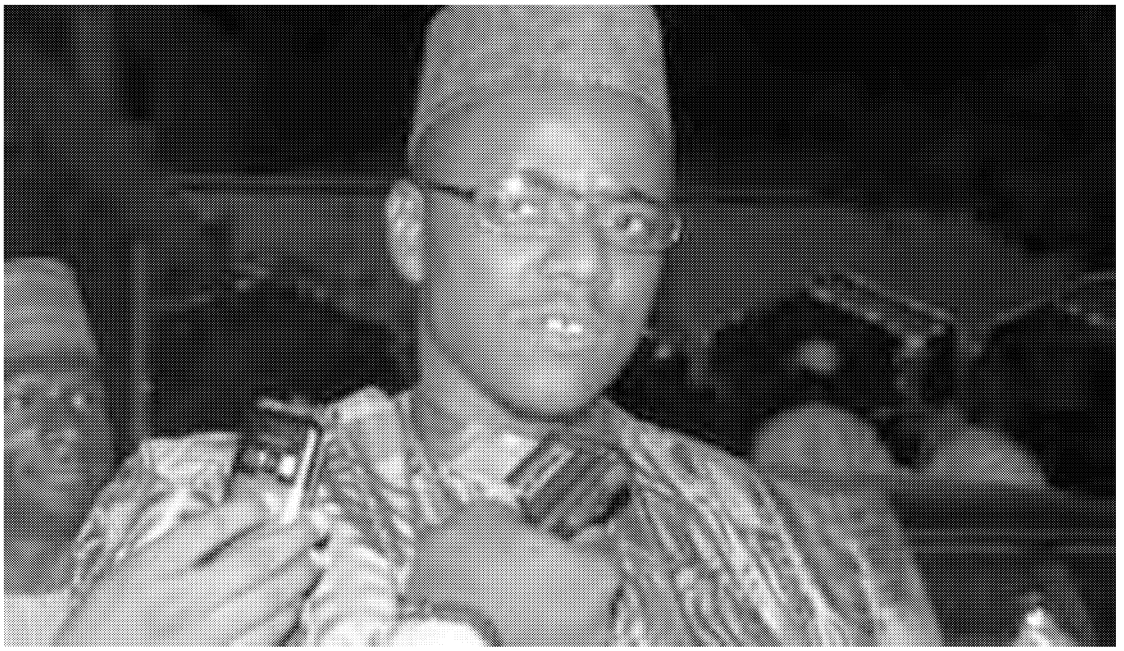
HSBC, based in London, with U.S. offices in Delaware and around the world, is by no means the only major bank involved in money laundering for terrorists and drug dealers.

In 2011, the *London Guardian* reported on how Wachovia – now part of Wells Fargo – also found itself in hot water for "failing to maintain an effective anti-money laundering programme" back in 2006 after Mexican troops intercepted a plane carrying 5.7 tonnes of cocaine and $100 million, which were later traced back to laundering activities through the bank. Charges were brought against the bank, but resulted in only a relatively small fine. The Guardian reported:

> Criminal proceedings were brought against Wachovia, though not against any individual, but the case never came to court. In March 2010, Wachovia settled the biggest action brought under the US bank secrecy act, through the US district court in Miami. Now that the year's "deferred prosecution" has expired, the bank is in effect in the clear. It paid federal authorities $110m in forfeiture, for allowing transactions later proved to be connected to drug smuggling, and incurred a $50m fine for failing to monitor cash used to ship 22 tons of cocaine.

Money Laundering: SSS Detains Staff of 13 Banks over Lamido's Son

16 Nov 2013 Font Size: a / A



Aminu Suleiman Lamido

Jigawa governor's sons in EFCC's custody

Presidency denies claim that Jonathan was informed of a $250m bribery allegation

By Ike Aboyin, Jaiyeola Andrews, Adebiyi Adedapo and Obinna Chima

Senior personnel of 13 Nigerian banks have been languishing in detention in the holding facility of the State Security Service (SSS) for almost two weeks over allegations of terrorist financing and money laundering believed to have been perpetrated by Aminu Suleiman Lamido, son of Jigawa State Governor, Alhaji Sule Lamido.

Also on Thursday, Aminu and his brother, Mustapha Lamido, were arrested by EFCC over an alleged N10 billion fraud. They were arrested in Kano and flown to Abuja Friday and have since been under interrogation at the commission's headquarters.

The banks whose staff have been picked up are Fidelity Bank Plc, First City Monument Bank Plc (FCMB), Wema Bank Plc, Access Bank Plc, Skye Bank Plc, First Bank Nigeria Limited (FBN), Sterling Bank Plc, Diamond Bank Plc, Zenith Bank Plc, Unity Bank Plc, Ecobank Plc, Guaranty Trust Bank Plc (GTBank) and Citibank. The SSS, which has been on the trail of Aminu Lamido, THISDAY learnt, had sought an ex parte motion from the Federal High Court, Abuja, to freeze the accounts, in 13 banks, of Adold Engineering Company Limited, believed to be owned by the governor's son.

A copy of the ex parte motion, which was obtained from the court by THISDAY, showed that order to freeze the accounts was granted by Justice A.F.A Ademola on November 6, 2013.

It stated: "An order is hereby made freezing the accounts of the underlisted corporate body and financial institutions in the banks (1st – 14th respondents) indicated against their names for their suspected involvement with acts of terrorists' financing and money laundering.

"An order is hereby made compelling the 2nd to 14th respondents (the banks) in this case to deliver up and furnish the State Security Service/applicant in this case with the respective bank statements and mandate cards of the 1st (Adold

Engineering) and 2nd respondents (Fidelity Bank) in this case.

"An order of the Honourable Court is hereby made keeping the above listed accounts frozen until the conclusion of investigations.

"That the ex parte order of the court made is to last for one month from date of service on the respondents with liberty to party(ies) to comply to this court as they deem fit within the said period."

The ex parte granted by the court further showed Adold Engineering operated the following accounts; in FCMB – 11 accounts; Wema Bank – one account; Access Bank – three accounts; Skye Bank – four accounts; FBN – five accounts; Sterling Bank – three accounts; Diamond, Zenith and Unity Banks – one account each; Ecobank – two accounts; while GTBank and Citibank have one account each.

THISDAY further gathered that most of the staff of the banks were either picked up from their homes in Gestapo style, at bank branches, or were invited by SSS operatives in Lagos, Abuja, Jigawa and Kano, and whisked away to the SSS headquarters in Abuja, where they have been in detention for up to two weeks.

In the case of one of the affected banks, THISDAY was made to understand that their Chief Compliance Officer, GM Northern Operations, Kano and Jigawa Branch Managers, Chief Inspector, Head of Treasury and Head of IT have been the guests of the SSS for two weeks.

A source revealed that in one instance, the SSS operatives went to the homes of one bank official wielding menacing Uzi machineguns and ransacked the home, slit mattresses and children's clothes during their search for documents.

What is most worrisome for the banks is that none of the affected staff have been given access to their families and lawyers during the entire period of their detention.
A Central Bank of Nigeria (CBN) official who is aware of the clampdown on banks by the SSS said: "The situation is most worrisome because these personnel have been in detention for more than ten days.

"Our laws provide that no one can be detained for more than 48 hours and if the SSS has a case against them, they should be charged to court instead of holding them for days unend.

"We are also concerned that the SSS lacks the capacity to carry out a thorough investigation on financial crimes of this nature, as the Economic and Financial Crimes Commission (EFCC), which works in conjunction with the Nigerian Financial Intelligence Unit is better suited to these kinds of investigations.

"Besides, all the banks render anti-money laundering returns daily to the CBN and EFCC under an automated system, so if the SSS had made the relevant enquiries they could have been furnished with all the details they needed."

Another source in the banking industry alleged that the clampdown on banks goes beyond the allegations of terrorist financing and money laundering against Aminu Lamido, as the dragnet is being expanded to include Kano State and other states governed by the G7 governors.

"We believe this goes beyond the allegations against the governor's son. We are aware that Kano State Government is the next target and could also involve other G7 states. It may be more political than anything else," a bank official informed THISDAY.

When contacted, spokesperson for the SSS, Ms. Marilyn Ogar, confirmed that the SSS was investigating massive money laundering and corruption alleged to have been perpetrated by Aminu Lamido through his company, Adold Engineering.
She dismissed allegations that the SSS was targeting the G7 governors and the finances of their states, stressing, "The SSS is investigating massive money laundering and corrupt practices. That is all I can say on the matter. If the banks feel aggrieved, they should go to court."

Another SSS source also informed THISDAY that the security organisation has a holding charge for the bank officials until it concludes its investigation. Aminu Lamido has had a run in with the law in the past. About a year ago, he was arrested at the

Aminu Kano International Airport, Kano, for failing to declare $50,000 he had in his possession. He was later charged to court for money laundering.

Over N10 billion was allegedly transferred from Jigawa State Government accounts into the accounts in which the governor and his two sons have interest from 2007 till date.
EFCC is reported to have traced these transfers to 10 companies where Lamido and sons are directors and signatories to the accounts.

Some of the companies linked to the accounts include Bamaina Alluminium Limited, Bamaina Holdings Limited, Bamaina Company Nigeria Limited, Rawda Integrated Services Limited, Speeds International Limited and Saby Integrated Nigeria Limited.

Confirming the arrest yesterday in Abuja, the commission's Head of Media and Publications, Wilson Uwujaren said Aminu Lamido and Mustapha Lamido were arrested Thursday night in Kano over financial crimes running into billions of naira.
"I cannot tell you specifically the amount involved, but it runs into billions of naira," he said.

He also confirmed that the suspects were brought to the commissions headquarters in Abuja for interrogation.

Uwujaren explained that the arrest was an extension of Aminu's arrest in December 2012 for being in procession of $50, 000 at the Kano International Airport, and linked the Governor to illegal deals.

According to him, further investigation into Aminu's sources of income revealed other transactions which implicated his brother and their father.

"I am confirming to you that both Mustapha Lamido and Aminu Lamido were arrested last night in Kano and they were brought to Abuja this morning. They were arrested for money laundering investigation," he said. He added that "The 2012 case has been concluded and conviction secured, but further investigations about Aminu's sources of income revealed details of financial transactions involving him, his brother and the Governor himself."

Asked whether Governor Lamido would be invited to answer questions on the allegation, Uwujaren said investigations were still ongoing, but added that the governor maybe invited if need be.

He maintained that the issue of bail had not arisen as they were still undergoing interrogation.
"Nobody is discussing bail with them now, like I said, they are still undergoing interrogation," he said.
In another development, the Presidency yesterday denied the claim by Governor Lamido that he informed President Goodluck Jonathan that a serving minister collected $250m bribe and the President failed to act on the information.

A statement issued by the Special Adviser to the President on Media and Publicity, Dr. Reuben Abati, said: "We have noted with much regret, the grossly irresponsible, false and mischievous claim by the Governor of Jigawa State, Alhaji Sule Lamido that President Goodluck Jonathan has refused to act on information that a serving minister recently collected a bribe of $250 million from an oil company.

"The Presidency views the patently bogus allegation reportedly made by the Governor in a radio interview yesterday as an unacceptable and callous attempt to unjustly impugn the integrity of President Jonathan and cast aspersions on the seriousness of his Administration's efforts to curb corruption".

Noting that the allegation was absolutely without any foundation in fact or reality, because no such communication occured between them, the statement said, "We abhor Governor Lamido's descent to the unscrupulous, reckless and thoughtless peddling of arrant falsehood in a puerile effort to score cheap political points against President Jonathan for personal and sectional political gains.

"If, as he claims, Alhaji Lamido has credible information about a minister receiving the said amount as bribe, he should publicly name the minister involved without delay and provide evidence to support his allegation.

"In the event that he is unable to do so, he should be prepared to offer an unreserved apology to the President and Nigerians

for his unwarranted and unjust effort to denigrate, disparage and malign the President and the Federal Government" the Presidency said.

Tags: News, Nigeria, Featuered, money laundering

THE JERUSALEM POST
Israel's best-selling English daily and most-read English website

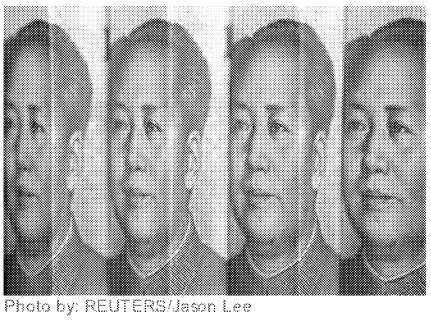


Photo by: REUTERS/Jason Lee

NY appeals court rules to apply Israeli law in Bank of China terror financing case

By YONAH JEREMY BOB
20/09/2013

Ruling seen as victory for families of terror victims suing Bank of China; Israeli law uniquely strict on indirect aid of terror finance.

Shurat Hadin – Israel Law Center won a significant battle in its terror financing case against the Bank of China, the center announced.

Shurat Hadin convinced the New York Appellate Division to apply Israeli law and keep the case, filed on behalf on 22 families, in New York, the center told The Jerusalem Post late on Thursday night.

The most dramatic aspect of the state appeals court decision was that it both reversed the lower New York court decision to apply New York law in the case, in favor of Israeli law, and it made this decision against recent precedents by the New York-based US Court of Appeals for the Second Circuit.

The state appeals court also reaffirmed the lower court's decision to keep the case in New York as opposed to moving it to China, and rejected outright the bank's appeal to apply Chinese law instead of either Israeli or New York law.

The court recognized the decision as significant, as Israeli law includes a right to sue and receive damages for violation of specific statutes, including a uniquely Israeli statute that places wide liability on banks and others that even indirectly aid or facilitate terrorists financing.

New York law's obligations on banks are more lenient regarding anything their clients may be involved in.

Certainly the entire case and chances of winning would have been radically different under Chinese law and in China than under Israeli law and in New York.

The victims and family members of victims of terrorist attacks perpetrated between 2004 and 2007 in Israel allege that starting in 2003, the Bank of China executed dozens of wire transfers for Hamas and Islamic Jihad totaling several million dollars.

The case is still far from trial or any sort of resolution, but unlike beating a regular motion to dismiss, where usually a plaintiff merely has to survive small procedural hurdles that do not impact the case later, this decision, especially in applying Israeli law, gives the plaintiffs a significant advantage at all points of the case going forward as the framework will always be one applying greater liability against the Bank of China.

The decision comes shortly after another major development where according to an ex-

The development comes shortly after another major development, where according to an exclusive report in the Post, key former Israeli government witness Uzi Shaya sent a letter out on the case that he was "inclined" to testify despite reports that China threatened to cancel Prime Minister Binyamin Netanyahu's visit to China last spring if Israel did not prevent Shaya from testifying.

Shurat Hadin had said that Shaya's letter would indicate that he has faced potential opposition from the Israeli government about testifying, but that he believes he can testify anyway.

Despite that belief, Shaya explained to Shurat Hadin that he wished to give the government time to formulate an official position, particularly since the government might, in the end, endorse his testifying.

In July, the bank's lawyers said that maybe the government was withholding Shaya's testimony because it believed his testimony would be inaccurate – though the court appeared to reject this out of hand.

The significant question of whether Shaya will testify is being reviewed by the government, according to an official letter response to the court from July 12 by deputy director of the international department of the State Attorney's Office, Yitzhak Blum.

The court expressed frustration that the letter did not give any deadline for an answer and indicated it would be responding to Blum's letter by requesting a deadline.

THE GLOBE AND MAIL

How a Canadian was charged with money laundering in sale of bitcoins

Tu Thanh Ha
The Globe and Mail
Published Wednesday, Feb. 12 2014, 3:11 PM EST
Last updated Wednesday, Feb. 12 2014, 9:00 PM EST

On a hot Florida morning a week ago, a young Quebecker named Pascal Reid showed up at a boutique hotel in Miami's Art Deco district, carrying a laptop and an electronic wallet that held $316,000 in digital currency.

Mr. Reid was expecting to meet a man who had purchased bitcoins from him before. The buyer was, in fact, an undercover agent for the U.S. Secret Service, which arrested Mr. Reid and charged him with money laundering.

More Related to this Story

- Federal Budget Canada to regulate bitcoin in war on dirty money
- Russia warns bitcoin could be used for financing terrorism
- Analysis To grow, bitcoin may need to shed its world of intrigue

The case has shone a spotlight on the way that virtual currencies such as bitcoin have been used for illicit purposes. The arrest is also significant because it targeted people using Localbitcoins.com, an online directory that is one of the last places where bitcoins can be traded anonymously, an expert said.

"Bitcoin may be pseudonymous, but actually buying and selling bitcoins anonymously is not easy," Nicholas Weaver, a senior researcher at the University of California at Berkeley's International Computer Science Institute, said in an e-mail interview.

He said there were past examples of criminals using Localbitcoins.com as a black-market venue. "Criminals have to buy their bitcoin using some anonymous method. Thus it is natural to expect law enforcement to continue to focus on anonymous transactions used to buy and sell significant quantities of bitcoin."

In Canada, concerns about the illicit use of bitcoins are reflected in Tuesday's federal budget, which stated that the government wants to bring in legislative amendments to regulate the "emerging risks" associated with online currencies such as bitcoin and prevent their use for terrorism or money

laundering.

According to his arrest form, Mr. Reid was told by the undercover agent that the money used to buy his bitcoins came from credit-card data stolen in the highly publicized hacking of the Target retail chain. Mr. Reid also asked the agent about buying forged identification papers, the police document alleged.

"The use of bitcoins in the transactions is a new technological flourish to this very old crime. Today's arrests may be the first state prosecutions involving the use of bitcoins in money-laundering operations," the office of Miami-Dade State Attorney Katherine Fernandez Rundle said in a statement after the arrest.

Mr. Reid is a 29-year-old Montrealer who moved to Florida about 15 years ago, according to his mother.

The allegations against Mr. Reid have not been tested in court. His lawyer, Ron Lowy, said the authorities are trying to send a message to other bitcoin users by prosecuting his client, who has pleaded not guilty.

The investigation began in early December last year when Secret Service Special Agent Mark Kramer went on the Localbitcoins.com website, looking for sellers of bitcoins. He saw that someone calling himself Proy33 could be contacted "anytime" to meet in public places and trade bitcoins for cash.

According to the arrest form, the agent texted Proy33, saying, "I want to start with about 600."

They met at a Starbucks, where Proy33 sold the bitcoins to Mr. Kramer, with a 20 per cent commission. Afterward, a surveillance team followed Proy33 to his Broward County home and identified him as Mr. Reid.

At a second meeting, Mr. Kramer bought nearly $1,000 in bitcoins and offered to sell stolen credit card data to Mr. Reid. The Quebecker declined but said he would "think about it," the arrest form says.

By the end of January, the two men agreed to a $30,000 transaction and Mr. Reid said he would send Mr. Kramer four to six bank account numbers to break up the deal into smaller portions, the arrest form alleges. Mr. Reid also told the agent that he would be flying to Switzerland to meet with bankers about bitcoins.

Mr. Reid later texted that "there has been some crazy stuff happening with cash deposits with Chase and Bank America since Saturday" and that they would need to meet in person.

They agreed to a rendezvous last Thursday at a beachfront hotel, the Casa Grande Suite.

They met around 9:30 a.m. and Mr. Kramer told Mr. Reid that the money used in the previous two

transactions came from credit-card data stolen in the Target hacking.

"Reid replied by stating that it would be good for the bitcoin community. Reid then redirected the conversation by asking if Kramer was able to obtain counterfeit Florida driver's licences and other counterfeit documents, such as social security cards and passports," the arrest form says.

The undercover officer mentioned the Target stolen credit-card data again and then showed a "flash roll" of $30,000 in $100 bills.

Mr. Reid inspected some of the cash, then, to prove that he was able to cover the deal, revealed that he had a wallet with 403 bitcoins, worth $316,000, the arrest form says.

Using a laptop, Mr. Reid completed the transaction, taking a $5,000 commission, the arrest form says. He was then arrested.

Less than two hours later, in the same hotel, in a similar investigation, investigators arrested Michell Abner Espinoza, a 30-year-old Peruvian who was approached on Localbitcoins.com in the same fashion as Mr. Reid.

Both men were each charged with two counts of money laundering and one count of operating an unlicensed money services business.

Mr. Reid is to return for a hearing in Miami-Dade criminal court on Feb. 27.

"He's a good kid. Never been any problem before, never, never, never," his mother, Chantal Desbois, said in an interview. "I don't know what could have happened. I don't understand."

Mr. Lowy, Mr. Reid's lawyer, described his client as a well-meaning "techno-geek" who is being scapegoated by authorities who are trying to send a message about the use of bitcoins.

"This is going to have a chilling effect on the public perception of bitcoins," he said in an interview.

infomart

NATIONAL POST

Euro brings risks to Latvian banks; Dirty money

National Post
Tue Dec 31 2013
Page: FP1 / Front
Section: Financial Post
Byline: Gary Peach
Dateline: RIGA
Source: The Associated Press

When Latvia adopts the euro on Jan. 1, it will bring with it a banking sector that is swelling with suspicious money from Russia and the east - just as the currency bloc is trying to clamp down on such havens.

It was just nine months ago that the eurozone had to rescue Cyprus, a similarly tiny member state that also specialized in attracting huge deposits from Russia. Since then, eurozone leaders have vowed to crack down on financial sanctuaries and improve transparency.

But as the 18th member of the eurozone, Latvia is likely to see a greater - not smaller - influx of dirty money as the country will be viewed as safer than other former Soviet states while financial oversight remains loose.

"Immediately after Latvia joins the eurozone, I imagine we're going to see an actual spike in dubious money flowing in," said Mark Galeotti, a professor at New York University who researches organized crime in the former Soviet Union.

For years, Latvia's political and financial leaders had hoped to create a mini-Switzerland in Eastern Europe - a place where capital in unstable countries such as Russia or Kazakhstan could either park for a while or channel its way further west to banking meccas like Zurich or London.

After a slight dip during Latvia's financial crisis in 2008-2010, the amount of non-resident bank deposits has risen rapidly over the past two years ahead of the country's entry into the eurozone.

"The issue with Latvia is that you have a pretty permissible political environment, and you have the massive and quite efficient infrastructure for managing these funds from the East. The question is, why wouldn't you want to go to Latvia?" Mr. Galeotti said.

Latvia has 20 domestically registered banks, or one for every 100,000 residents - an extremely high ratio. Of these, about 13 are considered "boutique banks" that rely almost exclusively on foreign funds, mainly from volatile countries of the former Soviet Union. Rather than lend to businesses and consumers, these tiny financial institutions primarily serve as safe havens or money transfer operations. They tend to keep their money in liquid assets so it can quickly be moved.

Some of the money is dirty. This year, Latvia's bank regulator slapped a 100,000-lat (US$200,000) fine on a bank for failing to exercise sufficient internal controls with money connected to the socalled Magnitsky case.

Sergei Magnitsky was a Russian **lawyer** who worked for Hermitage Capital, an investment fund whose chief executive accused Russian police officials of stealing US$230-million in tax rebates after illegally seizing Hermitage subsidiaries. In 2008, Magnitsky, at the age of 37, died in prison of pancreatitis, allegedly after being beaten and denied medical treatment.

Hermitage Capital claimed that tens of millions of dollars of the stolen money passed through Latvia.

Claiming confidentiality and a risk of destabilizing the industry, Latvia's regulator refused to "name and shame" the bank connected to the case. This refusal, as well as the small size of the fine, triggered criticism and renewed doubts about the regulator's integrity despite imminent eurozone membership.

"The regulators don't have teeth," Mr. Galeotti said. They maintain "a kind of culture that emerged in Latvia in the late 1990s ... which was ultimately 'Latvia desperately needs business, and therefore the role of the regulator is not to impede business,' " he said.

Non-resident bank deposits comprise nearly half of all deposits, which is unusual, and they are on the rise. In the first quarter of 2013, nonresident deposits soared 17.7% compared with the same period in 2012 - clear evidence that Latvia's attractiveness as a safe haven is not relenting. The economy has been the fastest-growing in the EU for the past three years and the country displays a remarkable degree of political stability.

"Latvia has historically had a large banking sector, has extremely strict data privacy laws, speaks Russian and 'gets' the post-Soviet mentality," said Tom Wallace, an analyst at C4ADS, a Washington, D.C.-based firm that specializes in data analysis and security.

Mr. Wallace, who co-authored a report on the links between Latvian banks and Ukrainian companies involved in the illicit arms trade, added that Latvia "is an EU member and so acts as a conduit to Western financial institutions. If you have money you want to discreetly move out of the former Soviet Union, Latvia has a lot of advantages."

Latvia's banks face scrutiny in a eurozone-wide review by the European Central Bank, which is trying to find weak spots in the financial sector to improve transparency and confidence.

The good news for the eurozone is that Latvia's banking system is not too big compared with its economy. That means the country is less likely to need a bailout from its new eurozone partners to save its banks, should they run into trouble, as happened with Cyprus.

As of Sept. 30, the banks held nearly 20-billion lats (US$30-billion) in assets, or about 120% of gross domestic product, far less than the average 320% in the eurozone in 2011.

On the flip side, for Latvia, the eurozone is now a safer economic bloc to join than it was 18 months ago, when many investors worried it would break apart. Markets have calmed since ECB vowed in the summer of 2012 to do whatever it takes to keep the bloc together.

Latvia's regulator says it has introduced a number of controls aimed at anti-**money laundering**, counter-**terrorist** financing and preventing excessively large sums from entering the banking system. Experts agree that the regulator has acknowledged the risks of dirty money and is addressing them, even if slowly.

But Latvian bankers say that pinpointing dirty money is not cut-and-dry.

"As anti-laundering regulations become more elaborate across the globe, so are the schemes used by persons who try to avoid them," said Arvids Sipols, who has worked 16 years in Latvian banks and is now on the board of Nord Capital Markets, a Riga-based asset management firm.

Illustration:
▪ Jason Alden, Bloomberg News Files / A Swedbank AB branch is illuminated against the night sky of Riga, the capital of the newest member of the eurozone.

NATIONAL POST

Criminals may exploit native banks: RCMP; Money Laundering; Tax-free status tempts organized crime, police say

National Post
Tue Oct 9 2012
Page: FP6
Section: Financial Post
Byline: Stanley Tromp
Source: Financial Post

Organized crime groups could exploit banks located on Canadian Native reserves to launder money and grow their profits, according to an RCMP criminal intelligence report.

"A recent Supreme Court of **Canada** decision created a new window of opportunity for organized crime groups," the RCMP warned in the November 2011 report on cigarette smuggling, obtained under the Access to Information Act.

That assessment followed a July 2011 ruling by **Canada**'s top court that interest income earned from deposits in banks located on reserves is not taxable under the long-standing Section 87 of the Indian Act, a decision that overturned two previous judgments, one from the Tax Court of **Canada**, and the other from the Federal Court of Appeal.

The appellant (a legitimate businessman) had earned interest on term deposits in an aboriginal credit union on the Mashteuiatsh Reserve in Quebec, even though he was a member of the Obedjiwan Reserve, where there was no bank. The majority ruled his membership location was unimportant, and also stated there was no need to consider whether under Section 87 the property or the activity which generated it "benefited the traditional Native way of life."

Yet two of the nine justices dissented, writing: "To grant the exemption in such circumstances would be tantamount to turning the reserve into a tax haven for Indians engaged in unspecified for-profit activities off the reserve."

The RCMP agreed, writing that, as a result of the ruling, "organized crime groups may seek to make arrangements with individuals of Native status to benefit from this tax protection. Such arrangements could be used to conceal the origins of illicit profits, as well as grow those proceeds with the tax protection through further investments.

"This decision has the potential to create barriers for law enforcement investigating the contraband tobacco market in First Nations reserves, as it provides an opportunity to launder earnings by filtering it through on-reserve bank accounts, and diverting the funds into the mainstream investment markets. It also provides an opportunity for tax evasion, and the ability to profit extensively from those earnings."

But some observers believe the RCMP warning is overstated, because the same cash reporting rules apply to aboriginal banks just as they did before the ruling, laundering is a separate topic from tax exemption and the judgment does not deal with forms of investment income other than interest on bank deposits.

"I just don't see how earning tax-free interest on the reserve would facilitate **money laundering**," said Jeffrey Pniowsky, a **lawyer** who intervened in the case for the Assembly of Manitoba Chiefs and who formerly worked for the Integrated Proceeds of Crime Unit of the Justice Department.

"That seems like a pretty far stretch," Mr. Pniowsky said. "The tax-free status was already happening, and this ruling only clarifies it. There is also a big difference between lawful tax avoidance and criminal tax evasion. Moreover, if there is a concern of natives increasing their exposure in the mainstream commercial world, so be it, and frankly speaking, their doing so is a good thing."

Aboriginal banks were created in **Canada** as one means to help raise natives out of poverty and economic dependence on the state. The National Aboriginal Capital Corporations Association (NACCA) was founded as a voluntary network in 1993 to aid aboriginal financial institutions. It has since developed into a formal association with 56 members, and for its members' guidance, its website publishes a sample Code of Conduct (modified from codes from the banking sector).

Point No. 11 states: "Prevent **money laundering** and fraud: we must comply with local laws, regulations and AFI standards on **money laundering** and fraud prevention."

On aboriginal banks' activity, Inspector Jean Cormier, acting director of the RCMP Proceeds of Crime Branch, said the ruling "would not change their reporting requirement under the Proceeds of Crime **Money Laundering** and **Terrorist** Financing Act."

Under the law, financial institutions in **Canada** must track cash transactions of more than $10,000 daily (or other large suspicious deposits) that could be used to fund criminal or **terrorist** activities within and beyond **Canada**'s borders, and report them to the Financial Transactions and Reports Analysis Centre of **Canada** (FINTRAC)

within 15 days.

FINTRAC posts 22 administrative penalties on its website (distinct from criminal penalties) that it imposed on named financial institutions since 2009, ranging from $3,190 to $169,080, for three credit unions but mostly money service outlets.

"Our first concern would be the initial deposit and introduction of any criminal proceeds of crime into accounts at any financial institutions," Insp. Cormier added. "The accumulation of interest is also of concern but secondary."

"The thing that might bring an elevated risk of **money laundering**," FINTRAC spokesperson Peter Lamey said, "is lack of compliance with the [Proceeds of Crime act], which is a separate matter from the court decision.

"This act applies to credit unions operated by aboriginal groups. If they are meeting their obligations under the law it should mitigate the risk that they might be used by criminals to launder money."

Edition: National
Length: 817 words
Idnumber: 201210090116

Tone: Negative
Ad Value: $9,462
Circulation: 159,480

NATIONAL POST

U.S. Fed warns Bank of Montreal on anti-money laundering controls

Financial Post | Business
Fri May 17 2013
Section: FP Street
Byline: Canadian Press

TORONTO - The Bank of Montreal and its U.S. subsidiary have agreed to beef up efforts to combat money laundering after American authorities found its operations in Chicago lacking.

The Canadian bank, U.S. Federal Reserve and an Illinois state agency have signed an agreement that gives BMO until late July to submit an acceptable plan for resolving the short-comings.

Among other things, the document says state and federal authorities identified problems when they examined the bank's branch in Chicago, where its BMO Harris Bank is based. The Fed said Friday the bank "lacked effective systems of governance and internal controls to adequately oversee" compliance with anti-money laundering rules.

Related

Canada's banks could be on the hook to bail out CMHC if disaster strikes

Oryx adds BMO as book runner on its $250-million IPO

BMO to open tiny 'studio' bank branches

Details of the deficiencies weren't disclosed in the document but it outlined steps for BMO to take including improved oversight by its board of directors and better internal training and reporting within the bank's organization. Bank of Montreal operates a U.S. consumer lending business in the U.S. Midwest through its Chicago-based BMO Harris Bank unit.

The agreement, dated April 29 and made public on Friday, outlines several deadlines for BMO to meet including an acceptable a written plan within 90 days and regular progress reports.

The bank said it was working to correct the problems.

"BMO is fully committed to the highest standards of regulatory compliance with Bank Secrecy Act/Anti-Money Laundering requirements and expectations in each of the jurisdictions in which we operate," BMO vice-president Paul Deegan said in an emailed statement.

In recent years, U.S. authorities have increased efforts to prevent criminals and terrorists from using the banking system for illicit activities. Among other things, it requires banks within its jurisdiction to comply with the Bank Secrecy Act's anti-money laundering requirements.

The 11-page agreement says BMO Financial Corp., the U.S. subsidiary that technically owns BMO Harris Bank, "lacked effective systems of governance and internal controls to adequately oversee the activities of Bank of Montreal's U.S. Operations with respect to legal, compliance, and reputational risks related to compliance with BSA/AML requirements."

Under the deal, the bank has agreed to provide funding for personnel and other resources to operate a system that "fully addresses the organization's compliance risks on a timely and effective basis."

THE HINDU

'HSBC arranged for opening of accounts abroad and withdrawal from Delhi itself'

Gargi Parsai

India Against Corruption members, Arvind Kejriwal, Prashant Bhushan and Shanti Bhushan addressing the media on money stashed in Swiss banks, in New Delhi on Friday. Photo: V.V.Krishnan The Hindu

Three from the list of 700, which was shared by France, disclose bank's modus operandi

India Against Corruption (IAC) released on Friday "the modus operandi" for transfer of undisclosed funds to Swiss banks as disclosed in the statements of three persons who had opened accounts in Dubai, Zurich and Geneva with HSBC Bank. They were named in a list of 700, which was shared by the French government in a compact disc with the Indian government last year.

The names of the 10 VIPs, including the Ambanis, Congress MP Anu Tandon, Jet Airways chief Naresh Goyal and the Burman brothers of the Dabur Group, were among the 700 whose names were not revealed by the government. The accounts held by them pertained to 2006.

IAC members Arvind Kejriwal and Prashant Bhushan said Parminder Singh Kalra and Praveen Sawhney, who gave their statements, were based in Delhi, while the third person, Vikram Dhirani, was from Ghaziabad.

The persons, who were questioned under Section 132 (4)/133A of the Income Tax Act, 1961, revealed the modus operandi of the "underground banking" system or the 'hawala' network (money transferred but not moved).

As per the papers released by IAC at a press conference here, Mr. Dhirani said in his deposition that he had opened an account with HSBC in Dubai in 2005 and closed it in 2006. A bank representative came to him in Delhi to open an account. He did not travel to Dubai for opening or operating it. The formalities was completed in Delhi. He agreed that a person authorised by bank officials would collect the cash from him, which would show up in his HSBC account in Dubai. After the money was deposited, Mr. Dhirani was given a confirmation. However, no document was given.

IAC said the statement revealed that Mr. Dhirani told income tax officials that he had deposited about Rs. 12 crore in alleged unaccounted income in the Dubai account over a period of time. The account was closed in 2006, and the money was withdrawn and given to him in Delhi. Neither did he go to Dubai to collect the cash, nor did he arrange for his representative to take the cash on his behalf. "The bank officials arranged for delivery of cash... in India."

According to IAC, Mr. Kalra opened an account with HSBC, Zurich, on the advice of a Swiss investment consultant based in Zurich. To make deposits of undisclosed money to the tune of Rs. 8 crore-Rs. 9 crore, he gave the cash in instalments to a person in Delhi. Every time, a different person came to collect the cash for being remitted in the Zurich branch of HSBC. The account was closed in 2008-09 even while he remained in Delhi.

"The statement shows," Mr. Kejriwal said, "that bank officials are providing illegal channels for transfer of cash from their client account-holder in Delhi to Zurich and vice versa."

He said Mr. Sawhney, who had opened an account with HSBC, Geneva, told income tax officials that his father had

transferred $ 1.8 million to this account. "Regarding the modus operandi for withdrawal of money, Mr. Sawhney said he used to call the bank officials in Geneva who would arrange for delivery of cash in India through their agents in the hawala channel. All discussions with the bank officials were on the phone. Every time he asked for cash, a different person used to come to deliver it and he knew none of them."

Keywords: Kejriwal allegations, Swiss bank accounts, tax evasion, Ambani brothers, anti-corruption movement, black money issue

BUSINESS

Tax Crackdown Broadens

HSBC Pushed on Secret Bank Accounts in India Unit

By BRENT KENDALL And EVAN PEREZ

Updated April 8, 2011 12:01 a.m. ET

WASHINGTON—The U.S. Justice Department on Thursday asked a federal court to force HSBC Holdings PLC to disclose the names of U.S. customers suspected of having secret bank accounts in India

The move opens up a new front in the U.S. crackdown on tax evasion and comes days before the April deadline for taxpayers to file individual returns. Previous cases focused on Americans with Swiss bank accounts.

In court documents, the Justice Department said HSBC bankers told prospective clients that, as a foreign bank, HSBC's India operations wouldn't disclose their accounts to the Internal Revenue Service.

Armed with that knowledge, U.S. customers "have been able to maintain these foreign accounts with reasonable confidence that the IRS would not discover them," government lawyers alleged.

Thousands of U.S. taxpayers of Indian origin have opened up accounts with HSBC in India since 2002, when the bank allegedly began soliciting their business, according to the U.S. government. It asked a San Francisco court to allow the IRS to serve a so-called John Doe summons against the U.K. bank's U.S. unit, HSBC USA, to get the names of its U.S. clients with Indian accounts.

Thousands of U.S. taxpayers of Indian origin have opened accounts with HSBC in India in recent years. Above, an HSBC bank in Mumbai. *Bloomberg News*

An HSBC spokeswoman in New York said the bank has been engaged in a "constructive dialogue" with U.S. authorities and hoped the summons issue "can be resolved expeditiously."

"While we haven't seen the summons, HSBC does not condone tax evasion and fully supports the U.S. efforts to promote appropriate payment of taxes by U.S. taxpayers," spokeswoman Juanita Gutierrez said.

She said the bank complies with the law in all the jurisdictions and cooperates with requests from U.S.

"Our international efforts are not about just one country or one bank; it's about our wider effort to ensure compliance with the nation's tax laws," IRS Commissioner Douglas Shulman said in a written statement.

U.S. law requires U.S. taxpayers to declare their global income and any foreign bank accounts with more than $10,000 during that tax year.

Mr. Shulman said the summons request "is focused on obtaining more information to help us determine if additional actions are needed."

Bryan Skarlatos, an attorney with Kostelanetz & Fink, LLP, said Thursday's move signaled that U.S. authorities, now in possession of additional data on offshore tax evasion, are broadening their efforts.

"They are going to follow up with these other banks and other countries because it's low-hanging fruit," he said. "The IRS knows the money is there."

Mr. Skarlatos said India has some form of banking secrecy, but nothing as strict as the Swiss system. He said that, hours after the Justice Department announcement, he already was receiving calls from concerned HSBC customers with undeclared Indian accounts.

According to the U.S. government, HSBC opened a New York office in 2002 and a Silicon Valley office in 2007 to solicit and maintain accounts based in India but closed them in June 2010. HSBC's Ms. Gutierrez said the decision to close the offices was made "in the ordinary course of business" due to "cost efficiencies and a realignment of that business model."

The request for a "John Doe" summons follows the January indictment of a New Jersey businessman, Vaibhav Dahake, on charges that he conspired to evade U.S. taxes by hiding offshore bank accounts in India maintained by HSBC.

In that case, prosecutors alleged HSBC employees took several steps to help Mr. Dahake "stay below the radar," including advising him to transfer and withdraw funds in smaller increments to avoid detection.

Mr. Dahake's lawyer declined to comment.

According to an electronic court docket, Mr. Dahake is scheduled to appear for a plea-agreement hearing on Monday.

In its court filings, the government said the Dahake case "is not an isolated incident."

More

Documents: Memo in Support of Summons | IRS Declaration

According to court documents, HSBC informed the IRS last September that at least 9,000 U.S. "premier" clients—high-net-worth customers—had deposits with HSBC's Indian bank. The government said 2009 bank figures showed that U.S. resident premier clients had Indian deposits of nearly $400 million.

U.S. officials said that as of 2009, U.S. taxpayers had only disclosed 1,921 HSBC accounts in India. The IRS is seeking client information on premier accounts as well as standard accounts maintained for less-wealthy customers.

The government's long-running probe against secret bank accounts led Swiss banking giant UBS AG to admit in February 2009 to conspiring to defraud the U.S. government of billions in taxes by helping wealthy Americans hide assets. The bank paid $780 million in a deal to avoid prosecution and eventually released the names of more than 4,000 U.S. clients.

Earlier this year, the U.S. charged four former Credit Suisse AG bankers with helping wealthy U.S. citizens evade taxes. Credit Suisse itself wasn't named in the indictment.

In February, the IRS announced a new leniency program that offers reduced penalties to tax scofflaws that voluntarily report their offshore accounts. The agency offered a similar one in 2009 in the wake of the U.S. case against UBS that brought in more than 15,000 disclosures.

Write to Evan Perez at evan.perez@wsj.com and Brent Kendall at brent.kendall@dowjones.com

FACTIVA DOW JONES

THE WALL STREET JOURNAL.
U.S. EDITION

U.S. Banks Steer Clear Of Sensitive Customers

By Robin Sidel and Andrew R. Johnson

1043 words
29 January 2014
The Wall Street Journal
J
A1
English

Under fire from several regulators, U.S. banks increasingly are rejecting customers involved in activities that are legal but might attract government scrutiny, according to executives, consultants and lawyers.

The banks are sacrificing revenue from a broad array of customers, from marijuana merchants and payday lenders to virtual-currency companies, online gamblers and people who have been convicted of a crime, in order to play it safe.

"In an era where banks are already suffering from a deficit of trust, the last thing they want to do is venture into things that can be perceived as risky, unsavory or detrimental to the social fabric," said Andy Schmidt, research director at consulting company CEB TowerGroup in Arlington, Va.

The decision to pull back comes at a time when banks are struggling with tepid loan demand, low interest rates and a thicket of new regulations.

While the temptation to deal with certain businesses might be high, some banking-industry veterans said, it isn't worth provoking regulators or adding more resources to ensure that the clients are meeting industry standards. And in the overall banking industry, such pullbacks aren't likely to hurt profits.

"Banks are making practical decisions about profitability versus risk exposure, and they are concluding this hill isn't worth the battle," said Gerard Comizio, a partner who specializes in banking at law firm Paul Hastings LLP.

J.P. Morgan Chase & Co. has jettisoned more than 2,000 customers since the New York bank last year decided to reduce its exposure to businesses that could add to its long list of regulatory problems, according to a person familiar with the bank's operations.

Among other things, the bank has said it won't lend to check-cashing companies and won't process transactions or clear certain types of payments for some 500 foreign banks.

J.P. Morgan also is cutting ties with a number of individual customers, from spouses of foreign leaders to people who have been indicted or convicted of a crime, said another person familiar with the lender's policies. The bank dumped twice as many of these customers in 2013 as it did in 2012, the person said.

The bank is ending the relationships even if there isn't any indication that the customer has done anything wrong, the person said. Instead, the bank doesn't want to spend the extra time and effort tracking activities of people who may be difficult to follow.

A spokesman for J.P. Morgan declined to comment on the number of clients with whom it has cut ties. The bank has paid more than $20 billion to regulators in the past year to avoid lawsuits and resolve compliance lapses, and has redeployed hundreds of employees to help resolve the issues.

The lack of banking services has been a big headache for Denver businessman Kayvan Khalatbari, co-owner of a medical marijuana dispensary and two pizza restaurants. He said he spent months last year wrestling with BBVA Compass after the regional, Texas-based bank dumped his accounts, including those associated with the pizza restaurants, an investment account and his personal account. BBVA Compass is a unit of Spanish lender Banco Bilbao Vizcaya Argentaria SA.

"It was a tumultuous time for us," said Mr. Khalatbari, who said he was forced to pay vendors in cash for a while. He has since found other banks willing to take his business, including one that is aware of his medical marijuana operation, which now has an account under a nondescript name. He declined to identify that institution.

"BBVA Compass does not bank businesses engaged in activities related to the cultivating, selling or distribution of marijuana," said a BBVA spokesman, who declined to comment on Mr. Khalatbari's accounts, citing privacy laws.

Some relief may be on horizon for legal marijuana businesses. Last week, U.S. Attorney General Eric Holder said during a discussion at the University of Virginia that the administration would soon announce regulations to address the issue. "You don't want just huge amounts of cash in these places," Mr. Holder said. "They want to be able to use the banking system."

The banks have refused to provide traditional deposit accounts to merchants operating marijuana businesses in Colorado, where recreational use of the drug became legal this year, and in states where medical marijuana is legal. The banks have said they are following federal law, which deems marijuana illegal.

Meanwhile, bankers said they are backing away from some types of businesses because they don't have sufficient controls to ensure their clients' customers are following the law. That is especially the case when it comes to money laundering, an area that is attracting interest from regulators and law enforcement.

Banks also are finding it particularly troublesome to do business with check-cashing firms and payday lenders. Such companies are under scrutiny from regulators and lawmakers for charging high fees and providing murky disclosures to customers, even if they are operating legally.

Bank of America Corp. said last year that it is exiting its relationships with payday lenders and isn't pursuing any new business in the industry.

New York and other states have targeted payday lenders whose loans allegedly violate state laws capping interest rates. Last week, online lender Western Sky Financial LLC and two affiliated firms agreed to pay $1.5 million and refund some interest payments to borrowers under an agreement with New York Attorney General Eric Schneiderman, who had sued the companies for charging annual rates as high as 355%. Western Sky neither admitted nor denied the allegations.

Bank of America, Wells Fargo & Co. and other big banks won't allow credit-card customers to use their plastic for online gambling in Delaware, Nevada and New Jersey, where such activity is legal.

Banks also are keeping away from doing business with companies involved with bitcoin, the virtual currency that has had connections with illegal activities even as it is becoming more accepted among mainstream merchants and consumers. On Sunday, federal prosecutors arrested a prominent bitcoin entrepreneur and charged him with money laundering. He hasn't entered a plea.

Grant Thornton

Reporting Entity Sector Profiles: Lawyers Appendices

Prepared for FINTRAC | March 31, 2014

Appendix A: Industry statistics and reporting entity data

Lawyers sector SIC codes

Code	Description
8111	Legal Services

Lawyers industry NAICS codes

Code	Description
5411	Legal Services
54111	Offices of Lawyers
54112	Offices of Notaries (NAICS 54112)
54119	Other Legal Services

Using NAICs codes, searches for statistical data on the Lawyers sector were carried out on Industry Canada's Canadian Industry Statistics (CIS) site.

Offices of Lawyers (NAICS 54111)

Exclusions

- offices of notaries (54112, Offices of Notaries); and
- offices of legal and paralegal practitioners, except offices of lawyers and notaries (54119, Other Legal Services).

Number of establishments in Canada by type and region: December 2012
Offices of Lawyers (NAICS 54111)

Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	2,394	1,476	3,870	14.3%
British Columbia	2,898	2,228	5,126	19.0%
Manitoba	432	381	813	3.0%
New Brunswick	332	170	502	1.9%
Newfoundland and Labrador	135	112	247	0.9%
Northwest Territories	16	14	30	0.1%
Nova Scotia	370	295	665	2.5%
Nunavut	3	4	7	0.0%
Ontario	5,761	4,891	10,652	39.5%
Prince Edward Island	62	34	96	0.4%
Quebec	1,700	2,526	4,226	15.7%
Saskatchewan	336	384	720	2.7%
Yukon Territory	23	20	43	0.2%
CANADA	14,462	12,535	26,997	100%
Percent Distribution	53.6%	46.4%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Offices of Lawyers (NAICS54111)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	1,924	462	8	0
British Columbia	2,240	651	7	0
Manitoba	332	99	1	0
New Brunswick	279	53	0	0
Newfoundland and Labrador	80	55	0	0
Northwest Territories	12	4	0	0
Nova Scotia	277	91	2	0
Nunavut	1	2	0	0
Ontario	4,194	1,541	21	5
Prince Edward Island	47	15	0	0
Quebec	1,358	331	10	1
Saskatchewan	242	93	1	0
Yukon Territory	16	6	1	0
CANADA	11,002	3,403	51	6
Percent Distribution	76.1%	23.5%	0.4%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Legal Services (NAICS 54111)

Number of establishments in Canada by type and region: December 2012 Legal Services (NAICS 5411)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	2,581	1,805	4,386	13.1%
British Columbia	3,301	2,765	6,066	18.2%
Manitoba	460	426	886	2.7%
New Brunswick	351	189	540	1.6%
Newfoundland and Labrador	165	129	294	0.9%
Northwest Territories	17	17	34	0.1%
Nova Scotia	398	342	740	2.2%
Nunavut	3	8	11	0.0%
Ontario	6,504	6,276	12,780	38.3%
Prince Edward Island	67	48	115	0.3%
Quebec	2,945	3,749	6,694	20.1%
Saskatchewan	364	416	780	2.3%
Yukon Territory	25	22	47	0.1%
CANADA	17,181	16,192	33,373	100%
Percent Distribution	51.5%	48.5%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Legal Services (NAICS5411)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	2,074	499	8	0
British Columbia	2,549	744	8	0
Manitoba	352	107	1	0
New Brunswick	298	53	0	0
Newfoundland and Labrador	105	59	1	0
Northwest Territories	13	4	0	0
Nova Scotia	299	97	2	0
Nunavut	1	2	0	0
Ontario	4,783	1,692	24	5
Prince Edward Island	52	15	0	0
Quebec	2,321	613	10	1
Saskatchewan	265	97	2	0
Yukon Territory	18	6	1	0
CANADA	13,130	3,988	57	6
Percent Distribution	76.4%	23.2%	0.3%	0.0%

Offices of Notaries (NAICS 54112)

Exclusions

- offices of legal and paralegal practitioners, except offices of lawyers and notaries (54119, Other Legal Services); and
- offices of notaries public engaged in activities, such as administering oaths and taking affidavists and depositions, and witnessing and certifying signatures on documents, but not empowered to draw up and approve legal documents and contracts (54119, Other Legal Services).

Number of establishments in Canada by type and region: December 2012 Offices of Notaries (NAICS 54112)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	3	9	12	0.6%
British Columbia	127	59	186	9.3%
Manitoba	1	1	2	0.1%
New Brunswick	1	0	1	0.0%
Newfoundland and Labrador	1	0	1	0.0%
Northwest Territories	0	0	0	0.0%
Nova Scotia	0	0	0	0.0%
Nunavut	0	0	0	0.0%
Ontario	3	8	11	0.5%
Prince Edward Island	0	0	0	0.0%
Quebec	1,071	723	1,794	89.3%
Saskatchewan	0	0	0	0.0%
Yukon Territory	0	1	1	0.0%
CANADA	1,207	801	2,008	100%
Percent Distribution	60.1%	39.9%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Offices of Notaries (NAICS54112)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	3	0	0	0
British Columbia	90	37	0	0
Manitoba	1	0	0	0
New Brunswick	1	0	0	0
Newfoundland and Labrador	1	0	0	0
Northwest Territories	0	0	0	0
Nova Scotia	0	0	0	0
Nunavut	0	0	0	0
Ontario	2	1	0	0
Prince Edward Island	0	0	0	0
Quebec	837	234	0	0
Saskatchewan	0	0	0	0
Yukon Territory	0	0	0	0
CANADA	935	272	0	0
Percent Distribution	77.5%	22.5%	0.0%	0.0%

Exclusions

- offices of notaries (54112, Offices of Notaries); and
- offices of legal and paralegal practitioners, except offices of lawyers and notaries (54119, Other Legal Services).

Number of establishments in Canada by type and region: December 2012 Other Legal Services (NAICS 54119)				
Province or Territory	Employers	Non-Employers/ Indeterminate	Total	% of Canada
Alberta	184	320	504	11.5%
British Columbia	276	478	754	17.3%
Manitoba	27	44	71	1.6%
New Brunswick	18	19	37	0.8%
Newfoundland and Labrador	29	17	46	1.1%
Northwest Territories	1	3	4	0.1%
Nova Scotia	28	47	75	1.7%
Nunavut	0	4	4	0.1%
Ontario	740	1,377	2,117	48.5%
Prince Edward Island	5	14	19	0.4%
Quebec	174	500	674	15.4%
Saskatchewan	28	32	60	1.4%
Yukon Territory	2	1	3	0.1%
CANADA	1,512	2,856	4,368	100%
Percent Distribution	34.6%	65.4%	100%	

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

Number of employer establishments by employment size category and region: December 2012 Other Legal Services (NAICS54119)				
Province or Territory	Employment Size Category (Number of employees)			
	Micro 1-4	Small 5-99	Medium 100-499	Large 500+
Alberta	147	37	0	0
British Columbia	219	56	1	0
Manitoba	19	8	0	0
New Brunswick	18	0	0	0
Newfoundland and Labrador	24	4	1	0
Northwest Territories	1	0	0	0
Nova Scotia	22	6	0	0
Nunavut	0	0	0	0
Ontario	587	150	3	0
Prince Edward Island	5	0	0	0
Quebec	126	48	0	0
Saskatchewan	23	4	1	0
Yukon Territory	2	0	0	0
CANADA	1,193	313	6	0
Percent Distribution	78.9%	20.7%	0.4%	0.0%

Source : Statistics Canada, Canadian Business Patterns Database, December 2012.

NAICS Code 54111 –Office of Lawyers

Province	Number of Establishments
Alberta	1,425
British Columbia	2,266
Manitoba	371
New Brunswick	245
Newfoundland and Labrador	161
Northwest Territories	37
Nova Scotia	317
Nunavut	7
Ontario	4,958
Prince Edward Island	52
Quebec	1,729
Saskatchewan	396
Yukon	22
Total	11,986

Source: OneSource

NAICS Code 541191 – Title Abstract and Settlement Offices

State or Province	Number of Establishments
Alberta	10
British Columbia	32
Newfoundland and Labrador	1
Ontario	8
Quebec	1
Grand Total	52

Source: OneSource

NAICS Code 541199 – All Other Legal services

State Or Province	Number of Establishments
Alberta	140
British Columbia	319
Manitoba	37
New Brunswick	27
Newfoundland and Labrador	14
Northwest Territories	5
Nova Scotia	30
Ontario	1,098
Prince Edward Island	7
Quebec	1215
Saskatchewan	37
Yukon	2
Grand Total	2931

Source: OneSource

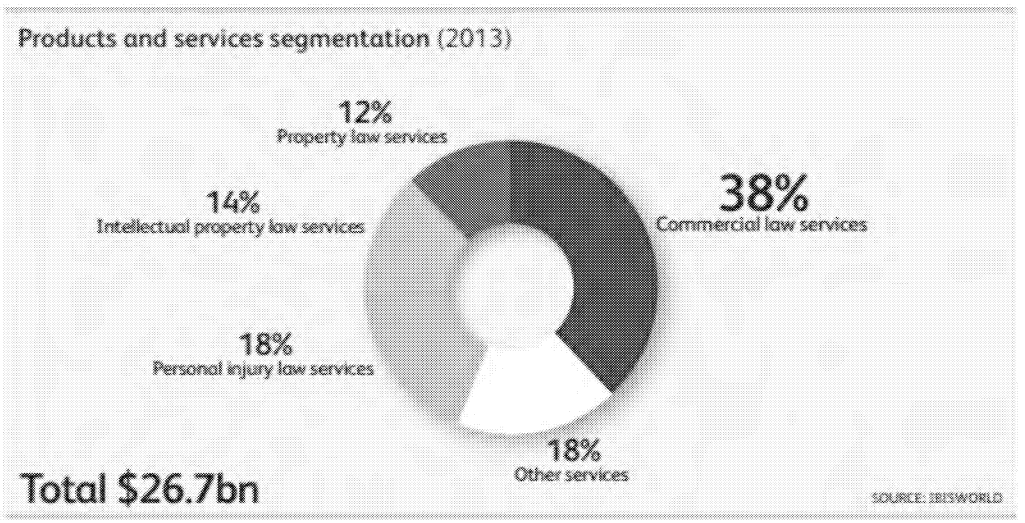
SIC Code 8111 – Legal Services

Ontario 4957

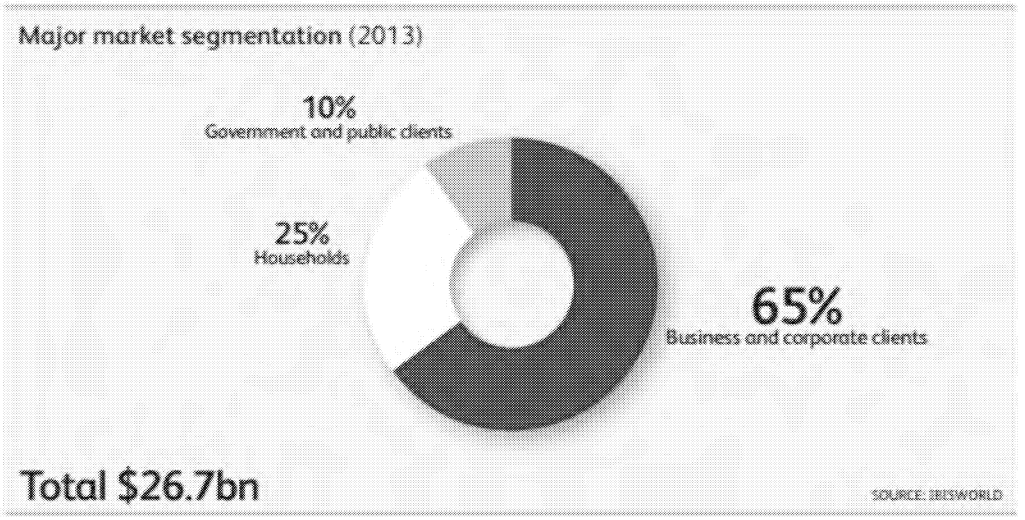
Province	Number of Establishments
Alberta	1,424
British Columbia	2,265
Manitoba	371
New Brunswick	245
Newfoundland and Labrador	161
Northwest Territories	37
Nova Scotia	316
Nunavut	7
Ontario	4,957
Prince Edward Island	52
Quebec	1,728
Saskatchewan	395
Yukon	22
Total	11,980

Source: OneSource

Products and Services Segmentation



Major Market Segmentation



Source: IBISWORLD

Canada's Largest Law Firms – 2014

Source: Lexpert

TORONTO: THE 20 LARGEST LAW FIRMS

	FIRM NAME	Toronto	All Offices		FIRM NAME	Toronto	All Offices
1	Borden Ladner Gervais LLP	273	769	11	Goodmans LLP	188	204
2	Blake, Cassels & Graydon LLP	270	534	12	Heenan Blaikie LLP	175	506
3	Osler, Hoskin & Harcourt LLP	258	380	13	McMillan LLP	155	313
4	McCarthy Tétrault LLP	238	544	14	Miller Thomson LLP	151	464
5	Torys LLP	228	255	15	Davies Ward Phillips & Vineberg LLP	146	231
6	Fasken Martineau DuMoulin LLP	221	631	16	Bennett Jones LLP	143	352
7	Gowling Lafleur Henderson LLP	220	715	17	Aird & Berlis LLP	140	140
8	Cassels Brock & Blackwell LLP	202	216	18	Blaney McMurtry LLP	129	129
9	Stikeman Elliott LLP	199	445	19	Dentons Canada LLP	126	473
10	Norton Rose Fulbright Canada LLP	190	604	20	Fogler, Rubinoff LLP	106	109

OTTAWA: THE 10 LARGEST LAW FIRMS

	FIRM NAME	Ottawa	All Offices		FIRM NAME	Ottawa	All Offices
1	Gowling Lafleur Henderson LLP	170	715	6	Kelly Santini LLP	32	32
2	Borden Ladner Gervais LLP	97	769	7	Heenan Blaikie LLP	30	506
3	Nelligan O'Brien Payne LLP	65	65	7	Smart & Biggar/Fetherstonhaugh	30	79
4	Perley-Robertson, Hill & McDougall LLP/s.r.l.	48	48	9	Emond Harnden LLP	27	27
5	Norton Rose Fulbright Canada LLP	37	604	9	Soloway, Wright LLP	27	27

MONTRÉAL: THE 13 LARGEST LAW FIRMS

	FIRM NAME	Montréal	All Offices		FIRM NAME	Montréal	All Offices
1	Norton Rose Fulbright Canada LLP	177	604	8	BCF LLP	95	120
2	Fasken Martineau DuMoulin LLP	170	631	9	Dentons Canada LLP	91	473
3	Heenan Blaikie LLP	158	506	10	Gowling Lafleur Henderson LLP	90	715
4	Stikeman Elliott LLP	155	445	11	Davies Ward Phillips & Vineberg LLP	85	231
5	McCarthy Tétrault LLP	142	544	12	Robinson Sheppard Shapiro L.L.P.	75	75
6	Lavery, de Billy, L.L.P.	139	162	13	Blake, Cassels & Graydon LLP	65	534
7	Borden Ladner Gervais LLP	124	769				

VANCOUVER: THE 12 LARGEST LAW FIRMS

	FIRM NAME	Vancouver	All Offices		FIRM NAME	Vancouver	All Offices
1	Fasken Martineau DuMoulin LLP	146	631	7	McMillan LLP	85	313
2	Borden Ladner Gervais LLP	136	769	8	McCarthy Tétrault LLP	83	544
3	Lawson Lundell LLP	99	116	9	Farris, Vaughan, Wills & Murphy LLP	77	90
4	Davis LLP	98	246	10	Clark Wilson LLP	76	76
4	Bull, Housser & Tupper LLP	98	98	11	Alexander Holburn Beaudin + Lang LLP	74	74
6	Blake, Cassels & Graydon LLP	91	534	12	Miller Thomson LLP	64	464

CALGARY AND EDMONTON: THE 16 LARGEST LAW FIRMS

	FIRM NAME	Calgary	Edmonton	All Offices		FIRM NAME	Calgary	Edmonton	All Offices
1	Bennett Jones LLP	171	36	352	9	Parlee McLaws LLP	34	52	86
2	Dentons Canada LLP	95	81	473	10	Miller Thomson LLP	33	52	464
3	Norton Rose Fulbright Canada LLP	151	—	604	11	McLennan Ross LLP	25	54	83
4	Burnet, Duckworth & Palmer LLP	142	—	142	12	Davis LLP	50	25	246
5	Borden Ladner Gervais LLP	129	—	769	13	McCarthy Tétrault LLP	56	—	544
6	Field Law	52	62	118	14	Witten LLP	—	54	54
7	Blake, Cassels & Graydon LLP	105	—	534	15	Brownlee LLP	12	45	57
8	Gowling Lafleur Henderson LLP	102	—	715	16	Osler, Hoskin & Harcourt LLP	52	—	380

WINNIPEG: THE 5 LARGEST LAW FIRMS

	FIRM NAME	Winnipeg	All Offices		FIRM NAME	Winnipeg	All Offices
1	Aikins, MacAulay & Thorvaldson LLP	97	97	4	Fillmore Riley LLP	60	60
2	Thompson Dorfman Sweatman LLP	73	77	4	Pitblado LLP	60	60
3	Taylor McCaffrey LLP	63	63				

ATLANTIC CANADA: THE 5 LARGEST LAW FIRMS

	FIRM NAME	Nova Scotia Total	New Brunswick Total	Prince Edward Island Total	Newfoundland & Labrador Total	All Offices
1	Stewart McKelvey	100	62	28	33	223
2	McInnes Cooper	109	50	18	27	204
3	Cox & Palmer	59	77	22	42	200
4	BOYNECLARKE LLP	51	—	—	—	51
5	Patterson Law	29	—	—	—	29

Appendix B: Case examples and typologies

The enclosed articles have been sourced from: news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Ex-Revenue Canada lawyer advised how to hide money offshore. CBC News, October 2, 2013.
2. Law Society '80%' sure missing lawyer died weeks after millions disappeared from trust. National Post, December 17, 2013.
3. Toronto lawyer facing fraud charges stripped of his licence. The Globe and Mail, November 16, 2012.
4. Trust account scam hits home – A true story. Advisor, Fourth Quarter 2009.
5. Money laundering conviction leads to lawyer's resignation. California Bar Journal, December 2001.
6. Nova Scotia lawyer admits embezzling 'friendly-fire' funds. The Globe and Mail, September 26, 2006.
7. Mortgage scam probed in Toronto house flips; Seven homes in the Junction were taken on a wild real estate tide that ended in a lawyer's suspension. Toronto Star, January 7, 2012.
8. Lawyer loses law license. The Kingston Whig-Standard, March 7, 2014.
9. Regina lawyer suspended. The StarPhoenix, December 18, 2013.
10. Disappearance of lawyer, and $3.6M, devastates clients. Mississauga News, November 29, 2013.
11. Lawyer who fled to France loses licence. The Ottawa Sun, October 29, 2013.
12. Toronto real estate lawyer charged with money laundering. The Globe and Mail, June 8, 2012.
13. Authorities to probe another disbarred lawyer. Kaieteur News, February 23, 2014.
14. U.S. and Canadian citizens charged with using offshore accounts and foreign nominee entities to launder $200,000. Department of Justice, March 24, 2012.

Exclusive

Ex-Revenue Canada lawyer advised how to hide money offshore

By Timothy Sawa, CBC News Posted: Oct 02, 2013 5:00 AM ET Last Updated: Oct 02, 2013 1:22 PM ET

An exclusive CBC News hidden camera investigation into the world of offshore banking uncovered a former executive with the Royal Bank of Canada and a former lawyer with the Canada Revenue Agency offering advice on how to hide money from Canadian tax authorities.

As part of the joint investigation with *Enquête*, the CBC'S French-language investigative program, CBC News hired a private investigator, who is also a restaurant and bar owner in Toronto, to test 15 different offshore service providers in Canada and abroad.

The investigator was given a story: over the years he had squirrelled away as much as a million dollars that he hadn't declared, and wanted to hide it offshore to avoid paying taxes.

More than half of the offshore service providers tested with hidden cameras by the CBC in Canada and Barbados provided advice that wouldn't stand up to scrutiny, according to CBC experts.

Among those tested during the CBC investigation was Gilles Gosselin, who practised law in Canada and used to work for the Canadian Revenue Agency before moving to Barbados.

His company's website says it specializes in helping Canadian companies with international business structure their company in Barbados — a perfectly legal activity.

The businessman travelled to Barbados to meet with Gosselin.

Gosselin told the businessman he wanted nothing to do with his plan. But when he was asked if there's anything preventing someone from opening an account at a bank somewhere and wiring the funds there, Gosselin was recorded on hidden cameras saying: "I just told you how the law works. And if you don't report the income in Canada, that's your business."

He later told the undercover businessman not to use Barbados because it's too expensive, there are too many reporting requirements and the stamp they put on his passport when he made this trip could get him caught.

Gosselin said if the businessman was audited, they would ask him why he was in the Barbados.

He also advised that if the businessman said he was there for vacation, "now you're in a position where you're

lying right," Gosselin said.

Recommended British Virgin Islands

Gosselin recommended the businessman use the British Virgin Islands to hide his million dollars and to avoid Canadian-owned banks offshore.

"You might not want to have a bank with a Canadian connection. There's other banks — Bank of Butterfield, which is a U.K. bank. So yeah I mean, it could be done," Gosselin said.

CBC policy for hidden-camera journalism

CBC's policy for hidden-camera journalism generally requires that we have credible information about wrongdoing before we film.

However when dealing with a secretive industry like this one, when the industry as a whole has come under critical scrutiny, the practice is to permit testing in this way, on a random basis.

He sent an email introducing the businessman to the British Virgin Island service provider. He explained the businessman needed an account there and that it should be "preferably with a non-Canadian bank."

But two hours later Gosselin sent a second email reminding the undercover businessman that he should follow all Canadian laws and report all Canadian income.

Andre Lareau, a professor at Laval University in Quebec, who teaches tax law, said that Gosselin, with his background at the Canada Revenue Agency, knows all the mechanisms for people who want to commit tax fraud. He said the plan involving the British Virgin Islands would be tax evasion.

Lareau added that the second email Gosselin sent is the right one and it's the information that he should have been giving from the beginning.

"It's kind of depressing that someone would go over, as we say, to the dark side so completely," said Jack Blum, an expert on white-collar financial crime in Washington.

Asked by CBC News why he helped the undercover businessman with his plan, Gosselin said that he told the man what he was contemplating was against the law in Canada.

"But if he wants to go ahead and open a BVI company and manage his assets with the BVI company, until he's actually gone there and done that, he hasn't done anything wrong," he said.

"This person told me that he was coming here, that he had a million dollars in a safety deposit box and he was looking to invest it outside of Canada, and that he wasn't — and I told him specifically that that was against the law. And my last communication with him says specifically that."

Gosselin later explained that his clients are usually legitimate Canadian-based businesses looking to take advantage of the legal tax benefits in Barbados.

He added that that he "probably entertained" the undercover businessman "more than I should have."

Banking executive among those tested

During the course of the CBC investigation, Lynn Garner, a vice-president with DGM, a private Barbados bank, was also among those tested.

Garner worked as an executive at several money management firms and banks and as the trust manager for the Royal Bank of Canada in Barbados.

At first, Garner was adamant that her bank would never get involved with someone like CBC's undercover businessman.

"We don't take clients who aren't reporting," she was recorded on hidden cameras saying. "So we don't — you know, our book is clean."

But then she went on to tell the undercover businessman how he could hide cash offshore, by setting up an anonymous paper company, moving the cash offshore and opening an account at her bank to hold the cash.

"You wire money from your account to an account at CIBC. Through CIBC head office, so it goes through your bank to CIBC Toronto, CIBC Toronto to CIBC Cayman. And then Cayman holds it on our behalf. So that's how it works," she said.

And she offered advice for avoiding detection by authorities when depositing the money.

"Depositing the money into the bank account in Canada, you'd have to do a little bit. It would take a long time."

She said if the cash is coming from Canada, he won't have to worry about a lot scrutiny from her about where he got it.

"If it's coming from a Canadian financial institution … we have to understand how you earned the money but we won't ask for proof as much except for a statement from the bank."

Garner then found someone in Barbados within a couple weeks who she said could help the undercover businessman create the offshore company to hold the cash at her bank.

But Lareau said Garner's plan constituted fraud and that it was sad to see people in the financial sector accommodating someone in this way.

"This is not a tape the bank would ever want to be made public. The fact that she's willing to take money she knows is tainted," said one insider, who used to run one of Canada's largest offshore banking companies.

In a statement, DGM said that it "is not engaged in any business practices that are not legal by the law of Barbados or of the laws of Canada. Any assertion to the contrary by the CBC will be aggressively rebutted both publicly and by legal means."

If you have tips on offshore havens, or other investigative stories, please email investigations@cbc.ca

Law Society '80%' sure missing lawyer died weeks after millions disappeared from trust

DREW HASSELBACK | December 17, 2013 | Last Updated: Dec 18 9:49 AM ET
More from Drew Hasselback

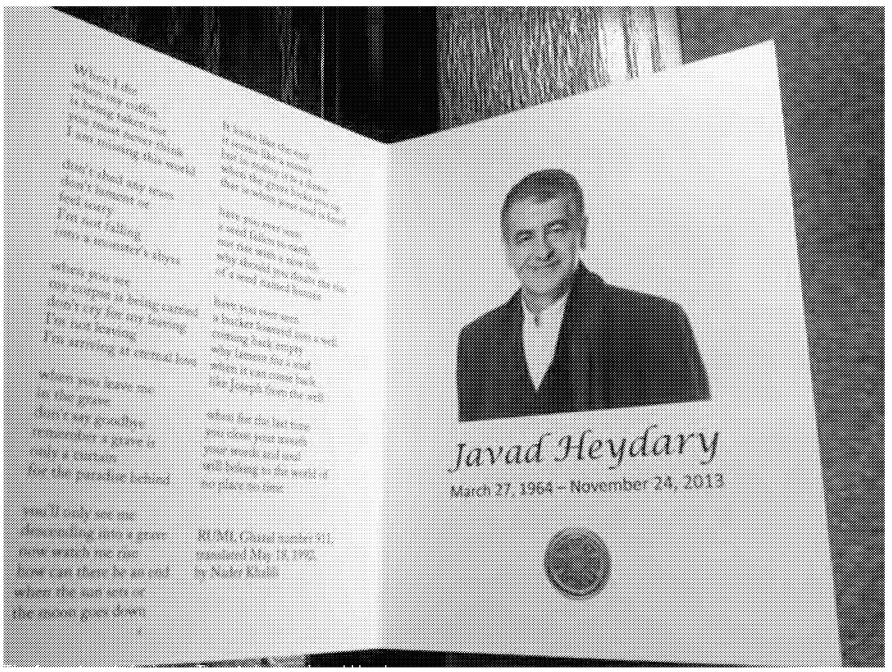


Photo: Drew Hasselback / National Post

The hunt for missing Toronto lawyer Javad Heydary and millions of dollars in missing trust account funds took a bizarre twist on Tuesday when counsel for the Law Society of Upper Canada told a Toronto courtroom it is now "80%" sure the lawyer died overseas on Nov. 24.

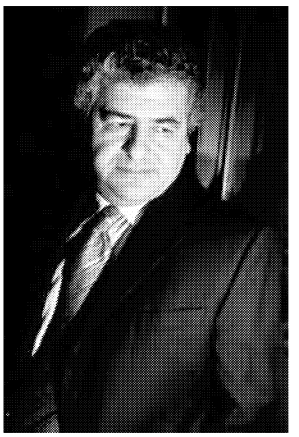
The Law Society is now seeking to confirm the paper work prepared just before a hasty funeral on Monday. The key document under review is apparently a statutory declaration by a former colleague of the lawyer who viewed the body and identified the deceased as Heydary.

It didn't feel like a funeral

If confirmed, the funeral marks an unusual end to the hunt for the whereabouts of the high-profile litigator. Witnesses say Heydary was buried in Richmond Hill, Ont., following a brief funeral service on Monday. The casket was sealed, though witnesses say it was briefly unlocked so some members of the family could view the body just before the conclusion of the service.

"It didn't feel like a funeral," one witness said after the court hearing. There didn't seem to be a lot of mourning, and children were laughing and playing during the visitation, the witness said.

But the internment will not trigger an immediate end to the hunt for millions in missing trust funds. On the contrary, counsel for the Law Society clarified in court on Tuesday that the investigation will continue as before, even if Heydary is now deceased.


Glenn Lowson photo for National Post

The funeral came just one day before an Ontario judge was scheduled to sentence the lawyer for civil contempt because he failed to comply with a Nov. 14 court order that he immediately return at least $2.1-million in trust account funds to former clients Samira and Hasan Abuzour.

The Law Society, which is the body that regulates the legal profession in Ontario, seized control of Heydary's legal practice on Nov. 25 after it learned that his trust account contained only $319,000, or some $3-million less than it was supposed to.

Heydary, who fashioned himself as a lawyer for victims of white collar fraud, left Canada on Nov. 15, the day after the court order was issued. He told staff at his Toronto law firm, Heydary Hamilton PC, that he needed to visit Dubai on business. While overseas, he told staff that he had suddenly been summoned to visit a sick uncle in Iran.

Staff remained in touch with him via email and phone until Nov. 18 or so. The last contact number he gave his staff was for a cell phone in Iran. The funeral card distributed on Monday states that Heydary died on Nov. 24, though it provides no cause of death. The funeral on Monday was organized shortly after the repatriation of the body.

Heydary has launched several high profile cases. He was representing investors in a lawsuit brought against developers of the Trump Hotel in Toronto. The plaintiffs claim they were induced to buy units in the project by "reckless and negligent misrepresentations" made by the defendants, among them Donald Trump himself. The lawsuit contains allegations that have yet to be proven in court.

Then there's the landmark summary judgment ruling Heydary obtained against Toronto businessman Robert Hryniak. That case has progressed all the way to the Supreme Court of Canada, which heard arguments last March but has yet to issue a written decision.

Heydary's undoing flows from another successful result. In April, the lawyer obtained a $3.6-million settlement for the Abuzours in a shareholders dispute. The couple spent months asking Heydary to release the funds from his trust account, and was ultimately forced to seek the court order that was issued Nov. 14. Heydary and his law firm were to give the Abuzours $2.1-million immediately, and provide proof the remaining $1.5-million was safely in the bank. Shortly after that, the Law Society seized control Heydary's legal practice and began looking for the missing trust funds.

Late last month, Justice Julie Thorburn of the Ontario Superior Court ruled that both Heydary and his firm, Heydary Hamilton PC, are in contempt of court for failing to comply with her Nov. 14 order. The matter was back in court on Tuesday for a sentencing hearing. However, the matter was adjourned after counsel for the Law Society said the regulator still needs to confirm that Heydary has died.

"I can say with about an 80-degree certainty that Mr. Heydary has passed," Margaret Cowtan, counsel for the Law Society, told court. But she said the regulator wants more proof before it is "100%" certain he is dead. In particular, she said the Law Society wants to review a statutory declaration made by an "independent third party" — namely a lawyer who once worked with Heydary who viewed and identified the body.

Judge Thorburn said she wants Law Society counsel to return to court on Jan. 20 with a detailed report about the status of the hunt for the missing money.

Speaking in court, Mr. Abuzour expressed his frustration over the loss of the money and the resulting adjournment. "I respect what you say. But what can I do? I don't have anything," he told the judge.

Judge Thorburn told Mr. Abuzour she understands his frustration. "The $3.6-million went somewhere," she said. If there's any consolation, she explained, it's that it's for the Law Society, and not him, to foot the bill for the investigation into where that money went. What's more, she added, the Law Society has rights to examine trust account records that outside investigators wouldn't be able to see due to solicitor-client privilege. "We're shocked that this happened," the judge said.

The Abuzours had hoped they could gain immediate access to some of the funds in the law firm's trust account. Judge Thorburn said she is not legally able to order that right now.

As of Nov. 25, only $319,000 was in the firm's mixed trust account, some $3-million less than was supposed to be there. Judge Thorburn explained in court that no funds can be released from that account until the Law Society figures out if any of that money is owed to other Heydary Hamilton PC clients or creditors.

THE GLOBE AND MAIL

LAW SOCIETY

Toronto lawyer facing fraud charges stripped of his licence

TIMOTHY APPLEBY
The Globe and Mail
Published Friday, Nov. 16 2012, 6:27 PM EST
Last updated Friday, Nov. 16 2012, 6:27 PM EST

A Toronto lawyer facing fraud and theft charges has been stripped of his licence after the Law Society of Upper Canada concluded he misappropriated more than $3-million of his clients' money, most of it belonging to a charitable foundation with long-standing links to the Toronto Rotary Club.

Over 2 1/2 years, the society said, Michael Ingram siphoned cash from trust funds he controlled and dispersed it to eight recipients, including his wife and his brother.

In all, there were more than 130 allegedly unauthorized transfers.

"The conduct in this case is egregious," said the LSUC, the body that oversees the province's lawyers.

"Over $3-million in trust funds were misapplied and over $2-million remains unpaid. ... The fact that over $2-million was taken from a charitable foundation is of particular concern."

Police say the cash was funnelled to the United States, Canada, Bermuda and Switzerland, possibly beyond, and where the money trail ends remains guesswork.

One of the clients was a charity. Although the law society does not name it in the ruling, it was the defunct Laughlen Centre, a long-term-care facility for seniors that the City of Toronto bought in 2006 for $8-million.

Mr. Ingram, 69, was charged in July of this year with theft over $5,000 and fraud over $5,000 and has a court appearance set for next month.

He has declined comment, and a message left on Friday with the lawyer who represented him at the LSUC disciplinary hearing, Nadia Liva, was not immediately returned.

The society found it "troubling" that Mr. Ingram did not attend the hearing.

Of the $8-million the city paid for the centre, about one-third was to have gone to the centre, which, until it ceased operations in 2004, was home to more than 200 residents.

The balance covered outstanding debts and mortgages.

Mr. Ingram, a former partner with the downtown law firm Coutts Crane Ingram, had been the charity's lawyer and had headed its board of directors.

In 2008, he was fired by Coutts Crane, to which he had belonged for 38 years, after the discrepancies came to light.

Coutts Crane also reported him to the law society, and in July of that year, Mr. Ingram agreed to cease practising law.

On learning its share of the funds was missing, the Laughlen Centre's board members in August, 2010, launched a lawsuit against Mr. Ingram, four of his former colleagues at Coutts Crane and three associates, seeking more than $2.5-million in lost funds, plus $1-million in punitive damages.

The suit accused the law firm of failing to supervise Mr. Ingram adequately and thereby being "vicariously liable" for the alleged theft.

The defendants denied that.

"CCI had reasonable safeguards in place to protect the funds in its trust account, which Ingram unilaterally and surreptitiously circumvented," their statement of defence read.

The defendants agreed to settle the suit for $1.5-million.

And because the Laughlen Centre had by then ceased to exist except as a legal entity, the money was paid via a liquidation firm to the Rotary Club, a greatly respected secular organization that had for years helped administer the centre and provide financial support.

For the same reason, the Rotary Club is named in the criminal investigation as the chief victim of Mr. Ingram's alleged theft, along with at least two smaller, unspecified charities.

The law society found that during the period spanning October, 2005, to May, 2008, Mr. Ingram shuffled the money between different trust accounts, and disbursed it to a range of beneficiaries, including overseas law firms, and at least one religious organization, The Glorious Praise Ministries.

As well, his brother received more than $100,000 to assist in a real estate venture, the law society wrote.

Fourth Quarter 2009

Advisor

An update on issues regarding liability protection for the legal profession.

Florida LAWYERS Mutual Insurance Company®

Trust Account Scam Hits Home
A True Story

By K. Judith Lane

K. Judith Lane
Lane & Ertl, P.A.
Daytona Beach
jlane@laneandertl.com
www.laneandertl.com

I had read from various sources, including The Florida Bar, that scam artists were actively trying to use lawyer trust accounts as a conduit to fraud and theft schemes, but to my knowledge, it was not something that local attorneys were dealing with. I just met with the FBI and to its knowledge, while the scam is being used on local businesses and individuals a great deal, ours was the first law firm hit with it. Here is what happened:

The story begins:

I was engaged via email and follow-up written correspondence by Microtel, Inc., a manufacturer in Grand Rapids, Michigan, to collect on a $325,000 debt alleged to be owed to Microtel by a local company Intellitec, Inc. I was hired to make a collection demand and, if needed, litigation. Importantly: I received a signed engagement letter and a request from Microtel to schedule a conference call to discuss the details of the dispute. At that point, nothing was out of the ordinary.

A few days later:

While we were trying to set up a phone conference with Microtel's president, Microtel sent me an email indicating its representatives had spoken with Intellitec and we should be receiving payment. Within days, I had an official check from Wachovia sitting on my desk for a little over $325,000, delivered by overnight delivery, payable directly to my firm's trust account.

Still, nothing totally out of the ordinary, but I was growing a bit suspicious as the Intellitec letter did not say very much and the folks at Microtel were not making it easy for my office to set up a phone conference with my new client to discuss the facts of the case or how to proceed.

I did not want to deposit the check into my trust account until I was certain Microtel was prepared to accept it as payment in full, so I emailed Microtel and called the company asking again to speak to the president. It was the Wednesday before Thanksgiving, so the banks were closed and I put the check in my safe.

Continued on page 2

Some risk management information on www.flmic.com is restricted to the policyholders of Florida Lawyers Mutual.
Contact FLMIC for the user name and password.

mailbox@flmic.com • www.flmic.com
800-633-6458

The following Monday morning, my paralegal got a call from Microtel's president asking what the heck was going on and who we were. He had just gotten all the emails from our office. He said he never contacted us for representation and, while he had done business with Intellitec a few years before, they did not owe him any money.

By chance, he happened to be looking at an old email account that he rarely used anymore and saw the communications between my firm and someone holding themselves out to be him and acting on behalf of his company. At that point, the scam was up. He went to the Grand Rapids FBI; I went to the Daytona Beach FBI.

The story ends:

The scam artists in this case were brazen enough to: 1) hack into an old email account belonging to the president of a successful Michigan business, 2) actually use his email account to conduct business with my firm and engage our services, 3) forge an engagement letter as president of Microtel with my law firm, 4) forge letterhead from Intellitec, a local business operating as a going concern, and 5) forge an official check from a bank.

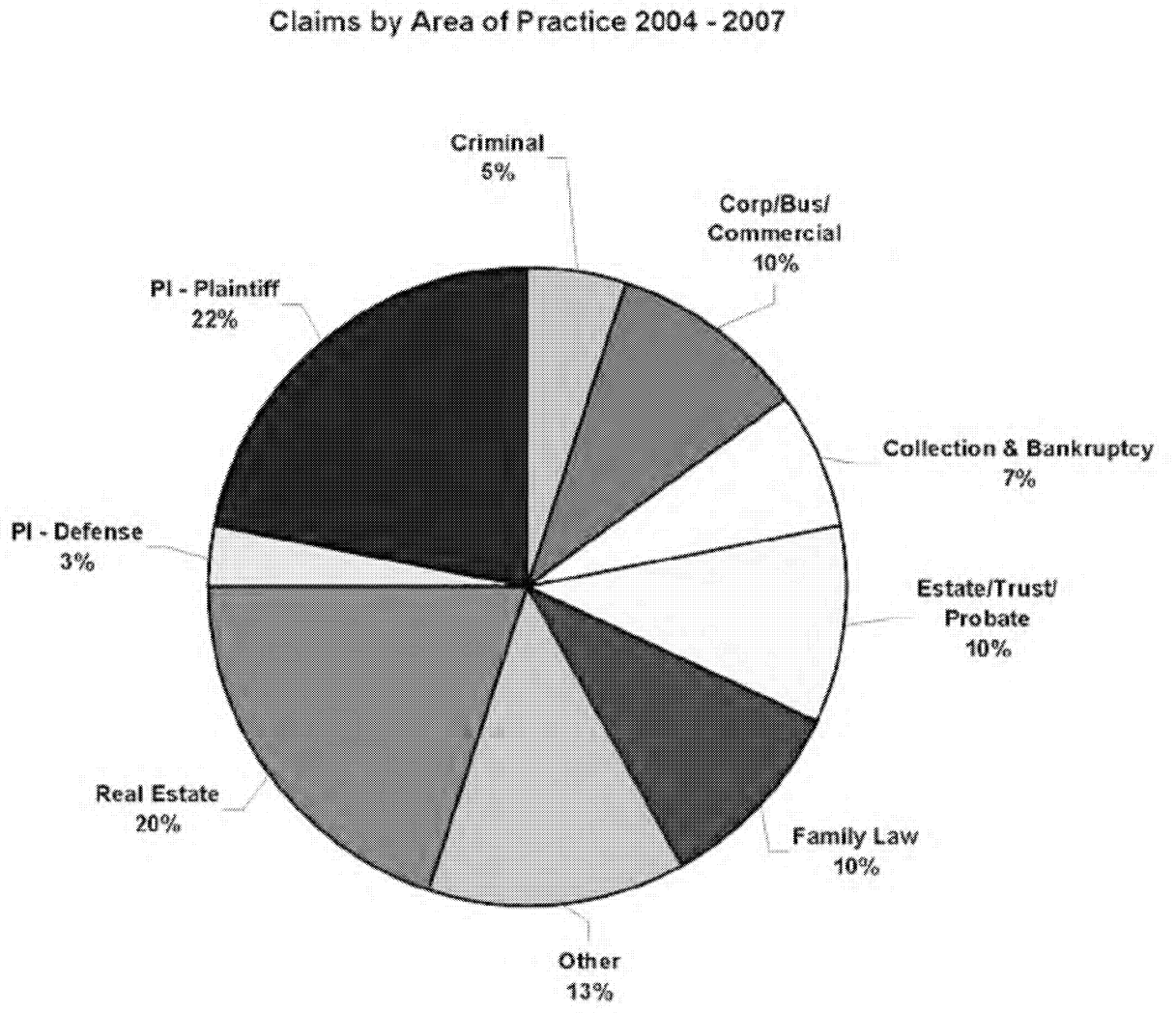
Had I deposited the money into my trust account, the next step would have been for Microtel to instruct me to wire the money to an account of their specifications. Typically, they instruct the lawyer to deduct the amount owed for legal fees and send the creditor the rest of the monies being held in trust. While we would not do that without the funds having actually cleared, in the interim, the imposter Microtel would have tried to get information from my firm's staff such as routing numbers, etc., to the trust account.

A number of firms are on the hook around the country for not waiting to make sure the checks clear before wiring the funds to the imposter client. Also, the banks are taking the position that, even if they verbally tell the lawyer that the funds are "available" or even if the wire transfer to the trust account is accomplished, the bank can still pull money back from the lawyer's trust account to satisfy the bogus official check.

The FBI says it is likely scam artists from Canada acting as an intermediary to other Nigerian scam artists. What makes it particularly realistic is that the written communications are not like the typical Nigerian or overseas emails you receive that are obviously scams. These are well written communications from someone with a very good command of the English language, and usually from a business person with very official looking documentation.

If anyone has a similar situation, they should contact the FBI. The Daytona Beach FBI agent I contacted says he has stacks of similar incidents on his desk from other businesses in the community being sued by the banks that made payment on the checks.

Claims by Area of Practice



Source: *Profile of Legal Malpractice Claims 2004-2007*, American Bar Association (2008)

Since 1985, the American Bar Association (ABA) has published a study of national legal malpractice claims data called the *Profile of Legal Malpractice Claims*. The chart above, "Claims by Area of Practice," is from the fifth and latest study, covering data from 2004 through 2007.

Regarding the results of the current study, the ABA wrote: " . . . noteworthy is how little the percentages have varied since the 2003 Study for the vast majority of claims categories." Personal Injury Plaintiff and Real Estate law have consistently ranked number one and number two respectively. The most dramatic change was the seven percent decrease in claims in the Personal Injury Defense category.

See a comparison of the areas of practice from all of the ABA malpractice studies, on page 4.

Comparison of Claims by Area of Practice: All ABA "Profile of Legal Malpractice Claims" Studies

Areas of Practice	2007	2003	1999	1995	1985
Personal Injury - Plaintiff	22%	20%	25%	22%	25%
Real Estate	20%	16%	17%	14%	23%
Family Law	10%	10%	10%	9%	8%
Estate, Trust and Probate	10%	9%	9%	8%	7%
Collection & Bankruptcy	7%	8%	8%	8%	11%
Criminal	5%	4%	4%	4%	3%
Corporate/Business Org.	5%	6%	9%	9%	5%
Bus. Transaction/Commercial	5%	3%	4%	11%	3%
Personal Injury - Defense	3%	10%	4%	3%	3%
All Other	13%	14%	11%	13%	11%

Totals may not equal 100% due to rounding.

407.382.1400 • 800.633.6458 • www.flmic.com • fax: 407.382.3130

Florida LAWYERS Mutual Insurance Company®

3504 Lake Lynda Drive • Suite 325
Orlando, Florida 32817-1484

CALIFORNIA BAR JOURNAL

OFFICIAL PUBLICATION OF THE STATE BAR OF CALIFORNIA - DECEMBER 2001

California BAR JOURNAL
Main Menu

REGULARS

Front Page - December 2001

News / News Briefs

- Partnership offers free legal services to terror victims
- Bills Signed by Gov. Gray Davis in 2001
- State Bar alcohol diversion program starts to take shape
- 56.9 percent pass the July bar exam
- Appeals court finds IOLTA constitutional

Trials Digest

Opinion

- From the President - Get involved in the art of legislation
- Our porous Canadian border
- Letters to the Editor

Appointment - Apply to serve on a bar committee

MCLE Self-Study

- Unbundling a hot-button

DISCIPLINE

Money laundering conviction leads to lawyer's resignation

A Los Angeles attorney convicted earlier this year of laundering money that was part of the haul from an armored car company heist has resigned from the State Bar with charges pending. **DAVID MATSUMOTO [#77325], 51,** was placed on interim suspension July 20 and gave up his license Sept. 6, 2001. He was sentenced in October to 27 months in federal prison after pleading guilty to six counts of money laundering and one count of aiding and abetting the filing of a false tax return.

Matsumoto, who lived in Las Vegas but practiced in Los Angeles, and his ex-law office manager, Joaquin Bin, were indicted in September 2000 on 71 counts of money laundering, structuring financial transactions and subscribing to a false income tax return.

Bin, a Santa Ynez Arabian horse-farm owner, pleaded guilty in April to seven counts of money laundering and was sentenced to 30 months in federal prison.

Matsumoto admitted he took $1 million from two of the robbers who stole $18.9 million from the downtown Los Angeles office of Dunbar Armored in 1997. Federal authorities said it was the largest cash robbery of an armored car company in U.S. history, and agents still don't know what happened to most of the money.

Bin also received $1 million from the robbers.

He and Matsumoto deposited their take in Matsumoto's client trust account. Some was used to buy a house in Las Vegas, Matsumoto wrote checks to the robbers to give the impression they were earning wages, and the rest of the money was invested, according to a federal prosecutor.

Most of the money was invested in Combustion Processing Manufacturing Corp., a Houston company that is trying to develop a machine to clean contaminated soil after oil spills.

ethical issue
- Self-Assessment Test
- MCLE Calendar of Events

You Need to Know

Discipline
- Ethics Byte - Lawyers are members of the public, too
- Money laundering conviction leads to lawyer's resignation
- Attorney Discipline

Public Comment

Matsumoto also issued a W-2 tax form to one of the robbers, implying that he earned more than $40,000 for legitimate work.

The case was broken when the FBI traced a broken tail light found at the robbery scene to a truck rented by Eugene Lamar Hill Jr. of Bellflower, one of the two who provided the money to Matsumoto and Bin.

After his arrest, Hill pleaded guilty and fingered his accomplices. All have been convicted, sentenced to federal prison for terms ranging from eight to 17 years, and ordered to pay $18.9 million in restitution.

Former Dunbar security guard Allen Pace III, who had been fired the night before the robbery, was convicted in June of masterminding the robbery.

He was sentenced to more than 24 years in prison.

Matsumoto, who was a sole practitioner, also faces charges stemming from a drunken driving arrest earlier this year.

Nova Scotia lawyer admits embezzling 'friendly-fire' funds

The Globe and Mail ^ | September 27, 2006 | Canadian Press

Posted on **September 28, 2006 at 1:01:29 AM EDT** by **Heatseeker**

Halifax — A high-profile lawyer who sued the U.S. government for the mother of a Canadian soldier killed by American friendly fire has admitted he embezzled money from his clients, CBC Radio reports.

A disciplinary board with the Nova Scotia Barristers Society heard that Dick Murtha billed for work he didn't do, hid insurance settlements from recipients and took out high-interest loans for clients without their knowledge, according to CBC.

That has added up to $200,000 now missing from his clients' accounts.

Darrell Pink of the society says Mr. Murtha violated almost every trust account regulation for maintaining books appropriately.

Mr. Murtha, a decorated war veteran, is claiming he suffers from post-traumatic stress disorder that dates back to his time in Vietnam, where he served with the U.S. Marines.

His lawyer, Brian Smith, says the 9-11 terrorist attacks and Mr. Murtha's work with Canadian families who lost relatives in the friendly fire bombing in Afghanistan have worsened his condition.

Mr. Murtha will be banned from practising law in Nova Scotia and his clients will be reimbursed by his insurance company or the barristers society, CBC reported.

Mr. Murtha was suspended last January while the society conducted its investigation. His office in nearby Lower Sackville, N.S., has been closed and the society transferred his files and clients to other lawyers with the help of a receiver.

Mr. Murtha represented the mother of Pte. Richard Green, who was killed in Afghanistan with three other soldiers when a U.S. pilot dropped a laser-guided bomb on their position during a night-firing exercise in 2002.

Mortgage scam probed in Toronto house flips; Seven homes in the Junction were taken on a wild real estate ride that ended in a lawyer's suspension

Toronto Star
Sat Jan 7 2012
Page: A1
Section: News
Byline: Tony Van Alphen Toronto Star

Something strange was going on in the Junction.

At least seven modest homes, all on avenues in the working-class west end of Toronto, experienced a pattern of flips and price jumps as much as 60 per cent in less than a day.

Most of the deals didn't include deposits. Purchasers got money back. Mortgages exceeded the value of homes. The same buyers and private lenders popped up in many sales.

In one sale, a buyer effectively sold a home to herself.

A few sales even involved a notorious real estate agent who ended up in prison last year for helping mastermind marijuana grow operations in scores of other houses across Toronto.

And behind all the 2003-2005 deals that often defied common sense is a freewheeling **lawyer** - Ron Allan Hatcher - representing multiple parties and running roughshod over his profession's rules of conduct.

A real estate expert, Jerry Udell, reviewed the complex and convoluted deals for the Law Society of Upper **Canada** in a subsequent disciplinary case. He concluded that all of them pointed to one thing - mortgage fraud.

A lot of it.

Mortgage fraud remains a serious problem in the real estate industry. In the U.S., it undermined the housing market during the bubble years of 2004-2005 and brought it crashing down.

But proving fraud in the U.S. and **Canada** can be time-consuming and elusive.

Finding victims is sometimes even harder. In the case of the seven Junction houses, police never laid charges or opened a criminal investigation.

The Ontario Real Estate Council, which regulates the industry, confirmed in November that it had opened an investigation into the transactions involving the houses and possibly more properties.

Except for a one-year suspension for professional misconduct against **lawyer** Ron Allan Hatcher by a law society panel recently, no one has experienced repercussions from the flips and other financial gymnastics involving those houses.

In response to requests from the Star for an interview, Hatcher noted in a brief email that the law society found "there was no fraud" and he suggested waiting for the panel's reasons and "all of the relevant facts."

The law society's panel ruled in October 2011 Hatcher engaged in professional misconduct for "participating in or knowingly assisting in dishonest or fraudulent conduct" by clients obtaining mortgage funds under "false pretenses."

It also found Hatcher, who became a **lawyer** in 1994, wasn't honest or candid with clients, didn't disclose conflicts of interest to them, or meet the standard of a "competent **lawyer**."

Former clients have also won at least two default judgments totalling more than $230,000 against him in civil courts for deficient work on house loans.

Mortgage fraud usually involves people falsifying information such as property values on loan applications so they can gain larger amounts of funds.

In many cases, they default on payments and mortgage funds disappear.

A normal real estate transaction involves a seller receiving money for a home.

But in the case of these seven houses, buyers received unexplained or unaccounted funds as well.

Flips at much higher prices would follow, with a combination of mortgages from financial institutions and private lenders.

In some instances, there were two flips on the houses.

In the final flip, the purchaser would gain as much institutional financing as possible based on the much higher prices negotiated between familiar players in each case.

While the law society panel focused on Hatcher's conduct in its deliberations, a stinging review of Hatcher's work by real estate **lawyer** Udell cited more than 20 "red flags" of "potential fraud" in the transactions.

One of the more curious series of transactions involved 148 Edwin Ave,. where Ivor Pinkett and his sister-in-law Helen Pinkett closed a deal to buy a house for $270,000 on Nov. 17, 2003. Their names would appear repeatedly in The Junction juggling.

The Pinketts' real estate agent for the purchase was high-flying Sau San (Jennifer) Wu, who would plead guilty to marijuana cultivation, tax evasion, utilities fraud, **money laundering** and violating bail conditions in May of this year.

Wu admitted acting as an agent in renting 54 houses to marijuana farmers and received a 61/2-year prison term. None of the grow operations involved the seven houses, according to police.

Hatcher represented both the buying Pinketts on the Edwin Ave. sale and private lenders, who provided a $279,000 mortgage - more than the actual purchase price.

A numbered company for the Pinketts then flipped the Edwin Ave. house for $310,000, or 15 per cent more. Oddly, the deal closed Nov. 14, three days before the first transaction.

The expert review by Udell, a Windsor **lawyer** with 35 years experience, said the price "was significantly inflated."

Furthermore, one of the buyers was Helen Pickett, who effectively bought the house from herself. There was to be a downpayment of $5,000, but the review couldn't find any record of it.

"The second agreement makes no sense and is an obvious sham," said Sean Dewart, a **lawyer** for the law society, in a brief at Hatcher's disciplinary hearing.

Hatcher ran into further conflicts in the latter transaction by acting for the Pinketts' numbered company (now the seller), and lender Bridgewater Financial Services, which provided a first mortgage of $284,580.

He also arranged for two more mortgages on the property totalling almost $100,000, which easily exceeded the purchase price again.

Udell's review for the law society said although Hatcher complied with a rule limiting mortgage amounts while representing borrower and lender, he should have declined the work in "such a clearly manipulated mortgage transaction."

The review also said Hatcher may have "misled" Bridgewater by telling the financial firm he held $37,100 in a **trust**

account for Helen Pickett's downpayment.

In fact, the property was bought with no equity.

In July 2004, Helen Pinkett defaulted and the property was sold under a power of sale process to another investor who was involved in a transaction on one of the other seven houses. Bridgewater collected $265,000, almost $20,000 less than its original mortgage investment.

Udell's review said Hatcher's multiple positions in the transactions were "extremely unusual."

It should have put Hatcher "on alert for a potential fraud" in connection with no deposits, price increases and mortgages exceeding 100 per cent.

He also failed to inform lender clients about the oddities, the review noted.

Ivor Pinkett, a house painter by trade, acknowledged buying and selling some of the houses, but stressed he didn't make any money and never suspected improprieties. Nor was he aware of the law society's case against Hatcher.

The Pinkett's also worked on renovating the homes to boost their value in a resale.

"There were flips all over the map," he recalled. "On some of the houses I worked on, we just walked away and never made anything."

He described Hatcher as a "nice guy and straight up," but added he was unaware about the suspension and hadn't talked to him in years. Helen Pinkett described him as "one of the nicest men I've ever met."

Meanwhile, the Edwin Ave. property continued to sell in transactions that involved some of the same players in previous Hatcher deals.

In 2006, the house sold for $450,000 under another power of sale, with the buyer receiving most of the financing from Money Connect Home Lending.

The listing described the home as "completely renovated."

The owner defaulted in 2009 and Money Connect conducted yet another power of sale.

This time, the house sold for $360,000, leaving Money Connect with a loss. The listing indicated "renovations started."

Transactions at a house on 176 St. Clarens Ave. again featured Hatcher representing the Pinketts as buyers.

There was a second flip with a 64-per-cent price increase in 14 months - from $329,000 to $540,000 - with no deposits and private lenders providing more than 100 per cent financing.

In that flip, which the society review described as "suspicious," Hatcher took on a new role - buyer.

Hatcher, his wife and mother bought the house when the owner who purchased from the Pinketts defaulted.

The price had also soared despite a gutting of the house, which made it uninhabitable.

The review also found that "substantial" funds were paid to renovate the property before closing the deal to the Hatcher family and the work was ultimately paid for by sale proceeds.

Udell said he had never seen such a practice in more than three decades of work.

Fellow **lawyer** Dewart had a blunt assessment of the St. Clarens transactions: "It was a sham and a fraud," he told the society.

He also charged in a brief to the law society that Hatcher had participated in transactions which he knew were frauds.

While admitting the failure to notify lender clients about jumps in property prices was "unprofessional and negligent," Hatcher insisted those actions didn't support allegations of complicity in fraud.

It remains a mystery whether Hatcher gained anything financially.

In his filings with the law society, Hatcher said there was no evidence he received excessive fees or payments on any of the seven properties.

TD **Canada** Trust, the Bank of Nova Scotia and Bridgewater Financial Services - which provided some of the mortgages for the properties - would not comment on whether they lost money.

Money Connect Home Lending, did not respond to inquiries.

Mortgage fraud can also have an impact on the local real estate market.

For example, quick house flips and a jump in prices can artificially raise the value of neighbouring properties.

In this case, it is unclear whether the big price increases or a general uptick in the market pushed up values on the same streets or nearby.

So where are the victims?

One veteran real estate **lawyer** who looked at the seven deals said it is possible that there were no victims because significant increases in market value swept away any possible losses.

"It appears the deals were designed to artificially inflate property values to get higher mortgage amounts than should be permitted," said the **lawyer**, who requested anonymity.

"But in these cases, everyone just got lucky and no one got hurt because market values eventually increased so much in Toronto. In the case of the banks, perhaps they just didn't do their due diligence and looked the other way. If property values had remained stagnant, it may have become a police matter."

In its arguments, law society staff told Hatcher's hearing that financial damage is not necessary to prove fraud under the law.

Some real estate officials say there is an industry impression that police only pursue major incidents of possible mortgage fraud.

However, Det. Sgt. Cam Field, who heads the Toronto Police Service financial crimes section, counters that his department will devote the staff and time if there is evidence of mortgage fraud.

"We know, based on the information from the law society, the potential of more victims in this alleged scheme," Fields noted. "If people think they were criminally defrauded, we strongly suggest they contact us."

In addition to the suspension and an order for $30,000 in costs, the law society rapped Hatcher with a reprimand and $2,000 in further expenses for failing to co-operate in the investigation of his conduct.

But society staff said the penalties aren't enough. They have appealed to a higher society panel to disbar Hatcher.

THE KINGSTON WHIG-STANDARD

Lawyer loses law licence

The Kingston Whig-Standard
Fri Mar 7 2014
Page: A3
Section: News
Byline: THE WHIG-STANDARD

A Kingston **lawyer** found guilty of professional misconduct for having sex with a client while representing both her and her husband in their divorce has been ordered to turn over his law licence or have it revoked. Jehuda Julius Kaminer had earlier been found in conflict of interest for initiating and maintaining a sexual or romantic relationship with a female client in 2006. Kaminer also received money from the client and failed to account for it nor deposit the money into a **trust account**. Kaminer also failed to properly respond to voicemail messages and letters sent by law society staff.

On Feb. 25, a hearing panel at the Law Society of Upper **Canada** ordered Kaminer to turn over his licence within 10 days or have it revoked.

He was also ordered to pay $20,000 of the Society's legal costs within six months. In January 2013, a Law Society hearing found Kaminer had engaged in unprofessional conduct for engaging in the relationship. In September he was suspended for six months.

The StarPhoenix

Regina lawyer suspended

The StarPhoenix (Saskatoon)
Wed Dec 18 2013
Page: A11
Section: Local
Byline: Barb Pacholik
Dateline: REGINA
Source: Leader-Post

The Law Society of Saskatchewan has taken the rare step of suspending a Regina **lawyer** - even before completing its investigation - after alleging misappropriation of thousands of dollars.

Well known family and estate **lawyer** Pauline Duncan Bonneau has been placed on interim suspension and isn't entitled to practise law until further notice.

Law society executive director Tom Schonhoffer said an interim suspension, while unusual, is imposed on occasion by the law society, the regulating body for the province's lawyers.

"It often is the result of an audit which provides information which is of immediate concern to protection of the public," he said.

Contacted Tuesday, Duncan Bonneau said she plans to resign her membership in the law society, meaning she would be ineligible to practise law regardless. "As a result of the problems, I have decided I will resign my membership and certainly regret the fact that these problems have occurred, but I'm doing my best to rectify the situation," added Duncan Bonneau, who has been practising law for more than 30 years.

"I did self-report the issues with respect to the **trust account** problems, and (have) made restitution," she said.

In its notice of suspension, the society accuses Duncan Bonneau of conduct unbecoming a **lawyer**. The allegations are that: In 2010, she misappropriated $19,800 from her **trust account**, by causing a law firm trust cheque that she created and signed to be deposited into her personal bank account.

In 2008, she misappropriated $14,879 from an estate when she took payment for a probate fee without ever having incurred that expense.

In 2011, she fabricated documents and submitted them to Information Services Corporation with the intent they be relied upon as genuine.

She took payment on two estate matters for legal fees totalling more than $70,000 via "in kind" payments of estate property without remitting income tax, GST or PST.

In 2013, she attempted to mislead the law society by providing it with a trust ledger that she had altered, along with additional altered supporting documents.

In response to the allegations, Duncan Bonneau said, "there were some accounting errors that occurred in my practice. I reported them to the law society, and made full restitution to the client that was involved." She said she also reported the situation to Revenue **Canada**. The suspension took effect on Dec. 11. **Lawyer** Scott Spencer of Robertson Stromberg has been appointed as trustee of Duncan Bonneau's legal practice. Schonhoffer explained that appointing a trustee further protects the public, by having someone to deal with clients' outstanding files.

He said the law society has an audit program that includes lawyers self reporting as well as unannounced "spot

audits" in law firms.

"It's often those types of processes that catch things," he said.

Schonhoffer declined to provide specific details about how this came to the society's attention while the investigation, which began only recently, is underway.

"Now an investigation committee is appointed by the law society and they make a report and decide whether a hearing is required," he said, adding the probe could take some time.

Schonhoffer said the Legal Profession Act requires the society to make a report to the attorney general's office if it discovers anything that may potentially involve a criminal act, "And so that (referral) will be done on this occasion."

In October and November, a hearing committee of the law society heard an unrelated complaint against Duncan Bonneau. The committee has yet to render its decision on liability.

According to the formal complaint in that matter, Duncan Bonneau was accused of altering a statement of account, abusing her power by threatening to increase fees charged to an estate if the beneficiaries requested a check by the court of her fees, and trying to compel a person to abandon a complaint against her to the law society.

bpacholik@leaderpost.com

Disappearance of lawyer, and $3.6M, devastates clients

Mississauga News
Fri Nov 29 2013
Page: 1
Section: News

MISSISSAUGA - Hasan Abuzour left the Middle East for **Canada** back in 2000, seeking refuge in a safe country renowned for its law and order.

Now he's virtually penniless and heading to court Friday - for the sixth time in seven months - desperately trying to salvage whatever he can from his life's hard work, some $3.6 million he thought was safe in a **trust account** and Heydary launched a high-profile lawsuit on behalf of investors in the Trump International Hotel & Tower.

No one is certain if the charismatic Heydary, 49, the founder of Heydary Hamilton and four other boutique downtown firms, is in his native Iran. According to one source, Heydary's wife told his law partners he's dead.

The Toronto Star has not been able to reach the wife or verify this.

The Law Society of Upper **Canada** is now in control of Heydary Hamilton, as well as Heydary Elliott, Heydary Green, Heydary Hayes and Heydary Samuel. Abuzour's **lawyer** Ray Thapar hopes auditors can unravel the complex financial web.

Most of the focus is on Heydary Hamilton because its trust fund is the only of the five firm's trust accounts that was solely controlled by Heydary himself.

Almost $163,000 was cleared out of the trust fund in just one day, Nov. 15. That was the court-imposed deadline for Heydary Hamilton, to hand over the Abuzour's money, according to financial records included in court filings.

That night Heydary, 49, left **Canada** for his native Iran, telling colleagues he had to tend to a sick relative. He hasn't been heard from since and no one answered the door at his Forest Hill Rd. home Thursday.

The Law Society of Upper **Canada** alleges that just $319,067.82 is left in the Heydary Hamilton trust fund and that Heydary himself is being investigated for "misappropriation, mishandling trust funds, and failing to comply with a court order."

In the wake of the resignations of some lawyers from the firm - and concerns among staff that Heydary "would be a very strong and disruptive presence in the office" if he returned - the Law Society took over as trustee of the businesses this week.

"I could have done family law, but I chose commercial litigation because there's no emotion, no drama," says Thapar, the Brampton **lawyer** that Abuzour is now looking to in order to save his family from financial ruin.

"But this is the worst I've ever seen. It's so important that people understand this is not just about a big Bay St. law firm, this is a real human tragedy."

Abuzour was an entrepreneur before coming to **Canada** from his native Gaza, buying up small apartment blocks, investing in businesses in hopes of building a better life in **Canada** for his family. His nine children range in age from 12 up to 32; four of them are married and on their own.

When Abuzsour decided to dissolve a printing business partnership last year, he needed a **lawyer** to handle the

paperwork. After searching the Internet, his son suggested hiring Heydary. Heydary ended up completing the deal for $200,000, says Abuzour. Abuzour was supposed to receive his $5.1 million share in installments, most of which were to be channeled through a trust fund, between last January and April.

Expecting to soon be flush with cash, Abuzour flew off to Egypt on vacation and put down a $500,000 U.S. deposit on a plot of land. Later he would put a $100,000 deposit on a property in Mississauga.

But after months, and more than 11 encounters with Heydary - who threw up a host of objections to handing over the money, including demanding sureties from Abuzour's former business partner on money the bank had already cleared - Abuzour contacted Thapar, head of commercial litigation at Simmons, da Silva and Sinton in August.

Worried that a relatively simple handover of funds had taken so long, he began proceedings to obtain the funds.

After numerous hearings, and what Thapar feared was just stalling from Heydary Hamilton, on Nov. 14 a judge gave the law firm until 5 p.m. the next day to hand over the funds.

The next night, the affidavit alleges, Heydary was on his way to Dubai and then his native Tehran.

"Lawyers are trusted to further the administration of justice and not obstruct it," says Thapar. "I've never seen anything of this magnitude.

As it stands, the Abuzours are not only out the $3.6 million, but also the $600,000 deposits on land deals which they can no longer afford to close.

"My clients made 11 requests to get the money and at every turn they were given excuse after excuse," says Thapar.

"What's happened here is a huge slight on the entire legal profession. When something like this happens it's a black mark on all lawyers."

Lawyer who fled to France loses licence

The Ottawa Sun
Tue Oct 29 2013
Page: 12
Section: News
Byline: MEGAN GILLIS, OTTAWA SUN

A former Ottawa **lawyer** accused of funneling hundreds of thousands from his clients before fleeing to France was stripped of his licence to practice law Monday.

Luc Edmund Barrick was a no-show at the Toronto hearing where he was found guilty of professional misconduct.

He was ordered to pay more than $100,000 to the Law Society of Upper **Canada**, which vowed to consider every option to collect the cash from Barrick, who lives in Paris.

"It's better than nothing, but ultimately what is it going to mean?" **lawyer** Meg Green asked. "They can't touch him there.

"The clients are not going to get their money back."

Green worked with Barrick as an associate in 2009 but left feeling she was owed money and suspicious that something wasn't right with her "charismatic, charming" colleague's dealings.

No criminal charges have been laid but an Ottawa Police spokesman said Barrick is known to

them and an investigation is underway.

The law society had alleged that between 2009 and 2011 Barrick raided a **trust account** of Barrick Domey Tannis LLP of more than $116,000 to finance a condo he bought in his own name and $58,000 for personal expenses.

Before he shut down the drained account in June 2011, he'd allegedly taken 11 clients' cash and retainers totaling $308,000.

There was $200,000 from two clients waiting for a property sale to close, $72,000 from a life insurance policy that was supposed to go to a beneficiary and a $25,000 divorce settlement.

Seven clients said they paid Barrick for services -- including filing for divorce -- never provided.

The former legal expert on a local radio show said in 2011 and again earlier this year by e-mail that that he'd left Ottawa for his health.

He has hemophilia.

"I became very ill and I had to withdraw from the practice of law much more quickly than I wanted to," he said, denying misappropriating funds and maintaining the condo was an investment for clients.

Two years ago, a judge called his actions "unprofessional and possibly criminal" as she set aside a six-figure default judgment against a local real estate agent.

The judge heard that Barrick had agreed to defend the man in a civil lawsuit then "absconded" with his $4,000 retainer.

"That left a very black mark on the legal profession," the judge said.

THE GLOBE AND MAIL

Toronto real estate lawyer charged with money laundering

Tu Thanh Ha **and** Jeff Gray
Toronto — The Globe and Mail
Published Friday, Jun. 08 2012, 10:37 AM EDT
Last updated Friday, Jun. 08 2012, 3:20 PM EDT

A long-time Toronto-area real-estate lawyer has been charged with money laundering in connection with a drug investigation where the RCMP froze more than $7-million in suspicious assets.

In addition to the money-laundering accusation, Kenneth James, 71, a solicitor whose law office, James and Associates, is based in Concord, Ont., has been charged with fraud over $5,000 and possession of proceeds of crime.

Also charged is Rosemary Cremer, 61, who faces one count of money laundering and one count of possession of proceeds of crime.

Ms. Cremer is an employee at Mr. James' law firm.

In addition to raiding Mr. James' office on Thursday, police also executed a search warrant at Ms. Cremer's Willowridge Road residence.

Mr. James lives at Ms. Cremer's residence but investigators are not aware of a personal relationship between the two, said Detective Inspector Derek Matchette of the RCMP's Integrated Proceeds of Crime unit.

Land records show that the house, which was purchased for $221,000 two decades ago, was re-mortgaged last February for $130,869. That debt was discharged two weeks ago.

The RCMP said they also filed money laundering and possession of proceeds of crime charges against Mr. James' law firm and two companies, Eveline Holdings Limited and Sterling Capital Inc.

Court documents in previous litigations show that Mr. James has acted as Eveline's solicitor in Ontario and that at one point he got part of a disputed $2-million sum to be wired to Eveline off-shore accounts in the Turks and Caicos.

The RCMP said the charges filed this week stemmed from a two-year investigation into the exportation of drugs from Canada that began in June 2010 with the force's GTA Drug Section. A primary suspect and other people have been arrested but details are under a publication ban.

"Criminal organizations frequently use sophisticated means to launder the profits of their crimes . . . By removing those illicit profits and bringing to justice those who assist criminal groups we are able to disrupt organized crime that affects all Canadians," RCMP Inspector Mark Pearson, the officer in charge of the Toronto Integrated Proceeds of Crime Unit, said in a statement.

Mr. James has previously been named in a number of civil litigations and one criminal case.

In an Ontario Superior Court decision last year in a Mississauga real-estate fraud case, the court heard that "fraudulently obtained funds" were moved between several accounts including one belonging to James and Associates.

Canadian trustees of the Church of Jesus Christ of Latter-day Saints have also alleged in court litigations that in 1990, Mr. James was the solicitor in a number of real-estate transactions where Mormon church properties were flipped and the profits pocketed without the church's knowledge. The church eventually dropped its action against Mr. James.

Mr. James also faces an ongoing disciplinary proceeding before the Law Society of Upper Canada, which he has been fighting. In May of 2010, the legal profession's regulator alleged he had participated in or knowingly assisted with "fraudulent or dishonest conduct" in connection with 12 Toronto-area mortgage transactions. If he is found to have violated the profession's rules, he could lose his licence to practise law.

Law enforcement agencies have long identified lawyers, and the use of their trust accounts by potentially unscrupulous clients, as weak links in worldwide efforts to crack down on money laundering.

But Canada's legal profession has waged a battle in court for over a decade, successfully resisting attempts to include it under Ottawa's anti-money-laundering regime. The rules, among other things, require bankers and others who handle money to report certain suspicious transactions. The Federation of Law Societies of Canada argued the rules threatened lawyers' independence and required them to betray their clients.

Instead, law societies across the country have brought in their own rules to combat money-laundering, including the banning of lawyers from accepting cash deposits into their accounts of more than $7,500, excluding payments of legal fees.

Authorities to probe another disbarred lawyer

FEBRUARY 23, 2014 | BY **KNEWS** | FILED UNDER **NEWS**

The leadership of Guyana's judiciary is to probe yet another Guyanese lawyer who has run afoul of the law while practicing overseas.

This has resulted in him being struck off the list of attorneys eligible to ply their trade in Canada where he committed the offence.

However, he is still operating openly in Guyana.

Attorney General Anil Nandlall told reporters on Friday that while "I have not yet received formal notification about the (Canadian) case," he has nevertheless forwarded correspondence to Chancellor Carl Singh about the issue of Attorney Vishnu "Joey" Poonai being disbarred by judicial authorities in Canada after he was convicted and served time for committing frauds that involved millions of dollars.

The former Canadian based lawyer was ordered by the Milton Superior Court back in 2007, to pay CND$59,000in restitution to several banks before serving his three and a half years prison term for mortgage fraud. Poonai was further disbarred by the Upper Law Society of Upper Canada.

Nandlall confirmed however that the members of the Guyana Bar Association (GBA) have expressed concern over the issue. This written concern, he added, has been dispatched to the Chancellor. "Someone from the Bar Association wrote to me and I forwarded the letter to the Chancellor," the AG said.

President of the local Bar Association Ronald Burch-Smith told media operatives that a member of the organization's Executive Council-in a personal capacity-wrote the AG last November expressing concerns over the disbarred lawyer. Secretary to the Bar Christopher Ram also confirmed making the issue known to senior judiciary officials.

Poonai told Kaieteur News that he will continue to practice here since he was admitted to Guyana's Bar, "long before" he was admitted to the Canadian and UK Bars. He said his, "problem in Canada has nothing to do with what I am doing here." "I am licensed to practice in Guyana and until somebody stops me… I will practice here."

According to the online report from Law Times, Poonai, the Brampton Ontario lawyer defrauded four financial institutions of some $4M. A 99-page agreed statement said that the former real estate lawyer admitted to engaging "in professional misconduct and that the appropriate penalty was immediate disbarment."

The law society said that Poonai was involved in 13 counts of professional misconduct, including acting as the solicitor in 49 mortgage transactions between 1997 and 2003 where he knowingly assisted in a scheme to obtain mortgage funds from mortgagees under false pretences, in what the court called a "flip fraud."

The total aggregated loss to the financial institutions (the rest was covered by insurance) was $2,853,403, according to the ruling from Poonai's criminal trial.

The lawyer was arrested in October 2003, and pleaded not guilty to the initial set of charges during his trial. At one point, he claimed that the Law Society of Upper Canada had given him permission to do the flips. The frauds occurred when a property was purchased around its market value, conveyed immediately afterwards for a falsely inflated, significantly higher price to a second buyer who was not a bona fide buyer and mortgage funds were advanced based on the higher second selling price. The difference between the funds needed to close the first deal and the mortgage for the second deal is the profit for the fraudsters, with the mortgage then falling into default.

In these lucrative flips, Poonai or another lawyer "acting in concert with him" would act for all the parties including the lending institution, without fully apprising the lender of the circumstances of the transaction.

In one of the transactions, the report said, the property saw a 2.123-per-cent increase in price over the two-week period between the first agreement and second agreement, resulting in a $275,999 profit. Another property increased by 1.508 per cent over four days.

The agreed statement notes that Poonai "admits that the transactions were dishonest and fraudulent and that he was aware of their dishonest and fraudulent nature."

The report went on to say that in October 2003, Poonai was also charged with five counts of fraud over $5,000 relating to 12 real estate transactions between April 2002 and May 2003. The court lists the Royal Bank of Canada, the Bank of Montreal, CIBC Mortgages Inc., and Scotia Mortgage Corp., as being defrauded in the schemes.

While the misconduct proceedings against him were initiated in 2003, in 2004 Poonai agreed to an interim suspension in exchange for an adjournment sine die of the law society proceeding, pending the outcome of the criminal trial.

He was found guilty on December 22, 2006 of four counts of fraud over $5,000 and pleaded guilty to an additional count of fraud over $5,000 on March 30.

In December, Poonai was found guilty of professional misconduct for providing legal services while suspended and

destroying client property. At that point, he was ordered suspended for two years. Ten days later, he was convicted of four counts of criminal fraud in the Ontario Superior Court, with Justice John Murray concluding: "Mr. Poonai acted in a manner that reasonable, decent persons would consider dishonest and unscrupulous."

It was noted by the Law Times that two other lawyers – Pretam Kaur Purewal and Patience Boatemaa Whyte – were also involved in the frauds. It was reported that, "They knowingly assisted in or encouraged dishonesty, fraud, crime, and/or illegal conduct or to have become the dupe of clients who were engaged in dishonesty, fraud, crime, and/or illegal conduct, with respect to several properties." Whyte was given permission to resign in January and Purewal was disbarred on March 19.

Grant Thornton

Reporting Entity Sector Profiles: Money Service Businesses Appendix B

Prepared for FINTRAC | March 31, 2014

Appendix B: Case examples and typologies

The enclosed articles have been sourced from news media databases, books and the Internet, and provide specific examples of the risk factors identified in the report.

1. Western Union faces probe for fraud-induced money transfers. Reuters, February 25, 2014.
2. The hawala money trail: How a tiny money-transfer service in Ottawa was linked to bin Laden's multimillion-dollar global financial empire. The Ottawa Citizen, November 10, 2001.
3. Israel cracking down on money changers. Haaretz, March 19, 2014.
4. Texas man convicted in $3.9 million money laundering scheme. United States Attorney's Office, Middle District of Pennsylvania, July 22, 2013.
5. Global finance: Currency probe reaches to Julius Baer. The Wall Street Journal, February 4, 2014.
6. Forex market investigation: Collusion in the chat rooms? Bloomberg Businessweek, January 2, 2014.
7. U.S. unveils world's 'largest' money laundering probe. ABS-CBNNews, May 29, 2013.
8. Fears of financing terror closes another money transfer outlet for overseas Somalis; Terror financing fears stop transfers to Somalia. Canadian Press, June 25, 2013.
9. Police investigate a money transfer service after allegations of theft. Australian Broadcasting Corporation News, December 12, 2013.
10. Funding terrorism: Illegal cash flows may be aiding terrorists. The Financial Daily, January 6, 2014.
11. Money agency fined for laundering. The Australian, December 18, 2013.
12. Italy money laundering probe swoops on 21 cash transfer bureau. Reuters, October 31, 2012.
13. 2 face charges of money laundering; Langley men operated two currency exchanges. The Vancouver Sun, June 27, 2009.
14. Raids on hawala trader expose Rs 400-crore deals. The Times of India, February 4, 2014.
15. Why did criminals trust Liberty Reserave? The New Yorker, May 31, 2013.

Western Union faces probe for fraud-induced money transfers

Tue Feb 25, 2014 12:43am EST

Feb 25 (Reuters) - Money-transfer company Western Union Co is being probed by the Federal Trade Commission and a U.S. district court over fraud-induced money transfers, the company said in a regulatory filing on Monday.

The company said it received a civil investigative demand from the FTC on Feb. 21, requesting documents related to consumer complaints regarding fraud-induced money transfers sent from or received in the United States since 2004.

Western Union also said it has received multiple subpoenas since Nov. 25 from the U.S. attorney's office for the Middle District of Pennsylvania.

The inquiries have sought documents related to complaints made by consumers to Western Union relating to fraud-induced money transfers since Jan. 1, 2008, as well as information about Western Union's agents, the company said in the filing.

"The government's investigation is ongoing and the company may receive additional requests for information as part of the investigation," Western Union said.

Western Union has been battling the FTC over a civil investigative demand for information about consumer complaints in December 2012. A federal judge in New York ordered the company to comply with the request last December.

The world's largest money-transfer company reported a 27 percent drop in fourth-quarter profit, largely due higher costs linked to tightened regulations to prevent money laundering.

OTTAWA CITIZEN

The hawala money trail: How a tiny money-transfer service in Ottawa was linked to bin Laden's multimillion-dollar global financial empire

The Ottawa Citizen
Sat Nov 10 2001
Page: B1 / FRONT
Section: Saturday Observer
Byline: Ian MacLeod
Column: Ian MacLeod
Source: The Ottawa Citizen; with files from Citizen News Services

After scouring the globe, the hunt for Osama bin Laden's cash flow came crashing down this week on an ironic Ottawa address -- Bank Street -- and a tiny money-transfer service in a Somali grocery store.

U.S. President George W. Bush alleged this week that the service used by unsuspecting Somali immigrants at the back of the modest south-end shop is part of a sophisticated, underground financial network funnelling millions to the al-Qaeda **terrorist** organization.

About five per cent of the cash transferred from such hawala operations to oversees family and friends is skimmed and diverted to al-Qaeda, officials charge. The worldwide network, they say, generates an estimated $25 million U.S. annually for Mr. bin Laden's **Terrorism** Inc.

The Canadian government quickly added the Ottawa service, Barakaat North America Inc., to its list of companies whose assets are being frozen in the war on **terrorism**. About $72,000 is believed to have been frozen in the business's bank account.

Across town the same day, Somali immigrant Liban Hussein stood outside his family's Orleans townhouse pleading his innocence to a newspaper reporter.

Mr. Hussein, 31, operates a Barakaat outlet near Boston and is charged there with illegally operating a money transfer business. He too is now on the U.S. blacklist. His brother, Mohamed, was arrested in Boston on Wednesday.

On Thursday, the shades were down and the Pineglade Crescent home appeared deserted.

Canadian officials have since offered few details on how the hawala counter at a mom-and-pop Ottawa grocery store and a man inside a home on a suburban Canadian street came to be fingered by the president of the United States for possibly aiding and abetting the world's most wanted thug.

But U.S. intelligence officials point to Barakaat North America's Somalia-owned parent firm, al Barakaat (Arabic for blessings), a banking and telecommunications conglomerate with branches from the United States to Australia.

The Boston Globe reported yesterday that the business was founded by Mr. bin Laden, Somali financier Ahmed Ali Jumale and a radical Somalia-based Islamic group. It is one of several connections Mr. bin Laden has to the war-torn African nation.

In fact, of the 62 organizations and individuals that had financial assets in the U.S. frozen this week because of suspected al-Qaeda ties, 25 are located or have offices in Somalia, where Mr. bin Laden is believed to have played a key role in the bloody campaign against U.S. peacekeepers in the early 1990s.

At the time, Somalia had a well-established financial network, much of it built on contributions from the Saudi

government and wealthy Saudis to the regime of Siyad Barre, which fell in 1991. In the political turmoil that followed, Mr. bin Laden was able to gain control of the network and use it to fund his anti-U.S. operations in Somali, according to the book Bin Laden: The Man Who Declared War on America.

Authorities say Mr. bin Laden and his associates have since used the network to help build their al Barakaat organization and bankroll a killing campaign on U.S. soil. U.S. Treasury Secretary Paul O'Neill this week called the business a "pariah of the civilized world" and said it also aides **terrorist** groups by fudging records, relaying intelligence, communications and helping far-flung **terrorist** allies stay in touch.

The Wall Street Journal says al Barakaat is one of the world's largest hawala networks. U.S. officials claim Mr. Jumale, the head of al Barakaat, has a long relationship with Mr. bin Laden stretching back to the war in Afghanistan in the 1980s.

"He has used al Barakaat's 60 offices in Somalia and 127 offices abroad to transmit funds, intelligence and instructions to **terrorist** cells," the White House said in a statement. Mr. Jumale denies any ties to Mr. bin Laden.

Still, official portrayals of Barakaat and related firms as shadowy, underground operations, are somewhat misleading. Barakaat North America Inc., for instance, is listed on page 644 of the Yellow Pages, under "Money Order & Transfer Services," right along with Western Union.

Sharif Abdalla, the man who ran the Ottawa service and whom authorities have not accused of any crime, said he deposits his customers' money into a TD-**Canada Trust account** and then has it legally wired to a company office in the United Arab Emirates city of Dubai. Mr. Abdalla says he has transferred about $700,000 annually since 1996 for clients across **Canada**. From Dubai, the money is believed to be relayed to the intended recipients by hawala brokers in various countries.

In a traditional hawala operation, a customer hands over cash to the agent who, for a small fee, promises to get the money to the recipient. The agent then arranges, either through a phone call, fax or e-mail, to have a hawala agent in the receiving country hand over the money in local currency.

The agents settle their accounts, perhaps once a year, to make sure that neither is owed any money. There is usually little or no paper trail and the agents' profits come mainly from changes in currency values and commissions off large transfers, often made by criminals.

But officials now realize that hawala networks also have had very open relationships with western banks and that there have been warning signs about some of al Barakaat's suspected activities.

The Wall Street Journal reports that al Barakaat used several unwitting U.S. firms -- Royal Bank of Scotland PLC's Citizens Bank unit, KeyCorp.'s Key Bank unit, J.P. Morgan Chase & Co.'s Chase Manhattan, and First Data Corp.'s Western Union, Citigroup Inc.'s Citibank unit and SunTrust Banks Inc. -- for its alleged activities.

About $110,000 U.S. in transfers from Dubai to two of the hijackers involved in the Sept. 11 attacks on New York City and Washington, D.C., moved from an exchange house in the U.A.E. via Citibank in New York to the hijackers' joint account at SunTrust.

The modus operandi of Barakaat North America, the newspaper says, is very similar to how a group of Russian-born businesspeople moved about $7 billion U.S. in questionable funds through Bank of New York Co. in the mid-to-late 1990s. Two people involved in that scheme since have pleaded guilty to a conspiracy to launder money; Bank of New York hasn't been charged with any wrongdoing.

The criminal complaint against the Husseins outlines ties between Barakaat North America and the al Baraka Exchange, an al Barakaat outfit that is one of dozens of wire-transfer houses that pepper Dubai's city centre and serve the more than two million foreign workers in the U.A.E, the newspaper says.

The complaint says the brothers opened accounts with two U.S. banks last year -- Citizens Bank in Boston and Key Bank in Portland, Maine -- so they could make transfers. From March 2000 through Aug. 1, nearly $1 million U.S. was transferred to the U.A.E. from the Key account. Between July 5 and Sept. 26 of this year, $595,373 was sent from Citizens to Chase in New York, then on to Emirates International Bank in Dubai, a hub of Islamic financial activity.

When the funds arrived at Emirates International, a prominent U.A.E. institution, they were deposited in the account of al Baraka Exchange. Many of of the city's wire-transfer houses, including al Baraka Exchange, offer to send transfers via Western Union, a unit of First Data Corp. of Denver. Government officials say the Sept. 11 hijackers also received funds from U.A.E. via Western Union. The company, which recently told investors it has signed agreements this year with transfer firms in India, China, Thailand, South Korea, Yugoslavia and the Ukraine, declined to comment other than to say it cooperates with law enforcement.

In all, yesterday's Boston Globe reported, Barakaat North America received deposits of more than $3 million between January and September alone. And as of Wednesday, U.S. officials said, they have seized nearly $1 million in Barakaat assets.

Authorities emphasized the Husseins may not have realized some of the money from their business might have eventually made its way to **terrorists**.

"There are no charges at this point about any connection to **terrorists** or suspected **terrorists**," said Samantha Martin, a spokeswoman for the U.S. prosecutor's office.

As far back as August 1997, Liban Hussein opened two accounts at another bank, BankBoston, and received permission to use the accounts to make transfers, the The Boston Globe reported

But in April 1999, BankBoston told Mr. Hussein it planned to close his accounts because of suspicious activity: repeated deposits and wire activity just under $10,000. He sued, claiming the branch manager told him his business was being used for illegal money laundering.

In court documents, Liban Hussein claimed his company functioned simply as a wire transfer agent for al Baraka, "not in any way different from other corporate businesses like the Western Union and the MoneyGram."

The Husseins' **lawyer**, Sam Osagiede, told The Boston Globe the FBI investigated the brothers and their company for possible links to **terrorist** groups and found no connection.

The U.S Treasury Department this week also froze a a Seattle bank account used by Barakat Wire Transfer Co., based in the back of a neighbourhood food market. Washington State documents show the business, formally established April 11, estimated its gross annual income at $28,001 to $60,000. Under the heading "business description," it says: "We transfer money sent by people in the U.S.A. to their relatives in Somalia, Kenya, Ethiopia, etc."

Other documents provided by Massachusetts regulators suggest another reason al Barakaat was able to penetrate the U.S. banking system with relative ease.

Al Barakaat's Mr. Jumale, documents indicate, learned his banking from Americans. From 1979 to 1986, according to a resume for Mr. Jumale submitted to Massachusetts regulators, he worked in Jeddah, Saudi Arabia as a senior clerk at the Saudi American Bank. The bank was founded by Citibank, which owned 40 per cent of it at the time he worked there. Among the bank's seminars he attended: "Money Remittance Operations."

But one of al Barakaat's European partners says the allegations against Mr. Jumale and the group of companies is a joke.

"Sheikh Ahmed (Ali Nur Jumale) has been a very good friend of mine over the years, and I am shocked at some of the perceptions of the Barakaat 'empire,"' said Mike Fitzgerald of Ireland's Microcellular Systems. "It is comical really."

Mr. Fitzgerald's communications company financed al Barakaat's move into telecommunications in the 1990s with an initial investment of $800,000, and says he is absolutely certain al Barakaat had no other source of funds.

"If bin Laden was involved, money would have come from him, but it never did," said Mr. Fitzgerald, who said his company was bought by InterWAVE of the U. S. last year.

Mr. Fitzgerald has spent years with Mr. Jumale and his associates, meeting him regularly in Dubai and training many of his leading managers in telecommunications for weeks on end in Britain.

"We have always had to trust them, and it would be impossible for them to be evil **terrorists**," Mr. Fitzgerald told

Reuters in a telephone interview. "You can look in Sheikh Ahmed's eyes, and you know he is a good person."

Analysts say the closure of al Barakaat, one of Somalia's biggest private sector companies and employers, will further cripple the economy in impoverished Somalia, already facing a humanitarian crisis caused by drought and inflation.

Al Barakaat

- Al Barakaat is a type of hawala, which means "in trust" in Hindi, an informal system of transferring funds globally based on trust, family, friends and a small fee that is used in many Arab, south Asian and East African countries.

- Hawalas are often housed in small nondescript rooms above a store, the tools of the hawala in **Canada** are a telephone, fax, safe and a book of receipts.

- the Manager of One Hawala Agency in Toronto That Services Primarily East African Clients, An Offshoot of a Company Based in Dubai, Said Canadian Brokers Transfer, on Average, Between $30,000 and $120,000 a Month.

HAARETZ.com

Israel cracking down on money changers

Demands more info on large transactions, details on big customers, to foil terror, money-laundering.

By Sivan Aizescu | 10:10 19.03.14 | 1

Tweet

Money changers face tougher reporting requirements, following the Knesset Constitution and Law Committee's approval of regulations yesterday to prevent them being used as conduits for laundering money.

The new regulations will require money changers to report on large transactions to the government's Anti-Money Laundering Authority, as well as the details of the customer.

They will also be required to implement a "know your customer" policy to ensure that customers are not connected with the shadow loan market or with terrorist groups.

Until now only banks were required to report such transactions to the authorities in which money laundering or terror finance might be suspected. But experts say money changers are key conduits for organized crime to launder money and that many changers are owned by criminal groups.

The new regulations — which passed the committee by a 5-4 vote — which go into force in another nine months, require money changers to report all transactions in excess of 5,000 shekels ($1,445) involving funds coming into or going out of the country without reporting the identity of the customer. The same rule will apply to all transactions in excess of 10,000 shekels cash or 50,000 shekels in any form.

They will also be required to identify all customers or beneficiaries of foreign currency transactions whose total business exceeds 200,000 shekels in any six-month period. Money changers will be required to identify the source of the funds being changed and report any suspicious transactions to the authorities.

Adi Barkai, an attorney who represents money changers, said the law added a regulatory burden on money changers and would not achieve its goals.

"The problem today is not about collecting information on customers. The problem is the lack of enforcement of existing regulations," Barkai said. "The authority knows very well that side by side with regulated money changers, a big industry of unsupervised changers is operating."

Combined with changes planned to tax regulations, the money changing restrictions will strike a blow at the ultra-Orthodox community, many of whose members engage heavily in off-the-books transactions to avoid taxes.

On Tuesday, Haredi lawmakers objected on procedural grounds to how the committee vote was conducted and asked it to be taken again, which resulted in the committee re-voting along the same lines two hours later.

Texas Man Convicted In $3.9 Million Money Laundering Scheme

FOR IMMEDIATE RELEASE July 22, 2013

The United States Attorney's Office for the Middle District of Pennsylvania, announced that following a week long jury trial before U.S. District Court Judge Christopher C. Conner, a Texas man was convicted on July 19 on 14 Conspiracy and Money Laundering counts stemming from a scheme to defraud hundreds of victims across the country, including several from central Pennsylvania, out of more than $3.9 million and to launder the proceeds.

Olufemi Adigun, age 27, of Stafford, Texas, was indicted in December 2012 along with two other defendants, Uchechukwu Stanley Ohiri, age 29, and Benjamin Chikwe, age 32, both of Houston, Texas.

According to U.S. Attorney Peter J. Smith, the trial revealed that in 2008, Adigun operated MoneyGram and Western Union outlets out of an empty Houston storefront known as "FAB Tax Services," a fictional tax service provider. The storefront was used by Adigun and his codefendants to intercept and launder $3.9 million sent by victims defrauded by advance fee, mass marketing schemes via the MoneyGram and Western Union money transfer systems.

The schemes rely heavily upon the MoneyGram and Western Union money transfer systems for success. More commonly known as Secret Shopper, Advance Fee, or Canadian Lottery schemes, perpetrators contact victims via the U.S. mail or the internet promising large cash prizes, lottery winnings, fictitious loans, or automobiles and motorcycles for sale. Counterfeit checks are sometimes sent to the victims who are induced into depositing them before returning a portion of the funds to the fraudsters via the MoneyGram and Western Union money transfer systems. The victims suffer a financial loss when the counterfeit checks bounce or after they send the fraudsters thousands of dollars of their own money for non-existent merchandise.

Adigun and his codefendants would intercept the victims' money transfers and launder the proceeds before sending the proceeds back to the fraudsters minus a money laundering fee, typically 10-20%. Adigun and his codefendants would also enter false payee identification information into the MoneyGram and Western Union databases, thereby maintaining the anonymity of the fraudsters and creating the illusion that a bona-fide payee had physically entered the receiving outlet.

In almost all of the schemes the victim sender is instructed to provide the Money Transfer Reference Number (MTRN) to the fraudster immediately after the transfer is sent. Armed with the MTRN, FAB Tax Services or any other corrupt money transfer agent could query the MoneyGram and Western Union money transfer databases and remove the funds from the systems, even though FAB was physically located thousands of miles away from the intended payee.

Adigun began operating FAB as a Western Union outlet in December 2007 and as a MoneyGram outlet in May 2008. Thereafter, more than 500 customers filed Consumer Fraud Reports (CFRs) with the two companies complaining they had been defrauded. The investigation revealed all 500 of the transfers had been paid out at FAB. As a result, MoneyGram and Western Union terminated FAB on August 20, 2008 and September 2, 2008 respectively. By that time, however, more than 1,241 victims had been defrauded out of $3,919,711. Adigun and his codefendants laundered $3.1 million of the $3.9 million by converting it into cash, withdrawing as much as $70,000 to $80,000 a day from 3 FAB bank accounts they controlled in the greater Houston area. The trio also forwarded another $650,000 offshore via the MoneyGram and Western Union money transfer systems, primarily to Canada, Nigeria and Romania. More than $100,000 of the offshore transfers were sent to just one MoneyGram agent in Toronto, which was also later closed for money laundering activity.

Adigun's codefendant, Benjamin Chikwe, pleaded guilty to conspiracy to commit money laundering and is awaiting sentencing. Uchechukwu Stanley Ohirihas remains a fugitive.

Following the conviction, Judge Conner revoked release and committed Adigun to prison pending the sentencing in October.

This case was investigated by the Harrisburg Office of the U.S. Postal Inspection Service and was prosecuted by Assistant United States Attorney Kim Douglas Daniel.

The Postal Inspectors' investigation has resulted in the conviction of more than 21 corrupt MoneyGram and Western Union agents from across the United States and Canada in the Middle District of Pennsylvania. The Postal Service's investigation has also resulted in the prosecution of MoneyGram in the Middle District for aiding and abetting wire fraud, and for its failure to maintain an effective anti-money laundering program as required by federal law. In November 2012 the Company entered into a Deferred Prosecution Agreement with the government that required MoneyGram to pay $100,000,000 into a victim's restitution fund, to make substantive improvements to its anti-money laundering programs, and to retain a Corporate Compliance Monitor selected by the government for the next five years.

FACTIVA DOW JONES

THE WALL STREET JOURNAL.
U.S. EDITION

Global Finance: Currency Probe Reaches to Julius Baer

By John Letzing and Chiara Albanese

549 words
4 February 2014
The Wall Street Journal
J
C3
English

The chief executive of Switzerland's Julius Baer Group AG said the private bank has had to "clarify a few cases" of currency trading to the country's regulator, an indication that the global investigation of possible market manipulation has spread beyond the big lenders that have been at its center.

Several of the world's largest banks, including Deutsche Bank AG and Citigroup Inc., have suspended traders since the probe started in April. Those two banks alone facilitate just under one-third of all currency trading.

During a presentation Monday of Julius Baer's annual results, Chief Executive Boris Collardi said the bank has been approached regarding the foreign-exchange probe, adding that it had to "clarify" some cases in which the bank had hired employees from larger lenders "more in focus" in the investigation.

In a subsequent interview with The Wall Street Journal, Mr. Collardi said the Swiss financial regulator, Finma, was the only one to contact the bank regarding the matter. Mr. Collardi said the regulator had inquired about "a couple of employees" who had joined the bank from UBS AG and Credit Suisse Group AG, though ultimately "it hasn't been necessary" to discipline or fire anyone as a result.

The Zurich-based bank maintains a foreign-exchange trading desk for its private banking clients. It ranks 62nd in global currencies-market trading, according to the annual Euromoney survey.

A spokesman for Finma said its investigation of foreign-exchange markets was continuing. UBS declined to comment on the Julius Baer probe, while a Credit Suisse spokesman didn't respond to a request for comment.

In October, Finma said it was conducting probes into "several Swiss financial institutions in connection with possible manipulation of foreign-exchange markets." That same month, in an interview with a Swiss media outlet, Credit Suisse Chairman Urs Rohner said the bank had received inquiries from regulators but hadn't found any evidence of foreign-exchange manipulation.

UBS, whose currencies-dealing business is one of the biggest, said in October that it had taken disciplinary action against employees during its internal review of its foreign-exchange business.

In January, HSBC Holdings PLC became the latest big bank to suspend traders. Around the same time, Citigroup suspended two people, adding to one previous firing over this issue.

As previously reported by The Wall Street Journal, Standard Chartered, PLC last year suspended a trader who had recently moved to the U.K.-based bank from UBS.

Meanwhile, Julius Baer said assets under management it will draw in from a continuing acquisition will be at the low end of expectations and reported a 30% decline in 2013 net profit.

The bank is in the midst of an acquisition of Bank of America Corp.'s Merrill Lynch wealth-management business outside the U.S., a process that is expected to last until next year.

Overall, assets under management rose 34%, to 254 billion Swiss francs ($280.3 billion), in 2013 from the previous year. Net profit fell to 187.8 million francs, pressured by the cost of the Merrill Lynch deal.

In Zurich, Julius Baer's shares fell 5.9%, to 41.44 francs.

Bloomberg Businessweek

Markets & Finance

http://www.businessweek.com/articles/2014-01-02/foreign-exchange-traders-may-have-used-chat-rooms-to-rig-market

Forex Market Investigation: Collusion in the Chat Rooms?

By Liam Vaughan, Gavin Finch, and Bob Ivry January 02, 2014

It's 3:40 in the afternoon in London, and computers blink red and green as traders buy and sell billions of dollars of currency. The pace picks up with the approach of the "fix"—the one-minute period beginning 30 seconds before 4 p.m. Trades made during the fix help determine the WM/Reuters currency exchange rates used as benchmarks by multinational corporations, money managers, and investors around the world to value contracts and assets.

As they check prices and complete deals, some traders participate in as many as 50 online chat rooms. Messages from salespeople and clients appear on their monitors, get pushed up by new ones, and vanish from view. Now regulators from Bern, Switzerland, to Washington are examining evidence that a small group of senior traders at big banks had something else on their screens: details of each other's client orders. Sharing that information may have helped dealers at JPMorgan Chase (JPM), Citigroup (C), UBS (UBS), Barclays (BCS), and others manipulate prices to maximize their profits, say five people with knowledge of the probes who asked not to be identified because the matter is pending.

At the center of the inquiries are instant-message groups with names such as The Cartel; The Bandits' Club; One Team, One Dream; and The Mafia, in which dealers exchanged information on client orders and agreed how to trade at the fix, according to the people familiar with the investigations.

Unlike sales of stocks and bonds, which are regulated by government agencies, spot foreign exchange trades—buying and selling for immediate delivery, not a future date—aren't considered investment products and aren't subject to specific rules. Traders are bound only by market abuse laws prohibiting trading on inside information and sharing confidential data about client orders with third parties. "This is a market where there is no law, and people have turned a blind eye," says Ted Kaufman, a former Democratic senator from Delaware, who sponsored legislation in 2010 to shrink the largest U.S. banks.

A lack of regulation has left the foreign exchange market vulnerable to abuse, according to Rosa Abrantes-Metz, a professor at New York University's Stern School of Business. "Since the gains from moving the benchmark are possibly very large, it is very tempting to engage in such a behavior," says Abrantes-Metz, whose 2008 paper *Libor Manipulation* about the London interbank offered rate helped spark a global probe of how that benchmark is set. "Even a little bit of difference in price can add up to big profits."

London is the world's biggest hub for currency trading, accounting for about 41 percent of all transactions, compared with 19 percent for New York and 6 percent for Singapore, according to a Bank for International Settlements survey. About $5.3 trillion changes hands globally every day, BIS

data show, as companies convert revenue into dollars, euros, or yen, and managers overseeing pensions and savings buy and sell stock around the world.

Spot currency trading is conducted in a small and close-knit community. Many of the more than a dozen traders and brokers interviewed for this story live near each other in villages dotting the Essex countryside, a short train ride from London's financial district. They stay in touch over dinner, on weekend excursions, or during rounds of golf. "This is a market that is far more amenable to collusive practices than it is to competitive practices," says Andre Spicer, a professor at the Cass Business School in London.

The data used to determine WM/Reuters rates for 160 currencies is collected and distributed by World Markets, a unit of State Street (STT), and Thomson Reuters (TRI). Bloomberg LP, the parent of *Bloomberg Businessweek*, competes with Thomson Reuters in providing news and information, as well as currency trading systems and pricing data. Bloomberg LP also distributes the WM/Reuters rates on Bloomberg terminals.

A story about possible exchange rate manipulation by Bloomberg News in June triggered internal probes as banks began reviewing millions of instant messages, e-mails, and transcripts of phone calls. The U.K.'s Financial Conduct Authority (FCA), the European Union, the Swiss Competition Commission, and the U.S. Department of Justice are investigating currency trading.

At least 12 foreign exchange traders have been suspended or put on leave by banks as a result of internal probes, and 11 firms have said they were contacted by authorities. Government-controlled Royal Bank of Scotland (RBS) turned over transcripts of instant messages. Deutsche Bank (DB) says it's cooperating with regulators, and UBS says it's taking unspecified disciplinary measures against employees. UBS, RBS, Citigroup, Deutsche Bank, JPMorgan, Goldman Sachs (GS), and Lloyds Banking Group (LYG) are banning traders from participating in chat rooms with employees of other banks, say people at the banks. None of the traders or their employers have been accused of wrongdoing.

One focus of the investigation is the relationship of three senior dealers who participated in The Cartel—JPMorgan's Richard Usher, Citigroup's Rohan Ramchandani, and Matt Gardiner, who worked at Barclays and then UBS—according to the people with knowledge of the probe. Some of the traders interviewed for this story say they eagerly sought entry to The Cartel's chat room because of the influence it exerted. Usher, Ramchandani, and Gardiner, along with at least two other dealers over the years, would discuss their customers' trades and agree on exactly when they planned to execute them to maximize their chances of influencing the fix, two of the people say.

Usher was the moderator of The Cartel, according to people with knowledge of the matter, who say the chat room died when he quit RBS in 2010. He revived the group with the same participants when he joined JPMorgan the same year as chief currency dealer in London, they say. Ramchandani is head of European spot trading at Citigroup. Gardiner joined Standard Chartered (STAN:LN) in London as assistant chief currency dealer. He previously worked at UBS in Zurich and was co-chief dealer with Chris Ashton at Barclays in London.

Usher, Ramchandani, and Gardiner were put on leave by their employers after the FCA opened its inquiry in October, according to people with knowledge of the matter. Ashton, now global head of spot trading at Barclays, has been suspended, along with five other spot traders at the bank in London and New York. Ashton and Ramchandani declined to comment. Gardiner didn't return messages left on his mobile phone. Usher couldn't be located, and JPMorgan declined to provide contact details for him.

Thomson Reuters says in an e-mail that it "would lend its expertise to support any authorities' investigation into alleged disruptive behavior on benchmarks." State Street says in an e-mail that "the WM/Reuters benchmark service is committed to reliability and robust operational standards. WM continually reviews recommended methodology and policies in order to ensure that industry best practices are considered."

The currency investigations are taking place as authorities grapple with a widening list of scandals involving the manipulation by banks of financial benchmark rates, including Libor and ISDAfix, used to determine the value of interest rate derivatives. "Some of these problems developed over many years without anybody speaking up," says Andrew Tyrie, chairman of Britain's Commission on Banking Standards and Parliament's Treasury Select Committee. "This is remarkable. It suggests something very wrong with the culture at these institutions."

The bottom line: *Authorities are investigating whether traders used chat rooms to rig rates in the $5.3 trillion foreign exchange market.*

Vaughan is a reporter for Bloomberg News in London.

US unveils world's 'largest' money laundering probe

Agence France-Presse
Posted at 05/29/2013 9:53 AM | Updated as of 05/29/2013 9:53 AM

NEW YORK- The United States on Tuesday unveiled the world's "largest" money laundering probe targeting the digital currency operator Liberty Reserve, striking a major blow against what a prosecutor termed the "Wild West" of virtual banking.

The Costa Rica-based entity, which handled huge amounts of money outside the control of national governments, is charged with running a "$6 billion money laundering scheme and operating an unlicensed money transmitting business," the US Attorney's office for New York said.

Prosecutors said Liberty Reserve processed at least 55 million illegal transactions for at least one million users "and facilitated global criminal conduct."

The probe involved law enforcement in 17 countries and "is believed to be the largest money laundering prosecution in history," the prosecutor's office said.

Liberty Reserve's principals were arrested Friday in a round-up launched simultaneously in Costa Rica, Spain and New York, sealing the fate of a company that had been one of the most successful in the popular but increasingly scrutinized world of unofficial banking and virtual currencies.

One of them, Russian citizen Maxim Chukharev, is set to be extradited to the United States, Costa Rican authorities said Tuesday.

The indictment accuses Liberty Reserve founder Arthur Budovsky -- a former US citizen who took Costa Rican nationality -- and his partners of creating a firm that masqueraded as a convenient and legitimate money transfer system.

In reality, the organization turned itself into the "financial hub of the cyber-crime world," the indictment said.

US Attorney Preet Bharara said "the only liberty that Liberty Reserve gave many of its users was the freedom to commit crime."

Customers would go to Liberty Reserve's now shut-down website to buy the online currency, known as LRs, that could then be used in transactions with other LR users.

The system was not registered with US authorities and unlike some other non-state currency systems did not require proof of identity for users.

Adding another important layer of anonymity, Liberty required customers to buy or sell their LRs via third party exchangers, meaning that there was no direct link between a customer's traditional bank account and Liberty's system.

An extra service would allow a user to hide "his own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system."

The system, the indictment says, was tailor-made for criminal transactions and money-laundering, facilitating "a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking."

"The scope of the defendants' unlawful conduct is staggering," the indictment said.

"With more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion."

Authorities say that when Liberty Reserve realized it was under investigation it made a show of shutting down, yet continued to operate behind an array of shell companies in Australia, China, Cyprus, Hong Kong, Morocco, Russia and Spain.

Budovsky and his partners started Liberty Reserve after an earlier similar venture, Gold Age Inc, which traded the E-Gold digital currency, was shut down by US authorities.

It was then that Budovsky, 39, emigrated to Costa Rica, later renouncing his US citizenship, and becoming resident in The Netherlands. He was arrested in Spain.

He and his four partners, who range in age from 27 to 46, face maximum prison terms of 20 years if found guilty of conspiracy to commit money laundering, as well as up to 10 years on charges related to running an unlicensed money transmitting business.

Chukarev was described as being co-responsible for Liberty Reserve's technical infrastructure.

Virtual currencies have grown exponentially, but face pressure on numerous fronts. The popular Bitcoin system has come under scrutiny by financial authorities and seen growing trading volatility.

Acting Assistant Attorney General Mythili Raman said the United States had used "every tool we have" to combat "global illicit finances."

As Bharara put it, "the global enforcement action we announce today is an important step towards reining in the 'Wild West' of illicit Internet banking."

"As crime goes increasingly global, the long arm of the law has to get even longer, and in this case, it encircled the earth," he added.

THE CANADIAN PRESS

Fears of financing terror closes another money transfer outlet for overseas Somalis; Terror financing fears stop transfers to Somalia

Canadian Press
Tue Jun 25 2013
Section: Business
Byline: Abdi Guled And Jason Straziuso

MOGADISHU, Somalia - When a bank transfers **money** to Somalia, can it be sure it's not sending **money** to **terrorists**? That question is forcing one of Britain's largest banks to cut ties with the largest cash **transfer** bank in Somalia, a company that brings in the majority of the country's $1.2 billion in yearly remittances.

Many in Somalia are in desperate need of **money**. Payments from family and friends overseas are how many get by, and that's why more than 100 aid workers and Somalia experts signed a letter this week pleading with the British government to find a solution.

Barclays bank will no longer allow customers to send **money** to Somalia via the Somali bank Dahabshil. A financial power-house in Somalia, Dahabshil describes itself as "the most trusted **money transfer** company for many immigrants willing to support their families and friends." But anti-terror laws hold banks - like Barclays - responsible if they **transfer money** to criminal or terror elements. As a result, fewer are willing to send **money** into Somalia.

Such transactions for Somalis in the United States became more difficult in late 2011, when a bank in Minnesota closed accounts that facilitated such transfers. Sunrise Community Banks decided to halt the transactions after two women were convicted of sending **money** to the **terrorist** group al-Shabab.

"It is recognized that some **money** service businesses don't have the proper checks in place to spot criminal activity and could therefore unwittingly be facilitating **money laundering** and **terrorist** financing," Barclays said in a statement. "We want to be confident that our customers can filter out those transactions, because abuse of their services can have significant negative consequences for society and for us as their bank."

Dahabshil did not immediately respond to a request for comment. The company's website says that customers "must provide government authorized identification and personal information for anti-**money laundering** compliance if amounts reach certain limits."

The group of aid workers and researchers said the decision at stake here "is a lifeline that provides essential support to an estimated 40 per cent of the population of Somalia." The group said it has seen firsthand the impact remittances have on families in the Horn of Africa.

"My son is in the U.K. He sent us **money** every month for our sustenance and school fees for the children. Where are we going to get the **money** to pay our bills?" said Dahabo Afrah, a longtime customer of Dahabshil in Mogadishu. "This is unfair to us and will affect hundreds of thousands of Somali people."

Many big banks in the U.S. have already stopped handling transfers to Somalia, saying the federal requirements designed to crack down on **terrorism** financing were too complex and not worth the risk. Last April, U.S. Bank confirmed it is working with Dahabshil to allow Somalis in Minnesota to send **money** back home. U.S. Bank spokeswoman Teri Charest said Monday that the bank is working closely with Dahabshil but the transactions have not yet started.

Barclays said it remains happy to maintain a relationship with businesses that have anti-financial crime controls. Western Union operates in Somalia but does not have a presence in many places, including Mogadishu, the capital.

The aid groups said that one study of financial transactions in Somalia found that 73 per cent of remittance recipients said that they use the **money** they receive from relatives - an average of $2,040 per year - to pay for basic food, education, and medical expenses.

"One-third of recipients said that they would not be able to afford basic food if the remittances were stopped," the group said in a letter to the British government on Monday.

The group is calling on the British government to help **money transfer** businesses to find alternative banking partners. It also asked that Barclays extend its termination deadline for six months until other solutions are found.

A study released earlier this month by the Food Security Nutrition Analysis Unit for Somalia, a project by the United Nations' Food and Agriculture Organization found yearly remittances to Somalia to be a minimum of $1.2 billion per year. The aid group Oxfam said that soon to be published research shows that Somali immigrants in the U.K. send more than $154 million back to Somalia each year, behind only the U.S.

Straziuso reported from Nairobi, Kenya. Associated Press reporter Amy Forliti in Minneapolis, Minnesota contributed to this report.

ABC

Police investigate a money transfer service after allegations of theft

275 words
12 December 2013
Australian Broadcasting Corporation (ABC) News
ABCNEW
English

The WA Police Major Fraud Squad is investigating a **money transfer** service over allegations they stole hundreds of thousands of dollars from customers.

The WA Police Major Fraud Squad is investigating the owners of a Girrawheen video shop over allegations they stole hundreds of thousands of dollars from customers.

The video shop doubles as a **money transfer** service, which is used by many in the Vietnamese community to wire funds overseas.

Clients of the service have been sending money back to **Vietnam** to repay student loans or to help relatives who are undergoing urgent medical procedures.

At least one alleged victim has lost nearly $70,000.

Detective Senior Sergeant Dom Blackshaw from the Major Fraud Squad says it is alleged the money is being siphoned off.

"We've had a number of complainants come forward and we've identified hundreds of thousands of dollars of funds that have not arrived at their intended destination and of course it is a investigation into the alleged theft of those funds," he said.

Local MP Margaret Quirk's electorate office has been flooded with complaints.

She says many of the alleged victims are anxious about what has happened to their money.

"The Vietnamese community is a very hard-working diligent community, they've earned that money the hard way and they are pretty concerned that it appears to have gone for good," she said.

Detectives recently raided the premises and seized documents and cash.

Police say the proprietors of the store are assisting them with their inquiries.

Investigators believe there may be more victims yet to come forward.

News

Funding terrorism: Illegal cash flows may be aiding terrorists

Staff Reporter

318 words
6 January 2014
The Financial Daily
PMFIND
English

KARACHI: **Terrorist** groups in the Federally Administered Tribal Areas (Fata) and Balochistan have been receiving billions of rupees each month through banking channels and money exchange companies, sources in Federal Investigation Agency (FIA) have revealed.

These companies in collusion with some bankers have been transferring huge amounts to unnamed bank accounts in Quetta and Peshawar. The FIA has recently found evidence of transfer of billions of rupees to the two cities in the last few months.

According to sources, the FIA made these discoveries during its investigations into the multibillion rupee Trade Development Authority Pakistan (TDAP) scam.

Ironically, the Financial Monitoring Unit (FMU) and other institutions, whose task is to curb the illegal business of hundi and hawala, are completely unaware of these dubious transactions, made right under their nose.

If the law enforcers can trace the people receiving billions of rupees through unnamed accounts in Peshawar and Quetta, they will possibly be able to unearth **terrorist** activities funded by this money.

Sources said that after these startling facts, FIA officials were busy uncovering the huge illegal business of **money transfer**. After discovering evidence of transfer of Rs1billion to Peshawar and Quetta in the last few months, the FIA has registered nine cases under the Anti-Money Laundering Act and arrested dozens of officials of private banks.

According to sources, a renowned money exchange company has transferred around Rs34billion to Quetta and Peshawar in the last few months through its unnamed accounts. Interestingly, money exchange companies and banks have no information about the senders and receivers of the money.

The FIA has frozen dozens of unnamed accounts in Quetta and Peshawar and issued written notices to their holders. However, as the details submitted for opening the accounts have proven to be incorrect, the FIA has started trying to look for their possible link to **terrorist** activities.

THE AUSTRALIAN
Australia's national daily newspaper

Finance

Money agency fined for laundering

ANTHONY KLAN, REGULATION

275 words
18 December 2013
The Australian
AUSTLN
1 - All-round Country
19
English

THE federal government has fined Ria Financial Services -- one of the world's biggest **money transfer** agencies -- more than $225,000 over 26 alleged breaches of anti-money laundering and counter-**terrorism** finance laws.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) said Ria Financial Services had operated unregistered Australian affiliates and had transferred money via those unregistered arms.

``The money remittance sector is recognised internationally as being particularly vulnerable to exploitation by criminals," AUSTRAC chief executive John Schmidt said yesterday.

He said the AUSTRAC required remittance, or **money transfer**, companies to be registered with the federal government, and that those laws had been in place for more than two years.

``The (registration) scheme was established to ensure that remittance service providers implement the necessary measures to identify, manage and mitigate money laundering and other risks," Mr Schmidt said.

``Money laundering points to other crimes that the Australian community does not tolerate, including fraud, people-smuggling, tax evasion and **terrorism** fighting.

``The industry should be on notice that we are supervising your behaviour and we will take action."

A spokesman for the Australian arm of Ria Financial Services declined to comment when contacted by The Australian yesterday.

The company had paid the $225,600 fine, AUSTRAC said.

Rita has 650 affiliates in Australia and is part of a global network of about 207,000 agents worldwide across 135 countries.

On November 1, 2011, it became mandatory for all businesses bound by the federal government's Anti-Money Laundering and Counter-**Terrorism** Financing Act 2006 to be enrolled on AUSTRAC's ``reporting entities roll", the agency said.

Italy money laundering probe swoops on 21 cash transfer bureaux

MILAN | Wed Oct 31, 2012 8:57am EDT

Oct 31 (Reuters) - Italian police have sequestered 21 money transfer bureaux as part of an investigation into a scheme to launder billions of euros from drugs and people trafficking.

The tax police said on Tuesday they had sifted through 30 million money transfer operations carried out in 2010-2011 through 11 of Italy's major payment agencies, with an overall value of 10 billion euros ($13 billion).

The probe, which started in the northern Italian city of Brescia, showed that 35 percent of the operations were for money laundering.

Police said they had found "a mechanism used extensively to let money of doubtful origin circulate", and that they were looking at possible failures by the agencies to prevent money laundering. ($1 = 0.7705 euros) (Reporting By Danilo Masoni; Editing by Robin Pomeroy)

THE VANCOUVER SUN

2 face charges of money laundering; Langley men operated two currency exchanges

Vancouver Sun
Sat Jun 27 2009
Page: A14
Section: Westcoast News
Byline: Gerry Bellett
Source: Vancouver Sun; with files from the Langley Advance

The operators of two Langley currency exchanges, Robinderpal Rathor, 30, and his cousin, Taranjit Rathor, 21, are facing several counts of money **laundering** and conspiracy to commit money **laundering** following a two-year investigation by the RCMP's Federal Integrated Proceeds of Crime Unit.

The pair will be in court July 15.

According to RCMP Sgt. David Gray, the investigation began in 2007 with investigators targeting Global Tourist Centre Currency Exchange and Capital **Forex** on suspicion that they were being used to launder proceeds of crime money.

On March 10, both men were charged after a total of $160,000 US was seized by police during the investigation. Undercover officers had infiltrated the businesses and successfully laundered $21,300 Canadian and more than $550,000 US, Gray said.

RCMP Insp. Wade Lymburner, who is in charge of the proceeds of crime unit, said money **laundering** was usually linked to drug trafficking. "People who knowingly participate in money **laundering** by turning a blind eye and not asking the right question on where the money is coming from, are contributing to help put profits into pockets of drug traffickers," said Lymburner, adding businesses owners should question the source of money before incorporating it into their own businesses.

Meanwhile, the unit has launched its annual Merchants Against Money **Laundering** awareness campaign. UBC students will give presentations to businesses about money **laundering** and how it negatively impacts communities.

infomart

THE TIMES OF INDIA

Raids on hawala trader expose Rs 400-crore deals [Chandigarh]

The Times of India
Mon Feb 4 2013
Section: News
Byline: Singh, I P

JALANDHAR: After the enforcement directorate unearthed a major hawala racket following raids on two operators - one in Jalandhar and the other in Ludhiana – on Saturday, several exporters are also reportedly coming under the scanner for shady transactions through hawala channels.

Sources revealed that the value of transactions through the Jalandhar-based operator – Happy Forex Pvt. Ltd -- is pegged at above Rs 400 crore in the preliminary estimates by directorate officials, who continued raids till late night at the premises of the money exchanger in Adda Hoshiarpur locality. According to sources, hawala operator Jiwan Kumar was into the trade for the last around two decades. He was a small courier for bigger operators earlier, but later grew to be very big in the business. It is learned that he had also developed proximity with some police officials.

He was the biggest hawala operator not just in Punjab, but in the entire north of Delhi region.

As ED has recovered several incriminating documents from the raided premises, it is emerging that several business houses were using this route for money **laundering**. "Land mafia is also involved in the transactions and the route was being used for turning black money into white by sending money abroad and then getting it back as payments for exports - which were being made at exorbitant prices," sources said.

Meanwhile, industry sources revealed that after netting Jiwan Kumar, fear has spread among industry and exporter circles, who were using the network, as they now fear that their modus operandi would be exposed and they would also face action.

Enquiries revealed that a hawala operator based in Ludhiana was doing business under the garb of jewellery exports. "Jalandhar and Ludhiana based operators were having a symbiotic relationship and were using each other in making transactions," they said.

The countries where the hawala network had connections included Dubai, UK and **Canada**.

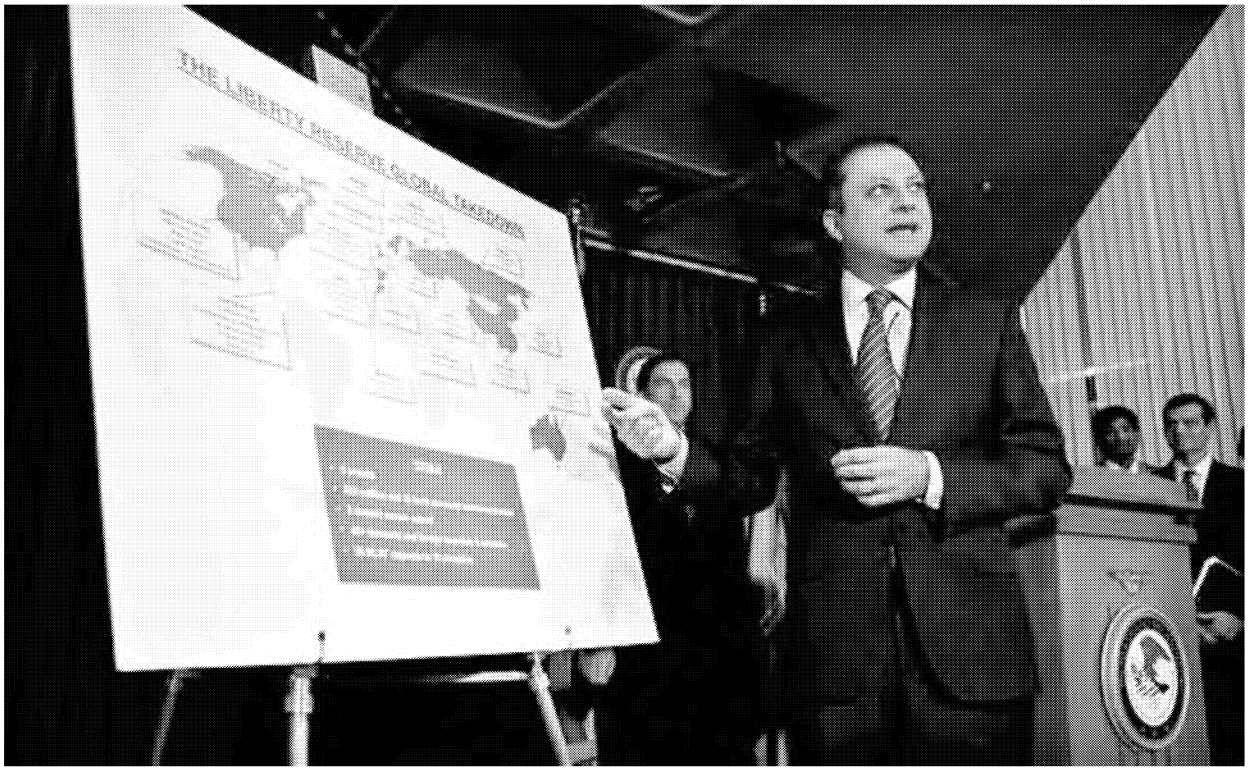
ED had also recovered Rs 1.15 crore cash from the operator's office. "He was doing hawala business under the garb of running a **foreign exchange** outlet. He was into the illegal trade even before getting a license for **foreign exchange** business and with time, he grew to be a big hawala operator, from being a small time fruit/vegetable vendor," said a man, who has been watching the operator's rise over time.

Man booked

Police have registered a case of theft, obstructing officials in discharging duty, criminal intimidation against one Gopi who had tried to run away with a bag carrying cash when enforcement directorate officials had raided a money exchange office at Adda Hoshiarpur in Jalandhar. While initially some police officials had claimed that the fellow was nabbed by them, on Saturday police said that he had managed to escape in the crowd even as they could pick the bag which fell down when they chased him. A senior police official said the bag had around Rs 30 lakhs. A case against Gopi was registered on the complaint of ED's assistant director Alok Kumar.

WHY DID CRIMINALS TRUST LIBERTY RESERVE?

POSTED BY JAMES SUROWIECKI



Liberty Reserve, the alternative-payment network and digital currency that federal prosecutors shut down a couple of days ago, was not, as it described itself, the Internet's "largest payment processor and money transfer system." (PayPal, obviously, is much bigger.) But Liberty Reserve was, by all accounts, the Internet's largest payment processor for illicit and criminal transactions. The Justice Department says that since the founding of Liberty Reserve, in 2006, it has handled more than fifty-five million transactions totalling more than six billion dollars, and as of last year it had more than a million users. In effect, Liberty Reserve provided a key piece of the infrastructure for criminal activity on the Web. What makes it so interesting is that it was only able to do so by getting hundreds of thousands of criminals to trust it.

Descriptions in reports of the legal action against Liberty Reserve have made its day-to-day business sound enormously confusing. So let's walk through how it worked. Liberty Reserve functioned like a bank that only took deposits in its own currency (also called the Liberty Reserve). If you wanted to launder money, you would open an account with Liberty Reserve, providing them with a name, which could be fake, and an e-mail address. The key to the scheme was that you couldn't then deposit money directly into the account. Instead, you had to work through middlemen, who were called "exchangers." These were typically unlicensed moneymen

in countries like Malaysia, Nigeria, and Vietnam, who bought Liberty Reserves in bulk from Liberty Reserve. You would pay them dollars (or whatever currency) for a certain sum of Liberty Reserves, which they would then deposit into your account. And when you wanted to withdraw money, the process worked in reverse, perhaps with an exchanger in a different country. (Liberty Reserve itself took a one-per-cent fee on transactions, while the exchangers typically charged five per cent or more.) The point of doing it this way was that the Liberty Reserve bank would have no identifying data for you (no record of how or from where you sent the money), since the deposits and withdrawals were all done through the exchangers.

This arrangement made money laundering easier, which seems to have been the main function of the network. But Liberty Reserves were also used as a digital currency, in the sense that that there were "merchants" who would accept L.R.s as a form of payment for goods and services. (Liberty Reserve actually designed a shopping-cart interface for their Web sites.) These merchants were, at least according to the government, "overwhelmingly criminal in nature," engaging in transactions in which both the buyer and the seller had an interest in anonymity. They included traffickers in stolen credit-card and social-security numbers, drug dealers, and hackers. If you wanted to pay for someone to hack a company's data, you could just transfer L.R.s from your bank account to theirs. What Liberty Reserve offered criminals, in other words, was something that had, relatively speaking, the anonymity of cash (since all that identified you was an e-mail address) in the virtual world.

What's fascinating about all this is that, at least for a while, it worked—drug dealers were willing to trade real drugs and hackers were willing to do real work in exchange for Liberty Reserves. That suggests they were confident that the currency wouldn't become worthless, and that when they wanted to trade their Liberty Reserves for dollars (or euros), they'd be able to do so with reasonable ease and at a reasonable price. This is a little surprising. It makes sense to accept dollars for your work, because you can be certain you'll be able to use them to buy stuff tomorrow—the fact that they're the legal currency of the U.S. is a good guarantee of that. But Liberty Reserves were backed by nothing at all. They were historically pegged to the U.S. dollar —one L.R. equaled one dollar—but there were no legally binding rules that guaranteed that exchange rate (the whole point of the system was that it was outside the law), which means that Liberty Reserve could, in theory, have raised or lowered the rate at will. More important, there were no restrictions that would have prevented Arthur Budovsky (who founded Liberty Reserve) from simply printing as much currency as he wanted and using it to buy illicit goods. (This makes it different from Bitcoin, which has been algorithmically engineered to permanently limit the number of bitcoins in existence.) Had Budovsky done this, it would have radically devalued the wealth that everyone else had in Liberty Reserves. Yet, even knowing that,

hundreds of thousands of people, many of whom broke the law for a living, put their faith in the system.

The reason they were willing to do so, presumably, was that the long-term value of Liberty Reserve as a business depended on it not screwing over its customers. Like good disciples of Adam Smith, Liberty Reserve's users relied not on Budovsky's benevolence but, rather, on his pursuit of his own self-interest. This was a good gamble for a while, but there was an important catch: because Budovsky couldn't protect Liberty Reserve from the U.S. government, all of those L.R.s are now essentially worthless. Still, Liberty Reserve's success (short-lived as it was) is a kind of testament, however perverse, to the fact that markets can flourish even when there is no government to supervise them, and no legal way to enforce the rules. When self-interest is well-harnessed, apparently, you get honor even among thieves.

Appendix 10

European Parliamentary Research Service – *Understanding Money Laundering Through Real Estate Transactions*

European Parliament

Understanding money laundering through real estate transactions

SUMMARY

Money laundering through real estate transactions integrates black funds into the legal economy while providing a safe investment. It allows criminals to enjoy assets and derived funds having camouflaged the origin of the money used for payment.

A number of techniques are used, namely cash or opaque financing schemes, overvalued or undervalued prices, and non-transparent companies and trusts or third parties that act as legal owners. Among the possible indicators are geographical features (such as the distance between the property and the buyer and their actual geographical centre of interest). In order to assess the existence of a money-laundering risk, concrete assessments of transactions and a customer's situation provide indications that help raise red flags and trigger reporting obligations.

The anti-money-laundering recommendations set out by the international Financial Action Task Force (FAFT) are implemented in the European Union (EU) by means of coordinated provisions (chiefly the Anti-money-laundering Directive). Customer due diligence and reporting of suspicious transactions are tools to address money laundering. Real estate transactions involve both non-financial and financial sector parties operating under different legal requirements. Yet, reporting of suspicious transactions in real estate is limited, leaving ample room for improvement.

Improvement is all the more necessary inasmuch as money laundering in general, and in the real estate sector in particular, has a major socio-economic impact, the magnitude of which is difficult to quantify. Awareness is however growing as a result not least of high profile examples of money laundering through real estate in a number of EU cities.

In this Briefing

EPRS | European Parliamentary Research Service

Author: Cécile Remeur
Members' Research Service
PE 633.154 – February 2019

Real estate: a haven for money launderers?

Abuse of the real estate sector (property in the form of land or buildings) has long been described as one of the oldest known ways to launder ill-gotten gains. Real estate is as attractive to criminals as it is to any investor (prices being generally stable and likely to appreciate over time) and is also functional (the property can be used as a second home or rented out, generating income). Real estate also provides a veneer of respectability, legitimacy and normality. This applies to both residential and commercial properties as part of a reliable and profitable investment strategy.

Real estate transactions can involve large sums and are subject to more limited scrutiny with regard to money-laundering risks than financial sector transactions, as non-financial sector rules are much more limited.[1]

Some illustrative snapshots

This is a worldwide phenomenon,[2] with plentiful examples from Canada, the United States, Australia and New Zealand to the European Union, Africa, Asia and Middle East.[3] The transactions used for money laundering mainly concern houses and buildings, but any form of immovable property can be used to this end, for instance vineyards.

Some textbook cases, such as those for instance in Vancouver[4] or London, highlight striking features such as:

- discrepancy between the usual income and wealth of the owner and the property: in some cases, the most expensive properties in the city are owned by individuals with no income or wealth that would allow them to purchase such a property;
- an anonymous owner, as a result of recourse either to a third party or to companies, trusts or similar arrangements;
- a property's underestimated or overvalued price;
- the indication by a country that there is a risk of money laundering by its citizens in another country.[5]

Real estate in the money laundering cycle

Money laundering is the process used to camouflage the illegal origin of funds generated by illicit or criminal activities. By successfully laundering the proceeds of criminal activities, the illicit gains can be enjoyed without fear of their being confiscated. In real estate, money laundering involves using such funds to pay for the transaction (predicate offence of money laundering). Real estate plays a role (mainly) in the third and final stage of the money-laundering cycle, after the placement and the layering phases.

Placement consists of moving funds directly associated with a crime and introducing them into the financial system (e.g. breaking up large amounts into small deposits or purchasing financial instruments such as money orders). **Layering** is then designed to hide the trail and hinder pursuit by distancing the illegal proceeds from the source of the funds, using layers of financial transactions.

Purchasing real property is one way to **integrate** black money into the legal economy, while also returning the illegally derived proceeds to the criminals concerned. In addition, when sold or rented, real property provides what appears to be a legitimate source of income.

Addressing the misuse of real estate for money laundering

Identifying the misuse of real estate to launder money

Reports based on surveys provide for a typology of the basic techniques used for laundering money through the real estate sector. The Organisation for Economic Co-operation and Development (OECD) published two in two consecutive years: the 2007 FATF report 'Money laundering and

terrorist financing through the real estate sector' and the 2008 OECD report 'Real estate sector: Tax fraud and money laundering vulnerabilities'.[6]

Examples of real estate money laundering display some or all of the following features:

- complex loans or credit finance (used as a cover for laundering money, their repayment can be used to mix illicit and legitimate funds, black and legal money);
- non-financial professionals;
- corporate vehicles;
- manipulation of the appraisal or valuation of a property (undervaluation, overvaluation and successive sales at higher values);
- monetary instruments;
- mortgage schemes;
- investment schemes and financial institutions.

To complement this typology, other features can serve as specific indicators of real estate money laundering, such as:

- recourse to third parties by customers (sellers and buyer) for concealment of ownership;
- unusual income (e.g. no income, or inconsistency between income and standard of living), unusual rise in financial means, unusual possession or use of assets, or unusual debt (e.g. mortgage with low income or unidentified lender) on the part of the legal owner;
- use of front companies, shell companies, trusts and company structures, allowing the criminal not to appear as the real owner;
- rental income to legitimise illicit funds (either with rental funds provided by the criminals for the tenants to legitimise illicit funds, or renting the property to a third party they use as the legal owner);
- property renovations and improvements using illicit funds that increase the value of the property, which is then sold at a higher price;
- consideration of geographical elements.

In short, these techniques and indicators highlight the **unusual nature** of the transaction compared with a normal situation, pointing to a possible suspicious transaction.

Mitigating risks and detecting suspicious transactions

The challenge is to spot the money laundering behind the real estate transaction. Possible indicators of money laundering (red flags) help risk-based assessment. Guidance has been established as a tool for the sector at both global and national levels. Professional representative bodies have also developed implementing tools.

The process demands familiarity with the normal conduct of business so as to be able to identify unusual or suspicious patterns relating to customer risk, transaction risk or geographical risk (these are sometimes clustered in pairs, geographical aspects being added to the first two risk types). A number of questions need to be asked before, depending on the answer, the transaction can be found to be suspicious and reporting obligations triggered.

Customer risk relates primarily to the buyer, but concerns may broaden to include the seller and any other persons intervening in the transaction. The ability to identify the real purchaser and ascertain whether involvement of third parties or a corporation obscures the owner's identity (without a legitimate business explanation) is central to ascertaining customer risk.

Customer risk also covers purchases involving high-ranking foreign officials or their families, who require specific attention either as politically exposed persons (PEPs) or because of specific international provisions, such as sanctions.

The **transaction risk** relates to a variety of elements regarding for instance the type of property, successive transactions, under- or overvaluation, mismatch between buyer and property, and financing risks relating to the source of funds, use of cash or use of complex loans. Concerns can be aroused as a result for example of a lack of interest in obtaining a better price, or a buyer purchasing property without viewing it, or with no visible interest in its characteristics. In short, this relates to the concern that the transaction does not appear to make professional or commercial sense.

Geographical risk can relate to both the property and the buyer. The first question is whether the location of the property matches the location of the buyer and the seller. Then the question arises as to whether they are located in a jurisdiction with weak anti-money-laundering regimes, that supports or funds terrorism or that displays a high degree of corruption. The same questions apply to the origin of the funds.

Another scrutiny-raising factor can be a large unexplained geographical distance between the location of the property and that of the buyer.

Tackling the problem: a work in progress

Anti-money-laundering framework and real estate

Some of the features and concepts that are relevant to understanding the anti-money-laundering (AML) framework in relation to real estate are set out below.

Anti-money-laundering framework

The FATF is an intergovernmental body whose objective is to set standards for the development and promotion of national and international policies to combat money laundering and terrorist financing. Its recommendations increase transparency and enable countries to take successful action against the illicit use of their financial systems. FAFT recommendations are intended to be implemented in countries' legal texts. The recommendations were last updated in 2012.

In the European Union, the first anti-money-laundering framework dates back to the 1990s. It has been revised constantly in order to mitigate risks relating to money laundering and terrorist financing. It encompasses: Directive (EU) 2015/849 of 20 May 2015 on preventing the use of the financial system for money laundering or terrorist financing (the fourth AML directive) – as amended by Directive (EU) 2018/843 of 30 May 2018[7] – and Regulation (EU) 2015/847 on information accompanying transfers of funds, which makes fund transfers more transparent, thereby helping law enforcement authorities to track down terrorists and criminals. The EU's money laundering rules set minimum requirements, leaving Member States free to impose stricter requirements if they consider it necessary to do so according to the risk.

Geographically targeted approach

As the use of real estate for laundering money is concentrated in a number of geographical areas, targeted questions can generate matches. This is the case in the US where real estate geographic targeting orders (GTOs) made in 2016 and renewed in 2018 have been issued by the US Financial Crimes Enforcement Network (FINCEN) for a number of geographical locations, with varied monetary thresholds for each area. Some of these require the identification of the natural persons behind companies used to pay all cash for luxury residential real properties.

This looks like a well-targeted tool, but a geographically targeted tool bears the risk of the phenomenon moving to other areas beyond its reach.

Real estate gatekeepers and the risk-based approach

Two FATF documents, the report on Money laundering and terrorist financing through the real estate sector and the Guidance on the risk-based approach for real estate agents, issued in 2007 and 2008 respectively, address the real estate sector's vulnerability to money laundering.

Gatekeepers in real estate transactions are a wide range of professionals governed by different regulations and anti-money-laundering obligations, who to varying extents have an obligation to assess risks and, if need be, report them.

In updated Recommendation 22, the real estate sector belongs to the designated non-financial businesses and professions (DNFBP) category. DNFBPs are required to run customer due diligence checks based on risk assessment and record-keeping requirements. This includes real estate agents involved in transactions for their clients concerning the buying and selling of real estate and also lawyers when preparing or carrying out such transactions for their clients. To this end, guidance can help gatekeepers to identify risks and implement obligations. Among the gatekeepers, the financial sector also has a role to play when it is involved in the transaction. This role is important but should not be over-relied upon, as not all transactions pass through a financial sector intermediary, especially in the case of cash transactions. The legal professions have a particular role to play, as they sometimes provide advice on structures and contracts relating to transactions and can be involved in conveyancing.

In order to apply a **risk-based approach** to detecting and if need be reporting suspicious transactions, there is a need to ascertain the true identity of each customer by running a customer due diligence (CDD) / know your customer process (i.e. identifying and verifying the identity of clients, monitoring transactions and reporting suspicious transactions).

This spans from the simple identification and verification of the identity of clients (in the case of real estate transactions, the vendor, the purchaser and any other parties involved) to the more complex identification of the beneficial owner. Identifying the beneficial owner,[8] who may be shielded either behind a third party acting as legal owner or behind a corporate vehicle, such as a company (a shell company for instance), a trust or a similar vehicle.

Suspicious transaction reporting (STR) must take place when there is suspicion or reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing. Financial institutions are obliged to report, and the non-financial sector has the same or a similar obligation in a series of transactions defined in the recommendations.

Still a lot to be done?

A number of shortcomings in anti-money-laundering practices have been identified.[9] A 2017 European Commission report on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities[10] puts forward recommendations (that predate the adoption of the fifth AML directive and implementation of the provisions of the fourth AML directive). The report takes stock of the fact that 'the real estate sector is also exposed to significant [money laundering] risks, due to the variety of professionals involved in real estate transactions (real estate agents, credit institutions, notaries and lawyers)'.

With this in mind, a number of critical assessments have been made by specialised NGOs, starting with Transparency International, whose recommendations[11] call for an overhaul of money-laundering measures on a global scale and for proper enforcement. The recommendations are based on the following essential elements:

Ability to **identify the owner of the real estate**:

- introducing public beneficial ownership transparency for companies owning properties in a Member State and inserting some (minimum) requirements and

checks on foreign companies prior to having access to the real estate market, so as to tackle money laundering risks;
- ensuring identification of the beneficial owners of legal entities, trusts and other legal arrangements; and
- introducing a geographically comprehensive public register of beneficial ownership (overseas territories and specific status territories such as the United Kingdom Crown Dependencies);

Coverage of **all professionals involved** in real estate transactions:

- ensuring 'fit and proper' tests for professionals engaging in real estate transactions, and proper and consistent supervision of professionals involved in real estate with regard to money-laundering risks, as well as enforcement of the rules;
- addressing globally the inadequate coverage of anti-money-laundering provisions, extending due diligence requirements to the full range of non-financial professionals and businesses that might be involved in the buying and selling of real estate;
- ensuring sanctions in case of non-compliance, and sanctions for involvement in money laundering schemes;

Proper implementation of anti-money-laundering requirements **(preventing getaways)**:

- ensuring that due diligence checks are undertaken, either by financial institutions or by the non-financial sector when financial institutions are not involved (problem of cash transactions going unnoticed). This involves lawyers and real estate professionals in particular;
- ensuring submission of suspicious transaction reports (STRs) globally where there are reasonable grounds to suspect that the transaction is related to money laundering;
- conducting adequate checks on politically exposed persons and their associates, including national PEPs;

Reaction to cases of properties bought with laundered money:

- strengthening enforcement action (starting with the proceeds of corruption), using existing tools such as unexplained wealth orders and national equivalent provisions;
- ensuring a rapid reaction to trace stolen assets.

The recommendations also call for adequate resources for the authorities responsible for tackling money laundering and corruption.

Real estate money-laundering impact

Money-laundering impact on the legal economy

As with any non-recorded phenomena, an assessment of the scope of money laundering can only yield estimated amounts. There are limited reliable sources. Data on illicit financial flows[12] and money laundering are made available by the World Bank,[13] the OECD and the United Nations Office on Drugs and Crime (UNODC). There are some estimates on geographical areas that provide for some quantitative assessment. The 2011 UNODC report estimating illicit financial flows indicated that money laundered globally in one year could represent between 2 % and 5 % of global gross domestic product (GDP).[14] Although these figures vary, even the lower estimate underlines the significance of the problem.

As regards the quantification of tax fraud and money-laundering risks associated with the real estate sector, the 2008 OECD report Real estate sector: Tax fraud and money laundering vulnerabilities, based on a 2006 survey covering 18 countries, reported that none of the countries had reported official figures or statistics.

Another indication of the scale of money laundering via real estate is the share of real estate in criminal assets confiscated, which was estimated at 30 % between 2011 and 2013. Some studies have shown that real estate is considered a safe investment by criminals when it comes to laundering money.

The socio-economic effects of criminal financial flows on the legal economy and society are enormous. They cover the following elements: distortions in resource allocation from high-yielding investments to investments that run a low risk of detection, distortion of prices, notably in the real estate sector, unfair competition, risks of supplanting licit activities, negative impact on direct foreign investment, corruption, risks of real sector volatility, and strengthening of skewed income.

Trickle-down effect on real estate

Distortions of real estate prices and the concentration on limited sectors may have an impact beyond those areas and lead to increases in real estate prices, thus pricing people with legal sources of funds out of the market. Driving up the prices of real estate reduces housing affordability, something that has been witnessed in several cities in both developed and developing countries. This impacts not only those people rendered unable to purchase housing but also renters. In both cases, this can affect decisions about where to live, among other factors, resulting in a change of neighbourhood and the related displacement of less affluent households. Data on house prices are available for the EU (Eurostat data).

The contribution of foreign real estate investment to the growth in house prices is visible for a number of locations in the world. Upward and downward house price fluctuations and a shortage of affordable housing and offices can foster opportunities for foreign investment. Yet this does not necessarily correlate with money laundering. As for the impact of money laundering on real estate, there may be suspicions but there are no data. Indicators are found in high prices including payment in excess of value (not as such an indicator of money laundering but clearly one of luxury home prices and industry-pleasing).

Impact in the European Union

Examples are provided below for several EU Member States on the basis of publicly available information (press and reports when they exist). Some countries' situations are more often reported in the press and documented in specialised reporting. Yet as such, this is not an indicator of the greater scale of the problem in those countries, and conversely when no coverage or report is available, this does not indicate that the country is immune from such practices or from vulnerabilities to money laundering in the real estate sector.

In the **Czech Republic**, there have been reports in the press of cases of the existence of money laundering in real estate as well as the large number of properties bought by foreigners, with a high proportion from the same country.

The same goes for **France** where there are cases of money laundering through real estate, with undervaluation of real estate prices, recourse to opaque ownership, and opaque financing schemes, all typical of money laundering.[15] The press has reported the limited number of suspicious transactions reported, and the marginal improvement in real estate professionals' contribution to the fight against money laundering though real estate. There have also been several press reports that the phenomenon is not limited to luxury properties, but includes other immovable properties, such as vineyards.

In an investigation launched in September 2015 by the French public prosecutor's office and coordinated by Eurojust and Europol, a vast and complex money-laundering network in six Member States (Denmark, Germany, Estonia, Spain, Latvia and Lithuania) and in offshore financial centres outside Europe (Hong Kong and Singapore) included a number of real estate properties bought with the laundered proceeds of illegal activity.

In **Finland**, a €3.5 million money-laundering case was reported concerning island purchases in the south-west archipelago of Finland and under investigation.

Growing concern in **Germany** was reported in 2018, with a particular focus on Berlin, where prices are fast increasing, causing concern for renters and potential buyers. This triggered consideration of the idea of locking out foreign investors from Berlin real estate. There are a number of articles reporting a link with illicit money and seizures of related properties, and cases reported and investigated by the German financial investigation unit (FIU). The number of suspicious transactions reported by real estate agents is also limited. Real estate had already been identified as one of a number of individual economic sectors carrying money-laundering risks. A recent report on real estate money-laundering vulnerability provides an assessment of the magnitude of foreign money of unclear origin laundered into German real estate in 2017 (about €30 billion) and a description of the phenomenon.

Cases have also been reported by the press regarding **Greece**, while other specific features of the Greek real estate market show real estate prices can outweigh those outlined in the contract prices. A study considered the housing sector as well as the professions involved as being at high risk of money laundering. Golden visas also have a real estate impact, yet as such they are not linked to money laundering. Some cases have been investigated in the context of residence permission in an EU country.

In the **Netherlands**, a study Estimating money laundering risks shows that risks exist in real estate, with few concrete examples being reported. There are reported cases relating to organised crime and massive investment in new or planned residential housing projects, as well as in restaurants, through the use of private non-bank loans. In one older case, a real estate agency acting as a money 'laundromat' was prosecuted (for laundering money of criminal origin on behalf of dozens of its customers). Special attention to the growing influence of organised crime in the property market, in particular its grip on property formally owned by non-profit organisations and/or associations, has also been reported in the context of the seizure of illegally obtained assets.

In **Portugal**, the press and specialised reports highlight the existence of money laundering through real estate, with a link to the resident permit programme and its requirement to invest in the country. A number of beneficiaries of the programme may have acquired properties using laundered funds.

The issue has been found to be of particular importance in the **United Kingdom** and in particular in **London**. An inquiry on foreign home ownership was launched by London's mayor in 2016, with political follow-up. A number of reports provide a factual assessment of the role of overseas investors in the London new-build residential market and on the true effects of foreign investment on the UK property market. A July 2017 House of Commons Library briefing on Foreign investment in UK residential property provides data on the scale of overseas investment in housing and on property owned by overseas companies, and lists key issues associated with foreign ownership.

As regards quantitative data, the 2015 Transparency International report on Corruption on your doorstep and the 2017 Faulty Towers report provide an assessment of the scale of the problem.[16] They refer to the data of a 2016 Business innovation and skill survey indicating that between 2004 and 2014, 'over £180m worth of property in the UK has been investigated by UK law enforcement as suspected proceeds of corruption. Moreover, over 75 % of these properties use offshore corporate ownership. This is believed to be the tip of the iceberg in terms of the scale of the proceeds

Golden visa

Citizenship by investment (CBI) and residency by investment (RBI) schemes, often referred to as 'golden visas', are national schemes designed to attract foreign investment. Some of these schemes offer residency or citizenship rights in exchange for a sizeable investment, including real estate investment.

Concerns about money laundering arise when the beneficiaries happen to be using illicit money for the purchase of real estate.

of corruption invested in UK property through offshore companies'. The survey also details the location of the offshore company owners of a larger number of properties and draws a map of the city that highlights the boroughs most affected. According to Transparency International UK, the second report 'assessed 14 new landmark London developments, worth at least £1.6 billion. It found 4 in 10 of the homes in these developments have been sold to investors from high corruption risk countries or those hiding behind anonymous companies. Less than a quarter had been bought by buyers based in the UK'.

A public register requiring overseas companies that own or buy property in the UK to provide details of their ultimate owners is expected to be in place by 2021.

MAIN REFERENCES

FAFT, Money laundering and terrorist financing through the real estate sector, FATF/OECD, 2007.

FAFT, Guidance on the risk-based approach for real estate agents, FATF/OECD, 2008.

OECD, Real estate sector: tax fraud and money laundering vulnerabilities, 2007.

OECD, Money laundering awareness handbook for tax examiners and tax auditors, 2009.

ENDNOTES

1 As one press article puts it: 'probably the most advantageous aspect of buying real estate is that reporting requirements for suspicious activity are almost non-existent, particularly compared to banks and financial institutions, which are legally required to blow the whistle on anything that looks fishy' (US local news online).

2 See also F. Teichmann, 'Twelve methods of money laundering', *Journal of money laundering control*, 2017, Vol. 20, Issue 2, pp130-137.

3 For an illustration of this widespread concern, see: Money laundering and real estate – Why the real estate sector should prepare for regulation, Acuity, 2018.

4 This situation triggered the adoption of a speculation tax.

5 Canada has been identified 'as a country that [China] wishes to target for recovering the proceeds of Chinese corruption' in FAFT, Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report, September 2016, footnote 10, p.16.

6 Similar analyses have been made globally, see for instance the 2008 FINCEN Suspected money laundering in the residential real estate industry and the Australian government's strategic analysis on Money laundering through real estate.

7 A consolidated version is available in Eur-lex.

8 The beneficial owner 'refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement'. On the initiative of the G20, work is ongoing to establish A global framework for tracing beneficial ownership.

9 Prior to the implementation of the most recent changes in the EU AML framework. For all of them, only limited experience has been gained so far to assess the provisions.

10 Article 6 of Directive (EU) 2015/849 requires the Commission to draw up, by 26 June 2017, a report identifying, analysing and evaluating money laundering and terrorism financing risks at Union level.

11 Recommendations in the 2017 Faulty Towers report focus specifically on the London property market. The report also includes a specific recommendation to introduce more transparent regarding off-plan property purchases (buying from plans before the property has been built). The 2018 Towards better AML practice – real estate scoping paper is not based on a specific geographical area.

12 According to the World Bank Group's response to illicit financial flows, the term 'Illicit financial flows (…) generally refers to cross-border movement of capital associated with illegal activity or more explicitly, money that is illegally earned, transferred, or used that crosses borders. This falls into three main areas: the acts themselves are illegal (e.g. corruption, tax evasion); or the funds are the results of illegal acts (e.g. smuggling and trafficking in minerals, wildlife, drugs, and people); or the funds are used for illegal purposes (e.g. financing of organised crime)'.

[13] In the World Bank Group's response to illicit financial flows: a stocktaking (dated March 22, 2016), a range of figures is quoted and the report states that 'While these estimates are difficult to verify (and are not always consistent), they indicate that the amounts involved are significant and pose widespread problems'.

[14] Estimating illicit financial flows resulting from drug trafficking and other transnational organised crimes Research report, in 1988, p.7.

[15] For more information, see M. Feferman and Y. Pelosi, L'immobilier face au blanchiment et au financement du terrorisme, RICS, Edition PC, December 2017.

[16] Statistics included in the report are based on data available at the time of the preparation of the report.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Appendix 11

Transparency International Canada – *No Reason To Hide: Unmasking the Anonymous Owners of Canadian Companies and Trusts* - 2016

TRANSPARENCY INTERNATIONAL CANADA

NO REASON TO HIDE

Unmasking the Anonymous Owners of Canadian Companies and Trusts

Appendix 11

About Transparency International and Transparency International Canada

Transparency International (TI) is the world's leading non-governmental anti-corruption organization. With more than 100 chapters worldwide and an international secretariat in Berlin, TI has helped put corruption on the agendas of governments and businesses around the world. Through advocacy, research and capacity building work, TI strives toward a world that is free of corruption.

Transparency International Canada (TI Canada) is the Canadian chapter of Transparency International. Since its foundation in 1996, TI Canada has been at the forefront of the national anti-corruption agenda. In addition to advocating legal and policy reform on issues such as whistleblower protection, public procurement and corporate disclosure, we design practical tools for Canadian businesses and institutions looking to manage corruption risks, and serve as an anti-corruption resource for organizations across Canada.

Acknowledgements

TI Canada and the author of this report would like to thank the Omidyar Network and the TI-Secretariat for the generous financial support that made this publication possible. We would also like to extend our gratitude to BC MLA David Eby for obtaining the land titles and corporate filings used in our research on Vancouver real estate, as well as to all of the stakeholders in industry, government and civil society who provided insights and feedback during the drafting of this report.

We are particularly grateful for the support and guidance offered by the members of TI Canada's Beneficial Ownership Working Group:

Noah Arshinoff
Peter Dent
Don Jack
Denis Meunier
Bruce Moore
Susan Reisler
Claire Woodside

Author: Adam Ross, White Label Insights
Design: Deana Oulianova, DIMA Design Studio

Table of Contents

Foreword

We are in the midst of a monumental shift in societal expectations about transparency. Whistleblower disclosures such as the Panama Papers and Luxembourg Leaks have provided concrete examples of the ways in which legal entities and arrangements – companies and trusts – are exploited to the public's detriment by those looking to avoid taxes or launder the proceeds of crime and corruption, among other nefarious aims. The abuses exposed through these leaks and others have resonated with the public and triggered widespread interest in what were once dismissed as mundane legal issues.

Governments around the world also appear to be recognizing the threats posed by under-regulated legal entities and arrangements. In 2014 the G20 issued its *High-Level Principles on Beneficial Ownership*, acknowledging the importance of transparency in protecting the integrity of the global financial system. In 2016 the European Commission mandated its 27 member countries to collect and publish information on the beneficial owners of companies registered within the bloc. The UK has already enacted legislation and implemented new disclosure rules, and other countries are following suit.

As more countries put up barriers to the criminal and corrupt, those looking to game the system will gravitate to jurisdictions with weaker standards. As the following report demonstrates, Canadian companies and trusts are particularly vulnerable to exploitation. Beneficial owners can remain entirely anonymous – their identities concealed even from the government agencies entrusted with enforcing laws and regulations. Anonymous ownership creates unnecessary obstacles for our law enforcement and tax authorities, fostering a climate of impunity due to low perceived risk.

Beneficial ownership transparency is by no means a panacea for corruption and financial crime. However, by stripping anonymity from legal entities and arrangements we can make those crimes easier to detect and prosecute, thereby deterring them. Beneficial ownership reform presents an opportunity for Canada to meaningfully reduce financial crime and honour our international commitments. We must adapt to emerging international standards or risk becoming a beacon for the corrupt.

Paul Lalonde
Chair and President
Transparency International Canada

Alesia Nahirny
Executive Director
Transparency International Canada

Glossary

AML	Anti-money laundering
BVI	British Virgin Islands
CRA	Canada Revenue Agency
DNFBP	Designated non-financial businesses and professions
FATF	Financial Action Task Force
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
G8	Group of eight leading advanced economies
G20	Group of 20 major economies
OECD	Organization for Economic Cooperation and Development
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
RCMP	Royal Canadian Mounted Police
StAR	Stolen Assets Recovery Initiative
STR	Suspicious transaction report
TF	Terrorist financing
TI Canada	Transparency International Canada
UNODC	United Nations Office on Drugs and Crime

Executive Summary

Anonymous companies and trusts are the getaway cars of financial crime. They enable criminals to hide behind a veil of secrecy, while giving them access to bank accounts and the means to use their illegally obtained wealth in the legal economy. These legal entities and arrangements are ubiquitous in money laundering cases, and are used to evade taxes, dodge sanctions and finance terrorism.

Legal entities and arrangements serve valuable purposes in society, such as limiting liability and enabling individuals to manage wealth for others. These legitimate functions of companies and trusts do not depend upon anonymity, and can still be served when their ownership is transparent. Hiding the identities of beneficial owners serves no constructive purpose to society as a whole, and it is time to close this legal loophole.

In November 2014, G20 leaders pledged to tackle corporate secrecy. They agreed to 10 principles, setting out concrete measures they would take to make beneficial ownership information transparent and accessible. The G20 countries committed to ensuring that all companies and trusts in their jurisdiction identify their beneficial owners and make that information available to law enforcement and tax authorities. Many governments are going further by making beneficial ownership information available to the public. For example, the European Commission has proposed public beneficial ownership registries for companies, and partially public registries for trusts.

Building on Transparency International's 2015 report, *Just for Show? Reviewing G20 Promises on Beneficial Ownership*, this report assesses Canada's progress in fulfilling its commitment to the G20 principles. It analyses the current legal framework and enforcement regime, and provides evidence showing the extent to which companies and trusts are misused in Canada. The report then takes an in-depth look at beneficial ownership in the context of the real estate market. It concludes with a series of recommendations for the Government of Canada and other stakeholders, which if implemented would bring Canada in line with international best practices.

Meeting Canada's G20 commitments

Transparency International's 2015 analysis found that Canada's performance was either "weak" or "very weak" in seven of the 10 G20 principles on beneficial ownership. In the past year, the government has tabled legislation to eliminate bearer shares (unregistered securities that are owned by whoever happens to physically hold the share certificate), but has otherwise made no measurable progress on any of the 10 principles. In September 2016 the Financial Action Task Force – the global anti-money laundering authority that informed the principles – published an evaluation of Canada that was highly critical of the secrecy it affords to legal entities and arrangements. The task force called on the government to make beneficial ownership information accessible "as a matter of priority."

Canada's secrecy regime

In Canada, more rigorous identity checks are done for individuals getting library cards than for those setting up companies. Corporate registries do not verify identification and most do not require information on shareholders, let alone beneficial owners. Most provinces also allow nominee directors and shareholders, who do not need to disclose that they are acting on someone else's behalf. Though a law has been proposed to eliminate bearer shares at the federal level, they are still allowed in much of the country.

Trusts in Canada do not need to register or file a record of their existence. There are estimated to be millions of trusts in Canada, though only 210,000 are registered to pay taxes. Trustees do not need to keep any record of beneficial owners, nor do they need to disclose that they are acting for others when transacting with banks or other businesses.

The lack of available information on private companies and trusts, and who owns them, is a huge obstacle for law enforcement and tax authorities. The RCMP's success rate in pursuing money laundering is a fraction of what it is for other crimes. A suspect cannot be identified in more than 80 percent of cases, and only a third of the cases that go to trial result in a conviction. The cost to the treasury in lost tax revenues is impossible to measure given the lack of data on legal entities and arrangements, but is likely in the billions of dollars.

Secrecy in the real estate market

The average price of a home in Canada has skyrocketed in recent years, with the largest increases in Toronto and Vancouver. An influx of overseas capital is one of several causes of rising property prices, but the extent and impact of foreign investment remains unknown since very little data is collected on property owners. Individuals can use shell companies, trusts and nominees to hide their beneficial interest in Canadian real estate. Research by TI Canada shows that this practice is most prevalent in the luxury property market.

Analysis of land title records by TI Canada found that nearly half of the 100 most valuable residential properties in Greater Vancouver are held through structures that hide their beneficial owners. Nearly one-third of the properties are owned through shell companies, while at least 11 percent have a nominee listed on title. The use of nominees appears to be on the rise; more than a quarter of the high-end homes bought in the last five years are owned by students or homemakers with no clear source of income. Trusts are also common ownership structures for luxury properties; titles for six of the 100 properties disclose that they are held through trusts, but the actual number may be much higher as there is no need to register a trust's existence.

Recommendations

The key recommendation of this paper is for the Government of Canada to require all companies and trusts in the country to identify their beneficial owners. The government should then publish this information in a central registry that is accessible to the public in an open data format.

A public registry of companies and trusts that includes beneficial ownership information would be a low-cost, high-impact way of preventing their misuse. It would improve the effectiveness of law enforcement and tax authorities. It would help the private sector comply with regulations and make better business and investment decisions. It would also bolster Canada's reputation for fairness and transparency both at home and abroad.

This report concludes with several other recommendations, including:

- Nominees should be required to disclose that they are acting on another's behalf, and the beneficial owners they represent should be identified.

- Corporate registries should be given adequate resources and a mandate to independently verify the information filed by legal entities, including the identities of directors and shareholders.

- Beneficial ownership information should be included on property title documents, and no property deal should be allowed to proceed without that disclosure.

- The Government of Canada should make it mandatory for all reporting sectors – including real estate professionals – to identify beneficial ownership before conducting transactions.

- All government authorities in Canada should require beneficial ownership disclosure as a prerequisite for companies seeking to bid on public contracts.

1 Companies, Trusts and Secrecy

Corporations and trusts – legal entities and arrangements – serve valuable purposes in our society. They enable us to take risks, such as opening a business or developing a new product, without gambling our personal livelihoods. They allow us to manage wealth for others and plan for when we can no longer manage our own affairs. But legal entities and arrangements can also be exploited in ways that were likely never intended by those who designed them. When these structures were originally developed, safeguards were not built in to prevent people from hiding their identities, and after many decades of misuse it is time to close these loopholes.

The ease of setting up a company and the anonymity it affords has made corporations a useful vehicle for criminals. According to the OECD, "almost every economic crime involves the misuse of corporate vehicles [i.e. companies and trusts]."[1] Shell companies – corporations with no business activity – are frequently used to launder money, commit fraud, evade taxes, dodge sanctions and finance terrorism.

What is a shell company?

Unlike a regular company – one with business operations – a shell company is a hollow structure that is often set up solely to perform financial manoeuvres. It essentially only exists on paper.

Like other companies, shell companies are legal persons. They can sign contracts, take out loans and set up bank accounts.

Anonymous shell companies enable criminals to:

- **Get away with corruption.** In a 2011 study, the World Bank looked at 213 cases of grand corruption spanning three decades and found that corrupt politicians had used shell companies to conceal activities in more than 70 percent of those cases, enabling the theft of US$56.4 billion.[2] One of those cases involved the son of Equatorial Guinean president, Teodoro Obiang Nguema Mbasogo, who the US Department of Justice took to court over US$32 million in luxury real estate and other assets that he had bought with the proceeds of corruption. Most of those assets were owned through anonymous shell companies.[3]

- **Launder proceeds of crime.** The United Nations Office on Drugs and Crime (UNODC) estimated the total value of money laundered worldwide to be around US$2.1 trillion in 2009, or 3.6 percent of global GDP.[4] The vast majority of that money goes undetected, and much of it is laundered through shell companies.[5] US law enforcement finds less than 1.5 percent of the estimated US$65 billion in annual drug proceeds in America.[6] In one of the detected cases a high-level trafficker, who was given a 150-year sentence in 2014, used a typical shell company structure to buy more than US$14 million in Florida property.[7] In another case detected in the US, the Zetas drug cartel used a network of shell companies to buy and sell racehorses.[8]

- **Evade taxes.** Tax evasion by individuals costs the world's governments some US$190 billion each year, according to conservative estimates.[9] The figures for aggressive tax avoidance – arrangements that are technically legal but contrary to the spirit of the law – are much higher. Opaque legal entities and arrangements enable most tax avoidance schemes, such as one designed by KPMG that reportedly hid at least C$130 million from the Canadian tax authorities before it was discovered in 2013. Though the matter has yet to be resolved in the courts, available evidence suggests that the scheme used shell companies based in the Isle of Man to help multimillionaire clients shirk domestic tax obligations.[10]

- **Commit fraud.** Shell companies are an essential part of the fraudster's toolkit, enabling them to create illusions of business success and cover their tracks. In 2010, Florida-based lawyer Scott Rothstein pleaded guilty to fraud charges after prosecutors unearthed a US$1.2 billion Ponzi scheme in which he used 85 shell companies to hide his interest in real estate and business ventures.[11]

- Legal entities and arrangements are also used to **channel funds to terrorist groups,**[12] provide cover for **insider trading and market manipulation,**[13] and **evade sanctions**[14] against international pariahs.

Who is a beneficial owner?

A beneficial owner is the natural person who ultimately owns, controls or benefits from a legal entity or arrangement and the income it generates. This term contrasts with the legal owners of a company (i.e. the shareholders) or with trustees, who might own assets on paper that are actually held for someone else's benefit.

Financial getaway cars

Since shell companies can be set up without disclosing who owns or controls them, it is difficult if not impossible for law enforcement to catch the perpetrators when an anonymized company is used to commit crimes. In many jurisdictions only the most basic information is kept on companies, and it is rarely independently verified. Shell companies are effectively financial getaway cars that can be used to enable criminals to vanish without a trace.[15] Leading law enforcement agencies have voiced their frustrations with the status quo, and many have joined the call for legal reform to collect and publish beneficial owner information.[16]

> "We will make a concerted and collective effort to tackle this issue and improve the transparency of companies and legal arrangements. Improving transparency will also improve the investment climate; ease the security of doing business and tackle corruption and bribery. It will support law enforcement's efforts to pursue criminal networks, enforce sanctions, and identify and recover stolen assets."
>
> – G8 Lough Erne Declaration, June 2013[17]

2 Big Talk, Little Action: Canada's Global Commitments

While the world's leading economies move toward greater transparency, Canada seems to be dragging its feet. The government has taken very few concrete steps, despite making strong commitments at high-profile events including recent G8 and G20 summits.

In November 2014, Canada and the other G20 nations adopted *10 High-Level Principles on Beneficial Ownership Transparency*, which set out specific measures that member countries "committed to leading by example in implementing" through "concrete action."[18] One year after the pledge was made, Canada was evaluated and ranked among the bottom three countries (with Brazil and South Korea), receiving a "weak" or "very weak" grade on seven of 10 principles by Transparency International.[19] At that time the only step Canada had taken to implement the 10 principles was to conduct a risk assessment, which it did in early 2015.[20,21]

Canada has made little progress in the past year with respect to its beneficial ownership commitments. The government recently proposed an amendment to the *Canada Business Corporations Act* that would eliminate bearer shares (an issue discussed in the following section), but has otherwise not moved to address the significant gaps between the status quo and international best practices.

Table 1: Canada's Compliance with the G20 High-Level Principles

G20 Principles		TI Ranking[22]
1	Definition of beneficial owner	 Weak
2	Risk assessment relating to legal entities and arrangements	 Strong
3	Beneficial ownership information of legal entities	 Very Weak
4	Access to beneficial ownership information of legal entities	 Very Weak
5	Beneficial ownership information of trusts	 Average
6	Access to beneficial ownership information of trusts	 Weak
7	Roles and responsibilities of financial institutions and businesses and professions	 Very Weak
8	Domestic and international cooperation	 Weak
9	Beneficial ownership information and tax evasion	 Average
10	Bearer shares and nominees	 Very Weak

Meanwhile, several G20 countries – including the UK, France, Australia and South Africa – have committed to establishing public registries of beneficial owners or have taken concrete steps toward doing so. In May 2015, the European Commission enacted a law that compels all EU countries to set up their own registries of beneficial ownership by June 2017,[23] and it has since directed that those registries be made public.[24] Even the US, which has the dubious distinction of hosting more shell companies than anywhere else on Earth, has tabled beneficial ownership legislation with support from Democrats, Republicans and the White House.[25]

Canada's inaction on beneficial ownership reform recently prompted criticism from the Financial Action Task Force (FATF), the world's foremost anti-money laundering authority. In a September 2016 evaluation, the FATF found that Canada has "achieved a low level of effectiveness" in mitigating the risks associated with legal entities and arrangements. It implored the government to ensure access to accurate and up-to-date beneficial ownership information "as a matter of priority."[26]

In an official statement issued for the Global Anti-Corruption Summit in London in May 2016, the Government of Canada committed "to exploring additional measures to improve our ability to collect timely and accurate beneficial ownership information."[27] It is now time for a specific, time-bound action plan to determine and implement those measures.

3 Canada's Secrecy Regime

Though Canada is not known as a global hub for money laundering and tax evasion, our legal framework and lax enforcement environment make it easy for individuals to misuse private companies and trusts with relative impunity. As previously highlighted, Canada is among the world's most opaque jurisdictions with regard to legal entities and arrangements. In the midst of a global shift toward greater transparency, Canada is an increasingly attractive destination for those looking to park and invest the proceeds of crime.[28]

Companies

In Canada, more rigorous identity checks are done for individuals getting library cards than for those setting up companies.[29]

Canada is one of the easiest places in the world to set up a company. All you need is a few hundred dollars, an address and someone to appoint as a director. There is no need to show documentation to prove who you are, and you are free to list other people – nominees – as the company's directors or shareholders. In all but two provinces – Alberta and Quebec – companies are not required to identify their shareholders. Beneficial owners can remain totally anonymous.

A recent study found that of 60 countries around the world – including known tax havens and secrecy jurisdictions – only in Kenya and a select few US states is it easier to set up an untraceable company than it is in Canada.[30,31] The study's authors sent emails to corporate service providers where they posed as possible terrorist financiers and corrupt government officials looking to set up a company that would hide their identity. Nearly two-thirds of the Canadian lawyers and incorporation agents that responded to their emails were willing to set up a company for them and act as their nominee. As a testament to the secrecy afforded in Canada, the law firm at the centre of the Panama Papers leak, Mossack Fonseca, marketed Canada to its clients as an attractive place to set up anonymous companies.[32]

The current system in Canada is particularly vulnerable to abuse, as none of the limited information that companies do disclose is independently verified. Canadian law enforcement agencies have complained that company records are often "outdated or imprecise," making it difficult to investigate suspected wrongdoing.[33] In some cases – particularly when a company is used to commit a crime or launder its proceeds – those behind it can intentionally provide false information. This is easily done as no identification is required.

Though it is illegal to do so, no company has ever been criminally sanctioned for failing to keep accurate records.[34]

Charbonneau Commission Invoicing Fraud

During a four-year investigation into Quebec's public works industry, the Charbonneau Commission documented widespread corruption, procurement fraud, price-fixing and links to organized crime.[35] The Commission found that Montreal-area construction firms used shell companies to generate false invoices for expenses on government-funded projects, costing taxpayers tens of millions of dollars each year.[36]

These false invoicing schemes typically include several companies with related beneficial ownership, which issue invoices to one another for fake services. They receive payment, convert it to cash and repay the balance less a commission. When a shell company comes to the attention of tax authorities, it is dissolved and another one is formed. One such scheme run by Normand Dubois – a construction firm owner who is now serving a six-year prison sentence for fraud – involved nearly a dozen shell companies with nominee directors and shareholders, which provided fake invoices to his own company and several others.[37] Those companies then billed the government for the falsified expenses.

As a Revenue Quebec investigator interviewed by the Commission lamented, "it's very hard to keep track of this… there is still a lot of false invoicing going on." With no disclosure of who the natural person is behind a shell company, tax authorities and investigators often struggle to connect the dots between related entities.

There is no centralized and publicly available data on how many companies exist in Canada. Each province and territory has its own corporate registry, with its own standards of information collection and disclosure. There is no central repository of company information. In the course of researching this report, TI Canada contacted each of the provincial and territorial registries in an effort to find out how many companies there are in the country. In most parts of Canada, basic data on the number of companies was not readily available even to registry employees. The fact that these figures were hard to come by reflects an overall lack of transparency and inadequate data collection with regard to Canadian companies.

Table 2:
Canadian Business Corporations

Province/Territory	Number of Companies[38]
Ontario	1,088,920
Quebec	950,000
Alberta	421,680
British Columbia	385,410
Federal	286,280
Saskatchewan	73,870
Manitoba	73,220
Nova Scotia	44,200
New Brunswick	33,610
Newfoundland	26,000
Prince Edward Island	7,140
Northwest Territories	7,070
Nunavut	4,500
Yukon	2,520
TOTAL	3.4 MILLION (APPROX.)

Trusts

What is a Trust?

A trust is a legal arrangement whereby an asset is conferred on one individual or entity (a trustee) to manage on behalf of others (the beneficiaries). The terms of the arrangement are set out in a trust instrument, which is typically drafted by a lawyer or notary.

Most trusts are used for legitimate purposes such as estate planning or managing charitable donations, but the confidentiality associated with them makes the trust structure attractive to money launderers and tax evaders.

There are estimated to be millions of trusts in Canada. No one knows how many there are, as Canadian trusts do not need to register their existence.

Canadian trusts are supposed to provide the Canada Revenue Agency (CRA) with information on their assets and trustees, and according to the CRA some 210,000 do. That constitutes a minority of the domestic trusts and foreign trusts with Canadian assets that are obligated to file tax returns.[39] Because trusts are treated as private contracts (and are often protected under attorney-client privilege) it is virtually impossible to identify those that do not meet their Canadian tax obligations.

There is an even greater degree of anonymity for beneficial owners of trusts than for beneficial owners of companies. A trust's existence does not need to be acknowledged by a government authority, and trust documents are entirely private. Under Canadian trust law, trustees have a fiduciary duty to their beneficiaries, and therefore have a practical need to know their identities. However, they are not required to keep records of the trust's beneficial owners or settlors (i.e. those contributing assets to the trust), nor are they required to do any customer due diligence. Trustees are often bound by confidentiality provisions in the trust instrument and are generally not compelled to disclose the trust's existence or the identities of its beneficiaries to the CRA or other authorities unless ordered to do so by a court.[40] Trustees can do business and execute financial transactions on behalf of a trust without disclosing their status as trustees, which poses a challenge for financial institutions and others trying to comply with their money laundering reporting obligations.[41]

The private nature of trust instruments, the fiduciary obligation of trustees to maintain confidentiality, and the absence of any record-keeping requirements combine to make trusts highly vulnerable to money laundering, according to a recent risk assessment by the Canadian government. Law enforcement agencies agree that trusts are "misused to a relatively large extent."[42] In a September 2016 evaluation, the FATF found Canada "non-compliant" with its standards on trusts.[43]

Nominees

Nominees add yet another layer of secrecy to private companies. As noted elsewhere in this report, it is legal to appoint nominees as directors or shareholders of Canadian companies. Nominees need not identify who they represent, or even disclose that they are acting on someone else's behalf. Like other directors and shareholders, there is no requirement for nominees to keep a record of a company's beneficial owners.[44]

There are two broad categories of nominee: professionals, such as lawyers or company service providers; and informal nominees, such as family members, friends or associates who front for the beneficial owner. In Canada, nominee shareholders are typically lawyers, who hold shares on behalf of their beneficial owner clients.[45] As expanded upon in the following pages, this practice can be problematic from a money laundering standpoint in light of the legal profession's exemption from reporting obligations.

The prevalence of nominees in Canadian companies – particularly with respect to nominee shareholders – is a major money laundering risk and a serious obstacle to law enforcement, as the recent FATF review made clear.[46]

Who are Nominees?

Nominees are individuals (or in some cases entities) who have been appointed to act as a director or hold shares on behalf of a beneficial owner. They are usually bound by contract to only act upon the beneficial owner's instructions, and in some cases they issue a power of attorney allowing the owner to conduct business directly.

Li Dongzhe and Li Donghu

In late 2004, two brothers on the run from Chinese authorities arrived in Canada. They stood accused of embezzling C$113 million from client accounts at a state-owned bank.

In 2000, Li Dongzhe partnered with a Bank of China branch manager, Gao Shan, and together recruited clients by offering kickbacks for depositing funds with the branch. Once the customers had deposited funds with the bank, the men forged documents and transferred money to accounts held by Li Dongzhe and his brother, Li Donghu.

Chinese police issued arrest warrants and Interpol Red Notices for the three suspects in early 2005. By that time, the Li brothers were already established in Canada with properties, bank accounts and vehicles registered in their names. Within a few months of the warrant being issued, the brothers had sold all traceable assets in Canada and restructured their holdings through nominees.[47]

Court transcripts show that investigators had difficulty identifying the Li brothers' Canadian assets due to their use of shell companies and nominees.[48] The brothers admitted that they sold or transferred all directly held assets in order to evade detection. Those efforts were somewhat successful; there are reportedly still tens of millions in unrecovered funds.

According to the RCMP, the Li brothers "placed vehicles, properties, utility bills, businesses and bank accounts into nominee names in order to avoid detection from the authorities."[49] Among the measures taken by the brothers to launder funds was the incorporation of a Manitoba company, Canada Century Greenland Investment Ltd., with a nominee director and shareholder. A bank account was set up for the company with Li Dongzhe as signatory. A police affidavit recounts a confession by Li Dongzhe that money deposited into that account included the proceeds of crime.[50]

A two-year cross-border investigation led to the Li brothers' arrest in Vancouver in February 2007. Unsuccessful in their petitions to stay in Canada, the brothers returned to China to face trial in late 2011. In September 2014, Li Dongzhe pleaded guilty to fraud charges and was sentenced to life in prison. Li Donghu and Gao Shan received 25-year and 15-year sentences, respectively.[50]

Bearer Shares

Canada is one of three G20 countries allowing companies to issue bearer shares.[51] Many other states have outlawed bearer shares because they are vulnerable to loss, theft and misuse. Even secrecy havens like Panama and the British Virgin Islands (BVI) have banned them. Though the use of bearer shares appears to be relatively uncommon in Canada, they are an antiquated instrument and a loophole for money launderers that could be easily closed.

What are Bearer Shares?

Bearer shares are unregistered securities that are owned by whoever physically holds the share certificate.

The federal government is currently taking measures to ban bearer shares. In September 2016 it tabled an amendment to the *Canada Business and Corporations Act*, Bill C-25, which will "clarify that corporations and cooperatives are prohibited from issuing share certificates and warrants, in bearer form."[52] The government should be commended for moving to ban bearer shares. Provinces that still allow bearer instruments should follow suit.

Legal Troubles

In Canada the vast majority of legal entities and arrangements are set up and administered by lawyers, who are therefore in a unique position to know what they are used for and who they benefit.[53] Lawyers frequently act as nominee shareholders and directors, and hold money in trust for their clients.[54] While there is nothing inherently wrong with these roles and activities, a significant loophole in transparency efforts has opened up in the absence of statutory reporting of beneficial owners.

In a ruling on February 13, 2015, the Supreme Court of Canada exempted lawyers and their firms from certain obligations under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) on the grounds that those requirements breached the constitutional right to attorney-client privilege.[55] Lawyers and their firms are no longer subject to PCMLTFA requirements to identify and verify clients' identities, maintain records, develop compliance regimes and be subject to Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) audits. This ruling created "a significant loophole in Canada's [anti-money laundering and terrorist financing] framework," according to the FATF, which recently assessed "the legal profession in Canada [to be] especially vulnerable to misuse."[56]

According to the FATF, the federal government is assessing how it might introduce new anti-money laundering provisions for the legal profession that would be constitutionally compliant.[57] A statutory requirement to collect and disclose beneficial ownership information would be a significant step in that direction.

R. v. Rosenfeld

In 2009, Ontario lawyer Simon Rosenfeld was sentenced to five years in prison on money laundering charges. Rosenfeld was arrested following a 2002 sting operation in which he laundered C$440,000 for an RCMP officer posing as a representative of a Colombian drug cartel. He used shell companies to set up bank accounts and structure those transactions and allegedly others involving millions of dollars.[58]

Rosenfeld bragged during a meeting with the undercover agent that it was "20 times safer" for a lawyer to launder money in Canada than in the US.[59] He described Canada as a "la la land" where white-collar crime goes unpunished,[60] and told the officer about five Vancouver-based lawyers who laundered upward of C$200,000 a month through trust accounts in return for a seven percent commission.[61]

In his sentencing, the ruling judge noted that Rosenfeld had exploited attorney-client privilege and the exemption from reporting obligations "to enhance his money laundering services" – an apparent nod to the vulnerability of the legal profession to laundering the proceeds of crime.[62] According to the RCMP officer's testimony, "In almost every case we are doing, lawyers are central."[63]

Enforcement and Sanctions

As the case study on page 22 demonstrates, Canadian legal entities and arrangements are attractive to criminals not only due to the secrecy they afford but also because of a perceived lack of enforcement and lenient sanctions. Data published by the RCMP and FINTRAC suggests that these perceptions are well founded. Active enforcement and the use of appropriate sanctions are crucial to deterring criminal activity and promoting compliance among institutions and professionals.

> "On paper, Canada has built a Rolls-Royce when it comes to fighting money laundering… but we forgot to put in the engine – an effective law enforcement that can take on these complicated cases."
>
> – Former RCMP Proceeds of Crime Investigator[64]

Enforcement

Canada's current anti-money laundering and terrorist financing (AML/TF) regime places much of the onus for detection on the private sector,[65] which acts as the first line of defence for verifying client identities, keeping records and reporting transactions to FINTRAC. While FINTRAC supervises these reporting entities for compliance with the PCMLTFA, it has no powers to investigate money laundering. FINTRAC collects and analyses vast amounts of data provided by these reporting entities, and shares intelligence with law enforcement agencies when that information might be relevant to a money laundering or terrorist financing offence. Police use the financial intelligence produced by FINTRAC to pursue these cases.

Requirements under the PCMLTFA for identifying and verifying the identities of beneficial owners have been watered down to facilitate compliance, in part because there is no publicly available beneficial ownership registry for reporting entities to consult. While financial institutions, life insurers, securities dealers and money services businesses must attempt to determine beneficial ownership,[66] they may take other less stringent measures to meet their obligations if they cannot do so. Under rules introduced in February 2014, financial institutions must confirm beneficial ownership information when opening a new account (though that information does not need to be independently verified).[67]

As for the other reporting entities, such as real estate brokers and developers, accountants, BC notaries, and dealers in precious metals and stones, there are no requirements to determine and record beneficial ownership, which would be burdensome in the absence of an accessible registry.

In the absence of comprehensive beneficial ownership checks, individuals using shell companies or trusts for nefarious purposes can use Canadian financial entities to move money, invest or take out loans. They can also launder proceeds of crime through sectors such as real estate or precious metals, which are regulated under the PCMLTFA but have no obligation to ask questions about beneficial owners. If those front-line actors do happen to identify something suspicious, all they can do is report the information to FINTRAC, which may subsequently refer the matter to law enforcement.

Most money laundering cases in Canada are handled by the RCMP. According to government records from 2011, a suspect can be identified in only 18 percent of cases, and only one-third of cases that go to trial result in a guilty verdict. These figures are about half of the national average for criminal cases overall.[68]

One of the FATF's key findings in its September 2016 assessment of Canada was that "law enforcement results are not commensurate with [money laundering] risk." According to the task force, there is an "insufficient focus" on money laundering, and investigations "generally do not focus on legal entities and trusts (despite the high risk of misuse), especially when more complex corporate structures are involved."[69]

Where legal entities and arrangements are used to commit and conceal crimes, there is often a web that spans multiple countries. The designers of these complex ownership structures do so knowing that law enforcement agencies have trouble cutting through red tape when an investigation extends beyond their jurisdiction. Agencies rely on cumbersome mutual legal assistance requests, which routinely take months if not years to be addressed and are often refused.

According to a former director of the RCMP's Proceeds of Crime Unit, the lack of successful cases "comes down to a tremendous weakness in our investigative and prosecutorial forces."[70] Though the RCMP has not provided a public explanation for its comparatively poor performance on money laundering cases, other leading law enforcement agencies have made it clear that a lack of beneficial ownership information is a major obstacle to their investigations.[71] Some have called for public registries as a solution.[72,73]

Sanctions

> **"Effective, proportionate and dissuasive sanctions should be available for companies, financial institutions and other regulated businesses that do not comply with their respective obligations, including those regarding customer due diligence. These sanctions should be robustly enforced."**
>
> – G8 Action Plan Principles, June 2013[74]

From a criminal justice perspective, FATF explains that sanctions for money laundering in Canada "are not sufficiently dissuasive."[75] The FATF has recommended that Canada "increase efforts to detect, pursue, and bring before the courts cases of… misuse of legal persons and trusts," and calls on the government to ensure that law enforcement agencies are better resourced to investigate money laundering.[76]

FINTRAC, in its role of ensuring compliance with the PCMLTFA and its regulations, has the power to issue administrative monetary penalties when violations are detected. In April 2016 it levied its first fine for compliance violations against a Canadian bank. The agency came under fire from industry groups and civil society for declining to name the institution or provide details of the offences that led to the C$1.1 million penalty.[77] Prior to that fine, FINTRAC had issued 73 administrative penalties totaling C$5.12 million against non-bank entities covered by the PCMLTFA, according to the agency's 2015 annual report.[78]

Though the penalties available to FINTRAC have been criticized for being too small to be sufficiently dissuasive,[79] the agency nonetheless appears to be making some headway in ensuring compliance with the PCMLTFA. According to the FATF, "Overall, supervisory measures taken in Canada are having an effect on compliance with improvements demonstrated – albeit to varying degrees – both in the financial and designated non-financial businesses and professions (DNFBP) sectors. Information provided indicates that compliance has improved."[80] While compliance may be improving overall, beneficial ownership rules are weak and sectors like real estate remain exempt from having to identify and verify beneficial owners.

4 Focus on the Real Estate Sector

Canada is both a desirable place to live and a secure market in which to invest. Property prices – particularly in Toronto and Vancouver – have risen dramatically in recent years, due in part to an influx of foreign capital.[81] Much of that capital is presumed to come from legitimate sources. However,

Canada's real estate sector is attractive to those looking to invest the proceeds of crime, due to a lack of beneficial ownership disclosure, low levels of compliance with AML/TF obligations[82], and limited anti-money laundering enforcement.

Tax evasion, facilitated by a lack of transparency in property ownership, also seems to be a growing problem in Canada that has gone largely unpunished.[83]

A September 2016 FATF report identified the **Canadian real estate sector as "highly vulnerable to money laundering,"** echoing the findings of a government risk assessment conducted the previous year.[84] According to the FATF report, the real estate market "is exposed to high risk clients, including [politically exposed persons], notably from Asia." **Though it does not name specific individuals, the FATF report refers to "cases of Chinese officials laundering the [proceeds of crime] through the real estate sector, particularly in Vancouver."**[85]

Canadian land title offices do not hold information about beneficial owners of property; they only record the titleholder, which can be a shell company, a trust or a nominee. Beneficial owners of Canadian property can therefore remain anonymous. This anonymity is particularly prevalent in the luxury market, as research conducted by TI Canada shows.

> "There are cases of Chinese officials laundering the [proceeds of crime] through the real estate sector, particularly in Vancouver, and the Chinese government has listed Canada as a country that it wishes to target for recovering the proceeds of Chinese corruption."
>
> – FATF Mutual Evaluation Report, September 2016

Nominees

Headlines were made in May 2016 when a student from China bought a Vancouver mansion for C$31.1 million.[86] Though the value of the transaction was unique, the deal is part of a wider trend whereby unemployed individuals are acquiring luxury property in the city with other people's capital. A 2015 academic study looked at a sample of 172 Vancouver homes purchased in the last several years for C$1.25 million to C$9.1 million, and found that 35 percent of them were owned by either homemakers or students.[87] TI Canada's own research has found that 11 of Greater Vancouver's 100 most valuable residential properties are owned on paper by students or homemakers. These individuals have no source of employment income and are likely nominees for family or friends, though in the absence of more comprehensive data we cannot know for certain.

The use of nominee owners is a common tool for money laundering through real estate. A 2004 study of 149 proceeds of crime cases successfully pursued by the RCMP found that nominee owners were used in over 60 percent of real estate purchases made with laundered funds.[88]

Gang Yuan

In May 2015, the remains of a wealthy Chinese businessman were found in a West Vancouver home owned by a relative who stands accused of his murder. Court documents show that the mining magnate used nominees to hold property and other assets – a practice that has complicated the settling of his estate.

Gang Yuan had made a fortune in mining in China's Yunnan province by the time he moved to Canada in 2007. According to court documents, much of that wealth can be traced to corrupt deals. Yuan allegedly bribed officials with gold bars in order to secure coal-mining rights for his company, Beijing Datang Investment.[89] In 2016, Yunnan's former deputy director of land and resources, Lin Yunye, was convicted of corruptly selling off C$243 million in state mining assets, including those awarded to Yuan's firm.[90]

Yuan was murdered at his West Vancouver home in 2015. According to court records, he bought the mansion for C$4.5 million in 2010 but registered the purchase in the names of his cousin and her husband, Li Zhao, Yuan's alleged killer.[91] The Zhaos are the legal owners of that property, which Yuan's family claims was beneficially owned by the late mining tycoon. According to the Yuan family's counsel, Gang Yuan used the Zhaos as nominees for "legitimate tax reasons."[92] Yuan owned at least two other luxury properties in BC, including a C$17.7 million mansion that is held through a trust company managing Yuan's estate. In the absence of a will, the ownership of those assets is now a matter for the courts to decide.[93]

Beneficial owners can use nominees to avoid or evade tax by claiming principal residence or first-time homebuyer exemptions.

Recent investigations show that in some cases the principal residence exemption is being used to defraud the tax authorities on a commercial scale. In September 2016, *The Globe and Mail* reported on the activities of Vancouver-based businessman Kenny Gu, who had bought and sold dozens of properties financed by Chinese investors.[94] Though Gu was the beneficial owner and had absolute control of those properties, his investors were used to hold title and secure mortgages. According to documents reviewed by the newspaper, many of the properties were listed as principal residences for Gu's clients despite the fact that they did not live in the homes. Principal residences have several tax benefits: taxpayers are not required to report the sale of a principal residence and they receive an exemption from capital gains tax. Contracts show that Gu's investors would receive a set return of around 15 percent, while he pocketed any remaining profit. Neither Gu nor his clients appear to have paid tax on their gains.

Shell companies

In Canada, as in many other jurisdictions, legal entities can hold title to properties. Special purpose companies are useful and legitimate tools in commercial real estate, where joint ventures are common and developers need to limit liability to a single project. More controversially, those buying and selling commercial properties can also avoid property transfer tax by selling equity in a holding company rather than changing the titleholder.

For the time being, this tax loophole is also available to owners of residential property that is held through shell companies.[95] As discussed elsewhere in this report, beneficial owners can use shell companies to keep their identities secret, making their use appealing to people with something to hide.

Shell companies are used extensively to hold luxury property in international hubs such as London and New York. A February 2015 investigative report by Transparency International UK revealed that more than 36,000 London properties are held by shell companies registered in offshore havens such as the BVI, Jersey and the Isle of Man. More than 75 percent of properties investigated by the London Metropolitan Police as suspected proceeds of corruption are held through offshore shell companies.[96] A *New York Times* investigation, also from February 2015, showed how more than 200 shell companies owned apartments in Manhattan's iconic Time Warner Center.[97] Many of those apartments were traced back to politically exposed persons and controversial international business figures. According to that article, more than half of the luxury properties sold in New York City in 2014 were bought through shell companies.

Using shell companies to create a veil between beneficial owners and their properties is more common in Canada than one might expect. New research by TI Canada (see opposite) shows that nearly one-third of the 100 most valuable residential properties in Greater Vancouver are owned through shell companies. Most of those companies are registered in Canada, so the identities of their directors and officers are a matter of public record, but their ownership cannot be ascertained. Several companies are registered in offshore jurisdictions where nothing but the most basic information is disclosed.

Trusts

Property in Canada can be owned through trusts, the existence of which may or may not be disclosed on title documents. In cases where a trust is identified on title, no further information is provided about the nature of that agreement or the identities of its beneficiaries. Canadian properties may be held through bare trusts, which separate the legal title from beneficial ownership but give the trustees no decision-making powers. According to some lawyers, bare trusts have become a common tool to avoid paying property transfer tax in some provinces, in particular in BC where tax is only payable when a change in legal title is filed with the land title office.[98] It is impossible to know how many properties are held through these arrangements, as they are not registered and do not appear on land title records.

The Importance of Gatekeepers

Gatekeepers and intermediaries such as brokers, developers, notaries and lawyers are involved in the vast majority of real estate transactions and therefore can play a key role in detecting money laundering. Most of these gatekeepers have obligations under Canada's anti-money laundering law (the PCMLTFA) and its regulations. However, FINTRAC data suggests that there are low levels of compliance among professionals in the real estate sector.[99] As discussed in the previous section, there is a reporting exemption for lawyers and Quebec notaries, and several other types of intermediaries in the real estate sector are not covered by the current legislation, such as mortgage brokers and private lenders. Considering these weaknesses, it is no wonder why the sector is attractive to those looking to launder and hide the proceeds of crime.

Canada is one of seven G20 countries where real estate agents are not required to identify the beneficial owners of clients buying and selling property.[100] Some 20,000 Canadian real estate brokers are covered by the PCMLTFA, but there are major shortcomings in their compliance with the Act.[101] A recent review by FINTRAC of some 800 agencies found "significant" or "very significant" deficiencies at 60 percent of them with respect to money laundering controls.[102] According to FINTRAC, in the decade from 2003 to 2013, only 279 suspicious transaction reports (STRs) were filed in relation to real estate transactions, despite some five million sales taking place.[103]

It seems that little is being done to push real estate professionals to take their responsibilities more seriously. Despite pervasive non-compliance with Canada's anti-money laundering law, FINTRAC has only issued 12 financial penalties against realtors since December 2008.[104] Though there are criminal penalties of up to C$2 million and five years' imprisonment for failure to report suspicious transactions, no known cases against real estate professionals have been pursued.[105]

TI Canada Investigation into Vancouver Luxury Real Estate

TI Canada examined title documents for the 100 most expensive homes in Greater Vancouver, and found that nearly half of those properties – amounting to more than C$1 billion in assets – do not have transparent ownership structures. Of the 100 properties, 29 are held through shell companies (four of which are registered in offshore jurisdictions[106]), at least 11 are owned through nominees,[107] and six are held in trust for anonymous beneficiaries.

TI Canada's research suggests that the use of nominee titleholders is becoming more common.

Of the 42 high-end properties sold in the last five years, 26 percent are owned on paper by students or homemakers. In contrast, only one of the 58 homes bought before 2011 is owned through an obvious nominee.

More than one in four of the high-end properties sold in the last five years are owned by nominees, compared to 2% of the luxury homes bought before 2011.

Trusts also appear to have been used more by luxury property buyers in recent years. Titles for five of the six properties owned through disclosed trusts have been registered since 2011. As noted elsewhere in this report, there is no requirement to register trusts or even disclose their existence, so it is impossible to know how widely these arrangements are used.

Shell companies remain a popular tool for beneficial owners of luxury property in Vancouver. This ownership model was used in 30 percent of the titles registered in the past 10 years, as well as in 29 percent of the total sample reviewed by TI Canada.

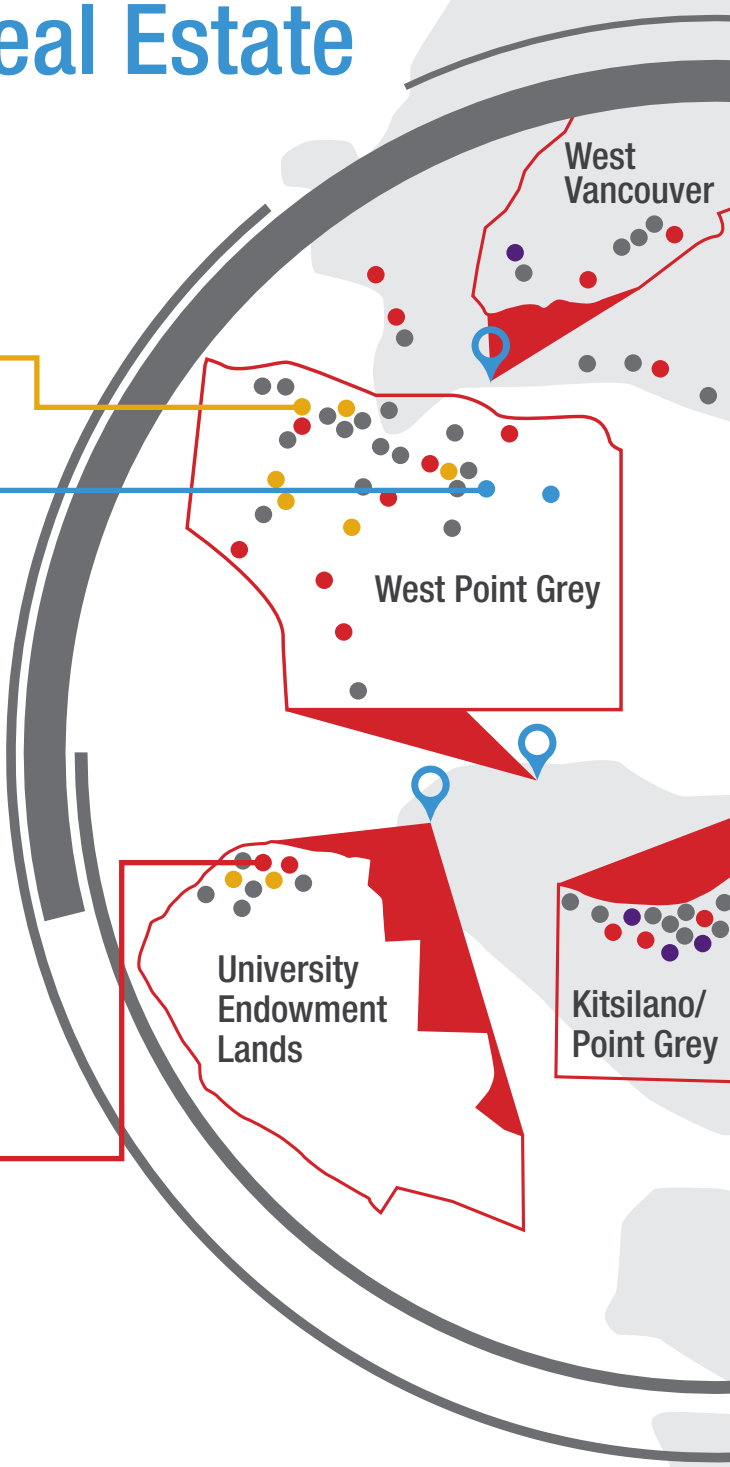
TI Canada has no reason to believe that the prevalence of shell companies, trusts and nominees in luxury real estate is unique to Vancouver. A similar assessment of high-value properties in other major Canadian cities was not possible within the scope of this report, given the costs associated with retrieving land title records. TI Canada would welcome further research into this area.

TI Canada Investigation Into Vancouver Luxury Real Estate

4833 Belmont Ave made headlines in May 2016 when it was bought for C$31 million by a student. Its true beneficial owner could not be identified.

4707 Belmont Ave is a C$57 million property owned through an anonymous shell company in the BVI.

5695 Newton Wynd is owned through a BC numbered company that's only director is a Vancouver lawyer. The owner of that company, and the property, are anonymous and sheltered by legal privilege.



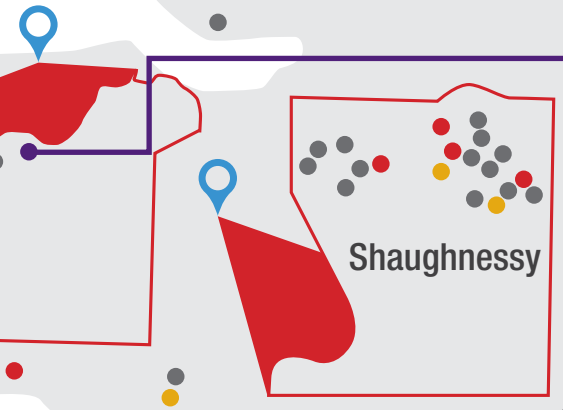
PROPERTY TYPES:

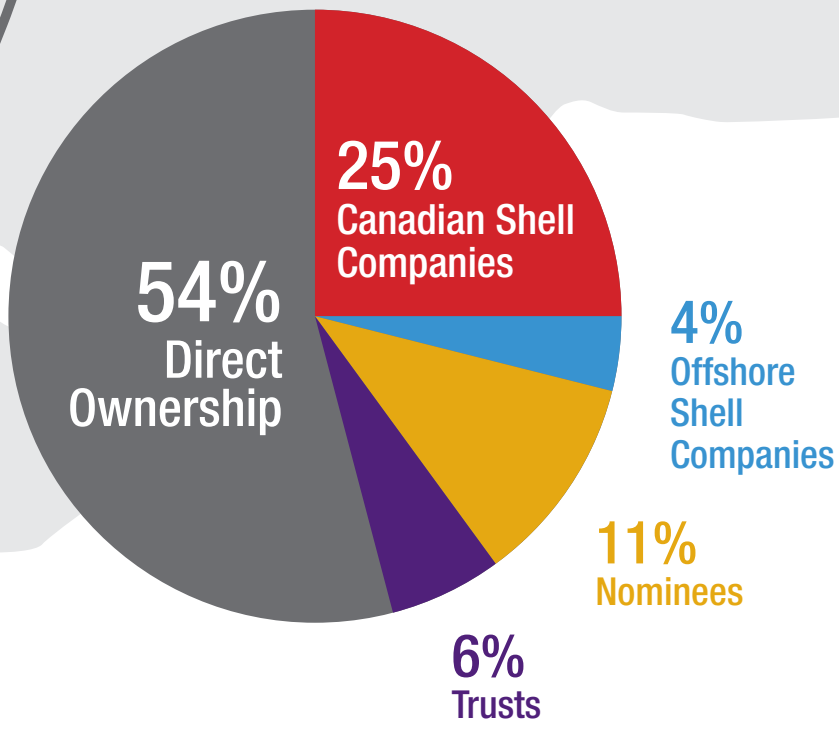
- Direct Ownership
- Domestic Company
- Offshore Company
- Nominee
- Trust

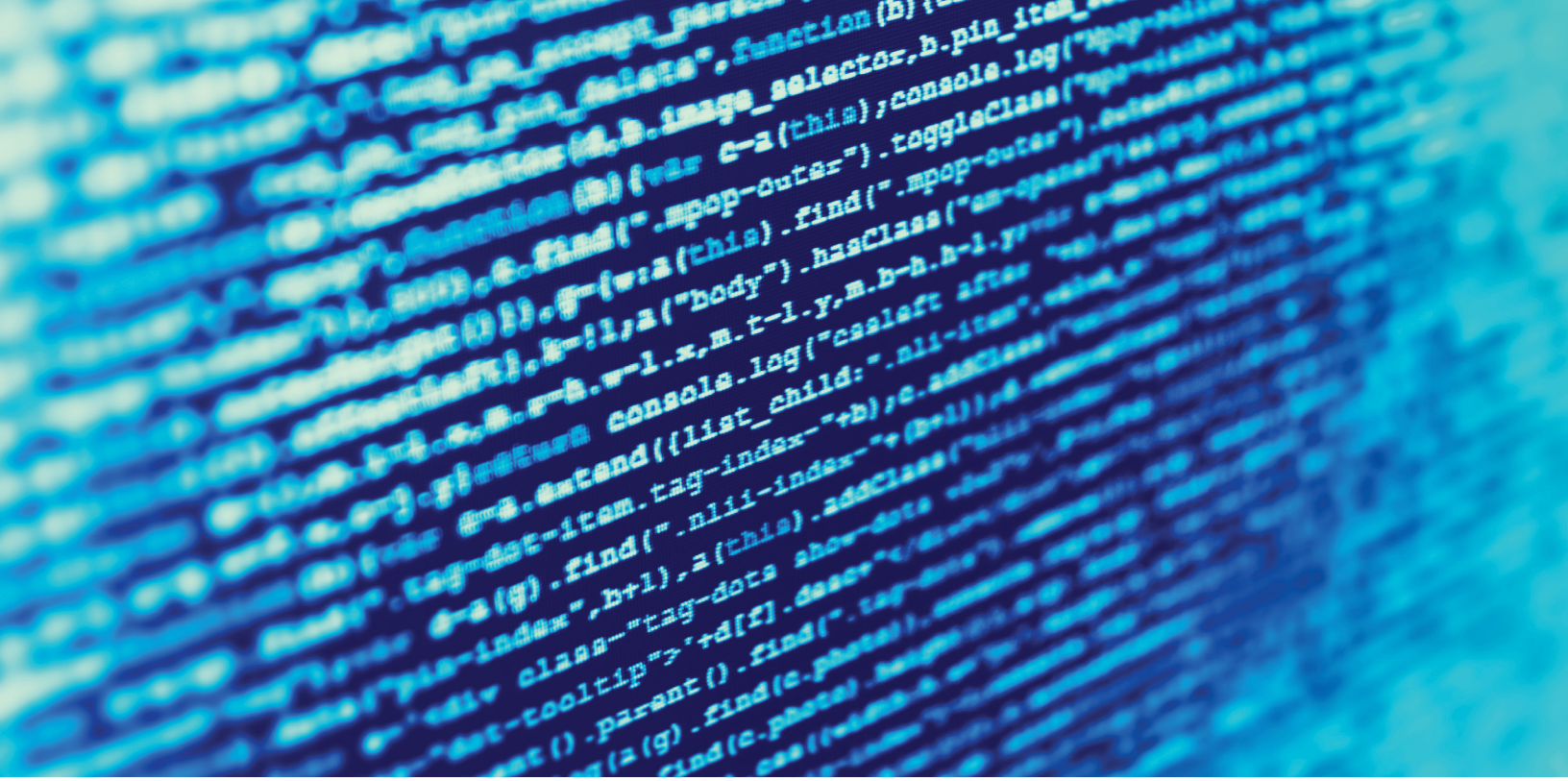
GREATER VANCOUVER

1011 Cordova St has two penthouse suites that are owned through a company registered in a Free Trade Zone in the United Arab Emirates. Their anonymous owner paid C$40 million for the apartments in 2013.

2531, 2925, 2999 and 3287 Point Grey Rd are all owned through express trusts, the beneficiaries of which are not disclosed.







5 The Case for a Public Registry of Companies and Trusts

TI Canada believes that the best way to address the numerous problems caused by the misuse of legal entities and arrangements is to create a publicly available registry that includes details on beneficial ownership. This low-cost, high-impact solution has the support of an extraordinarily broad coalition of stakeholders, and is already being implemented by several of the world's leading economies.

A public registry of companies, trusts and their beneficial owners would be of immense benefit to law enforcement, regulators, tax authorities, businesses, financial institutions, investors and the general public.

Among other benefits, an open, public registry would:

- **Cut red tape for law enforcement and speed up investigations.** Anonymous shell companies and nominees are a common obstacle for law enforcement, and cause many investigations to hit dead ends. If ownership information is only available on demand, or with a court order, criminals risk being tipped off. For cross-border investigations the current system of mutual legal assistance requests is time consuming and expensive, with even straightforward requests taking months, if not years. This has led to calls from public prosecutors[108] and law enforcement associations[109,110] for public registries that include beneficial ownership information.

- **Save the government money.** Anonymous companies and trusts deprive treasuries of billions of dollars in tax revenues each year, add considerable cost to law enforcement, and hinder asset recovery. When the US tabled legislation to require companies to disclose their beneficial owners, the Department of Justice and the Treasury were so supportive of the idea that they offered US$30 million to pay for its implementation.[111] The UK government[112] and the European Commission[113] conducted cost-benefit analyses and found that beneficial ownership registries could be a money saver. The UK study concluded that £30 million (about C$55 million) would be saved annually in police time alone, which would recover the cost of rolling out the policy change in its first year. Such efforts would also help to level the playing field, ensuring that responsible taxpayers do not shoulder the burden for those seeking to skirt the system. TI Canada encourages the Government of Canada to conduct a cost-benefit analysis of a central and publicly available registry of beneficial ownership information in order to better understand the economics of such a policy change in Canada.

- **Help the private sector meet its AML obligations.** Compliance with AML/TF regulations places a huge cost on reporting entities. A public registry would enable financial institutions and other regulated businesses and professionals to more effectively meet their AML/TF obligations while cutting costs.[114,115] The largest banking associations in the US[116] and Europe[117] are in favour of beneficial ownership registries, and executives at leading Canadian banks have expressed frustration with the current lack of transparency. The Chief Anti-Money Laundering Officers of two of Canada's largest banks have publicly acknowledged that their institutions are often unable to independently verify beneficial ownership information – a shortcoming attributed to the absence of publicly available data on beneficial ownership.[118] A public registry would enhance Canada's AML/TF regime, enabling reporting entities (including DNFBPs with limited resources) to conduct due diligence and verify beneficial ownership information.

- **Enable better investments and business decisions.** Most businesses and investors conduct due diligence before engaging with a third party. Doing so reduces the risk of violating laws, damaging their reputation and making poor decisions based on a lack of information. In a 2016 survey by consultancy EY, 91 percent of senior executives stated that it was important to know who beneficially owns the companies they do business with.[119] This opinion is shared by a group of institutional investors managing over US$740 billion,[120] and by a coalition of international business leaders,[121] both of which have called for laws mandating beneficial ownership disclosure.

- **Enhance trust and confidence.** By introducing a public registry with beneficial ownership information, the government would enable journalists, academics and civil society to scrutinize who owns companies and other legal structures. A public registry would reduce corruption and improve the functioning of high-risk sectors such as public procurement and lobbying. It would enhance Canada's reputation both internationally and at home, and improve public trust in government.

The benefits derived from beneficial ownership disclosure will be much greater if that information is made public in an open format. This can be done while preserving privacy rights and personal security, and without being burdensome on Canadian businesses and professionals.

- **Privacy.** TI Canada believes that a central public beneficial ownership registry can function while ensuring that legal rights to privacy are upheld, and would welcome more research in this area to determine the appropriate balance. In order for a registry to be effective, companies and trusts should be required to disclose the full name, nationality, government identification number and address of each beneficial owner. No more information than necessary should be collected. Personal data such as social insurance numbers should not be made public, nor should any documentation used to verify identity. A precedent for such a system exists in the UK, where residential addresses, identification numbers and complete dates of birth are kept from public view.

- **Security.** Criminal extortion is exceedingly rare in Canada. Disclosure of beneficial ownership information would not suddenly make wealthy individuals targets for extortion. Personal details such as government identification and street addresses would remain private in corporate registries, as would financial statements for private companies. Nonetheless, a tightly defined exemption for those with legitimate security concerns could be included in legislation.

- **Red Tape.** Making beneficial ownership information public will not involve much red tape. The responsibility for disclosure should rest with the directors of legal entities and the trustees of legal arrangements. Canadian companies are already required to keep records of their shareholders. Shareholders and beneficial owners are the same for the vast majority of privately owned companies – around 99 percent of them by some official estimates[122] – so the added disclosure requirements will not be a burden to them.

6 Recommendations

Beneficial ownership disclosure is not a silver bullet, but it is a key measure that is urgently needed to address the scourge of corruption and other crimes. There are several steps that the Canadian government can take to meet its international commitments to improve transparency, enable more effective law enforcement and tax collection, and deter the corrupt from using Canada as a safe haven.

Key Recommendation:

The Government of Canada should work with the provinces to establish a central registry of all companies and trusts in Canada, and their beneficial owners. The registry should be available to the public in an open data format. Corporate directors and trustees should be responsible for submitting beneficial ownership information and keeping it accurate and up to date.

Recommendations to Government and Law Enforcement

Companies

- All government authorities in Canada should require beneficial ownership disclosure as a prerequisite for companies seeking to bid on public contracts.
- Companies should be required to submit a contact form and official photo identification for each director, officer and beneficial owner upon incorporation and at the time of any change of control/ownership. This personal data should be kept securely by the applicable corporate registry and shared with the authorities when required.
- Corporate registries should be given adequate resources and a mandate to independently verify the information filed by legal entities, including the identities of directors and shareholders. Registries should be granted authority to apply sanctions for non-compliance with reporting requirements.
- Nominee directors and shareholders should be identified as such in corporate filings. They should be required to name the natural person on whose behalf they are acting. Nominees should keep contact details for that individual and ensure they are accurate and up to date.
- The Government of Canada should revise the *Canada Business Corporations Act* to eliminate bearer shares and instruments. Existing bearer shares should be converted to registered shares. The same should be done in any province that still permits bearer instruments.

Trusts

- Trustees should be required to keep accurate and up-to-date information on settlors and beneficial owners. They should be obliged to provide tax and law enforcement authorities with information related to any trust, regardless of that trust's confidentiality provisions.
- The Government of Canada should set up a central registry of trusts that identifies beneficiaries, settlors and trustees. This information should be made available to the public, after appropriate measures are taken to protect personal data.

Real Estate

- Beneficial ownership information should be included on property title documents, and no property deal should be allowed to proceed without that disclosure. In cases where a property is held through a nominee, this should be explicitly stated and the identity of the beneficiary should be disclosed.

- The Government of Canada should amend the PCMLTFA and associated regulations to make it mandatory for all reporting sectors – including real estate professionals – to identify beneficial ownership before conducting transactions.

Sanctions and Enforcement

- The Government of Canada should establish and apply dissuasive and proportionate sanctions for non-compliance with beneficial ownership disclosure. Those sanctions should include both criminal and civil penalties, and should be applied to ensure that beneficial ownership information is truthful, accurate and filed in a timely manner. Reporting obligations – and sanctions for non-compliance – should focus on those in control of legal entities and arrangements (i.e. directors and trustees) as well as beneficial owners themselves.

- Law enforcement and regulatory authorities should be more active in enforcing and punishing PCMLTFA violations by real estate professionals. Efforts should be taken to ensure that real estate professionals prioritize their AML compliance obligations.

- The Government of Canada should work to ensure that members of the legal profession (and Quebec notaries) are included in Canada's AML/TF regime in a constitutionally compliant manner.

References

1 OECD. "Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes," 2001.

2 StAR. "Puppet masters: how the corrupt use legal structures to hide stolen assets and what to do about it," 2011.

3 Sam Rubenfeld, "Amended complaint in Obiang case details alleged corruption," The Wall Street Journal, June 13, 2012.

4 UNODC, "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes," October 2011, (p.5).

5 FATF, "Money laundering and terrorist financing through the real estate sector," June 29, 2007, (p.12).

6 US Senate Caucus on International Narcotics Control, "The Buck Stops Here: Improving US Anti Money Laundering Practices," April 2013, (p.11).

7 "Spaniard Lopez Tardon sent to prison for 150 years in Miami money-laundering case," *The Miami Herald*, September 29, 2014.

8 US FBI, "A horse farm of a different color," June 28, 2013.

9 Oxfam, "Ending the era of tax havens," March 14, 2016, (p.12).

10 Harvey Cashore et al, "Canada Revenue offered amnesty to wealthy KPMG clients in offshore tax 'sham,'" *CBC News*, March 8, 2016.

11 United States of America v. Scott W. Rothstein.

12 Louise Shelley and Sharon Melzer, "The nexus of organized crime and terrorism: two case studies in cigarette smuggling," *International Journal of Comparative and Applied Criminal Justice*, Spring 2008.

13 Matt Robinson, "A $35 billion stock, an SEC halt and suspicions of market manipulation," *Bloomberg*, August 15, 2016.

14 Stephanie Ostfeld, "Shell game: hidden owners and motives," *CNN*, September 11, 2012.

15 Global Witness, "An idiot's guide to money laundering," April 10, 2013.

16 FACT Coalition, "Anonymous US 'shell' corporations: a national security Code Red," 2011. Transparency International UK, "Corruption on your doorstep: How corrupt capital is used to buy property in the UK," February 2015.

17 G8 Lough Erne Declaration, June 2013.

18 "G20 High-Level Principles on Beneficial Ownership Transparency."

19 Transparency International, "Just for show? Reviewing G20 promises on beneficial ownership," November 2015, (p.53).

20 Transparency International, "Canada: beneficial ownership transparency," November 2015.

21 Department of Finance Canada, "Assessment of inherent risks of money laundering and terrorist financing in Canada," August 2015.

22 Transparency International, "Just for show? Reviewing G20 promises on beneficial ownership," November 2015, (p.53).

23 European Commission, Directive (EU) 2015/849, May 20, 2015.

24 European Commission, "Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering," July 5, 2016.

25 US Congress, "Incorporation Transparency and Law Enforcement Assistance Act," 2015-2016.

26 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016.

27 Government of Canada, "Anti-Corruption Summit London 2016 Canada country statement," May 2016.

28 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.14).

29 Public libraries typically require proof of address and photo identification. No corporate registry in Canada asks for either.

30 Sharman et al, "Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies," 2013, (p.24).

31 The US market is dominated by incorporation agents, which have particularly low standards when it comes to collecting data on their clients. However, the study found that US lawyers were more compliant with international standards than their Canadian counterparts.

32 Robert Crib and Marco Chown Oved, "How offshore banking is costing Canada billions of dollars a year," *The Toronto Star*, April 4, 2016.

33 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.104).

34 Ibid.

35 Sidhartha Banerjee and Peter Rakobowchuk, "291 witnesses, 2,756 documents, 66,000 pages of testimony and 30 months later, Quebec corruption inquiry is finally over," *National Post*, November 14, 2014.

36 Jason Magder, "Fake invoices cost millions: Revenue Quebec," Montreal Gazette, March 11, 2014.

37 Ibid.

38 This data was obtained from employees at the provincial and territorial corporate registries, and in some cases from other government agencies. It could not be independently verified.

39 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (pp.25, 105).

40 Ibid. (pp.168-169)

41 Ibid. (p.208)

42 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (pp.51).

43 Ibid. (pp.168-169)

44 Transparency International, "Canada: beneficial ownership transparency," November 2015.

45 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.105).

46 Ibid. (p.8)

47 James Areddy, "China's most-wanted tries to make a final deal," *Wall Street Journal*, March 16, 2015.

48 The declaration of RCMP Cpl. Dave Armstrong can be viewed on the *Wall Street Journal* website.

49 Ibid.

50 Ibid.

51 Transparency International, "Just for show? Reviewing G20 promises on beneficial ownership," November 2015, (p.51).

52 Bill C-25, "An Act to amend the Canada Business Corporations Act, the Canada Cooperatives Act, the Canada Not-for-profit Corporations Act, and the Competition Act."

53 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.20).

54 Ibid. (p.105)

55 Canada (Attorney General) v. Federation of Law Societies of Canada, 2015/SCC/7.

56 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (pp.3, 15).

57 Ibid. (p.33)

58 R. v. Rosenfeld, 2009/ONCA/307.

59 Cyndee Todgham Cherniak, "Canadian lawyer receives harsh sentence for money laundering," April 23, 2009.

60 Betsy Powell, "Toronto lawyer Simon Rosenfeld goes to jail," The Toronto Star, March 9, 2009.

61 Paul Waldie, "Lawyers said key to money laundering," The Globe and Mail, March 18, 2005.

62 R. v. Rosenfeld, 2009/ONCA/307.

63 Paul Waldie, "Lawyers said key to money laundering," *The Globe and Mail*, March 18, 2005.

64 Julian Sher, "Money laundering going largely unpunished in Canada," *The Globe and Mail*, June 27, 2011.

65 Reporting entities, which include financial institutions, money transfer businesses, life insurance companies, accountants, securities dealers, real estate professionals, casinos, and dealers of precious metals and stones, among others.

66 FINTRAC, "Guideline 6G: Record keeping and client identification for financial entities," July 2016, (pp.38-41).

67 FINTRAC, "Regulations," SOR/2013-15.

68 Julian Sher, "Money laundering going largely unpunished in Canada," *The Globe and Mail*, June 27, 2011.

69 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.3).

70 Julian Sher, "Money laundering going largely unpunished in Canada," *The Globe and Mail*, June 27, 2011.

71 FACT Coalition, "Anonymous US 'shell' corporations: a national security Code Red," undated.

72 Federal Law Enforcement Officers Association, "Supporting transparency and law enforcement," August 1, 2013.

73 Fraternal Order of Police letter to Senator Carl Levin, July 16, 2013.

74 G8 Lough Erne Summit, "G8 action plan principles to prevent the misuse of companies and legal arrangements," June 2013.

75 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.36).

76 Ibid.

77 Sunny Freeman, "Anti-money laundering watchdog's secrecy a disservice to Canadian banking industry, advocate says," *The Toronto Star*, April 7, 2016.

78 FINTRAC, "Departmental performance report 2014-2015.

79 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.209).

80 Ibid. (p.98)

81 For instance, "CMHC: Foreign condo ownership concentrated in downtown Toronto" and "Chinese investment in Canadian real estate set to increase in 2016," *The Globe and Mail*, April 13, 2016.

82 FINTRAC, "Deter and Detect Money Laundering and Terrorist Financing: FINTRAC Annual Report 2014," (p.12).

83 Mike Hager, "Potential solutions to deal with tax evasion in real estate market," The Globe and Mail, September 18, 2016.

84 Department of Finance Canada, "Assessment of inherent risks of money laundering and terrorist financing in Canada," 2015, (p.32).

85 FATF, "Anti-money laundering and counter-terrorist financing measures: Canada mutual evaluation report," September 2016, (p.16).

86 Cassidy Olivier, "$31.1-million Point Grey mansion owned by student," Vancouver Sun, May 12, 2016.

87 Andrew Yan, "Ownership patterns of single family homes sales on the west side neighborhoods of the City of Vancouver: a case study," November 2015.

88 Stephen Schneider, "Money laundering in Canada: An analysis of RCMP cases," Nathanson Centre for the Study of Organized Crime and Corruption, March 2004.

89 Sam Cooper, "Suspect in murder of West Vancouver tycoon gave $14K to B.C. Liberals, donations records suggest," *The Vancouver Sun*, April 17, 2016.

90 Sam Cooper, "Tycoon slain in West Vancouver linked to bribery scandal," The Vancouver Sun, April 13, 2016.

91 Brian Hutchinson, "'I assume you want to kill me?: The mysterious life and death of millionaire murder victim Gang Yuan," *National Post*, June 12, 2015.

92 Lisa Rossington, "Money battle brewing after grisly murder at West Vancouver mansion," *CTV News*, May 20, 2015.

93 Jason Proctor, "Gang Yuan dismembered millionaire case: mothers plead for anonymity," *CBC News*, September 2, 2015.

94 Kathy Tomlinson, "Out of the shadows," *The Globe and Mail*, September 13, 2016.

95 Special purpose property holding companies may be accompanied by “bare trusts,” which are legal arrangements that enable a property to be managed for (and in many cases by) a beneficial owner without their name appearing on title.

96 Transparency International UK, “Corruption on your doorstep: How corrupt capital is used to buy property in the UK,” February 2015.

97 Louise Story and Stephanie Saul, “Stream of foreign wealth flows to New York real estate,” *The New York Times*, February 7, 2015.

98 Richard Weiland, “The naked truth about trusts,” November 2009.

99 FINTRAC, “Trends in Canadian suspicious transaction reporting,” October 2011. Alexandra Posadzki, “FINTRAC finds ‘ very significant’ deficiencies at realtors in money laundering probe,” *CBC News*, September 14, 2016.

100 Transparency International, “Just for show? Reviewing G20 promises on beneficial ownership,” November 2015, (p.44).

101 Department of Finance Canada, “Assessment of inherent risks of money laundering and terrorist financing in Canada,” 2015.

102 Alexandra Posadzki, “FINTRAC finds ‘very significant’ deficiencies at realtors in money laundering probe,” *CBC News*, September 14, 2016.

103 FINTRAC, “Indicators of money laundering in financial transactions related to real estate,” November 2016.

104 Alexandra Posadzki, “FINTRAC finds ‘very significant’ deficiencies at realtors in money laundering probe,” *CBC News*, September 14, 2016.

105 FINTRAC, “Penalties for non-compliance.”

106 The offshore companies are registered in the British Virgin Islands (2), Hong Kong (1), and Dubai’s Jebel Ali Free Zone (1).

107 Title documents often list the occupation of the titleholder. Those who declared their occupation as “student,” “homemaker,” or “housewife” were assumed to be nominees.

108 Carolyn B. Maloney press release, “Maloney and Vance call on Congress to stop anonymous terrorist and criminal shell corporation money laundering in New York City,” March 7, 2016.

109 Federal Law Enforcement Officers Association, “Supporting transparency and law enforcement,” August 1, 2013.

110 Fraternal Order of Police letter to Senator Carl Levin, July 16, 2013.

111 US Senate Caucus on International Narcotics Control, “The Buck Stops Here: Improving US Anti Money Laundering Practices,” April 2013, (p.25).

112 HM Treasury/DTI, “Regulatory impact analysis: disclosure of beneficial ownership of unlisted companies”, July 2002 (updated for Global Witness in 2013).

113 European Commission, “Cost benefit analysis of transparency requirements in the company/corporate field and banking sector relevant for the fight against money laundering and other financial crime,” February 27, 2007.

114 Transparency International, “Ending secrecy to end impunity: Tracing the beneficial owner,” 2014.

115 Open Society Foundation, “Terrorism, Inc: How shell companies aid terrorism, crime and corruption,” 2013.

116 Open letter to US Senate from The Clearing House Association, August 8, 2016.

117 European Banking Federation, “EBF position on the report from the European Commission to the European Parliament and the Council on the application of directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing,” June 12, 2012, (p.6).

118 Matthew McGuire, “Clearing up transparency: Beneficial ownership verification in Canada,” 2014.

119 EY, “Global Fraud Survey 2016: Combating corruption as a global priority,” 2016.

120 Global Witness, “Investors managing over $740 billion call for transparency over American company owners,” September 7, 2016.

121 The B Team, “The business case for ending anonymous companies,” January 15, 2015

122 HM Treasury/DTI, “Regulatory impact analysis: Disclosure of beneficial ownership of unlisted companies,” July 2002.

TRANSPARENCY INTERNATIONAL CANADA

Follow us on Twitter @TI_Canada

/company/transparency-intl-canada

/TransparencyInternationalCanada

transparencycanada.ca

Appendix 12

RECBC – *Anti-Money Laundering in Real Estate Course* – April 1, 2020

← Continuing Education

Anti-Money Laundering in Real Estate

Real estate professionals can play an important role in keeping proceeds of crime out of BC real estate markets.

COVID-19 RECBC EDUCATION UPDATE →

GO TO

MANDATORY FOR: ALL REAL ESTATE PROFESSIONALS

Anti-Money Laundering in Real Estate

RECBC's *Anti-Money Laundering in Real Estate* course is designed to give you the tools and knowledge you need to help prevent illicit funds from entering our real estate markets. By staying current and informed on anti-money laundering requirements and best practices, you can ensure that consumers are well-protected, and that the public can have confidence in BC's real estate industry.

Register Now

Appendix 12

Pricing

$100

Learn more about why RECBC has developed the course, and the impacts of money laundering in real estate, in this brief video with Erin Seeley, CEO of RECBC, and Peter German, author of the *Dirty Money* reports and an authority on anti-money laundering policies in Canada.

Course Overview

Who Must Take the Course

All licensed real estate professionals with licences expiring on or after April 1, 2020 are required to complete the Anti-Money Laundering in Real Estate course. Whether you are a representative, an

associate broker or a managing broker and whether you provide trading services, rental property management services or strata management services, you'll learn valuable information about preventing money laundering in this new course.

What You Will Learn

This self-paced online course gives you the information you need to understand why real estate is attractive to money launderers, how to identify red flags for money laundering, and the steps to take to report suspicious transactions.

Most importantly, you'll learn how to incorporate that knowledge into real actions that you can practice in your business. As a real estate professional, you are uniquely positioned to identify and report suspicious transactions because of your close working relationship with clients.

When to Take the Course

We encourage you to take the course as soon as possible within your two-year licensing period. Completion of the course is required in order to renew a licence beginning April 1, 2020.

Course Cost

For a limited time, save on the course fee.

Registration Dates	Price
April 1 — June 30, 2020	**$50**
after June 30, 2020	$100

** All real estate professionals are eligible to take advantage of the Anti-Money Laundering in Real Estate Course course promotional pricing. Anyone who registers for the course during this promotional period and successfully completes the course will be able to use it towards satisfying the continuing education requirements for their next licence renewal occurring on, or before, March 31, 2022.*

Course fees must be paid upon registration.

Course revenues support the development of further educational resources and courses to enhance your knowledge and support you to comply with regulatory requirements.

Course Length

Anti-Money Laundering in Real Estate is an online course that can be completed at your own pace over a three day period. In most cases, it is estimated the course will require a total of 3.5 hours

to complete.

The course must be completed within three days of registering, or the learner will be required to re-register.

Course Details

Developed in collaboration with anti-money laundering experts, the course is available through the Real Estate Division at UBC. It is a mandatory continuing education course for all licensed real estate professionals in BC. We thank FINTRAC for their support in this project.

Module 1	Introduction and Money Laundering Basics
Module 2	Background on the Anti-Money Laundering Regime
Module 3	Real Estate and Money Laundering
Module 4	Overview of Compliance Obligations
Module 5	Suspicious Transactions
Module 6	Emerging Issues

The course includes videos and knowledge check questions within each module. You will have three days from the start date you select in order to complete the course.
You must complete all course modules AND obtain a passing grade of at least 70% on the final assessment.

Once you have passed the final assessment, you will receive a course completion letter.

Registration Details

REGISTER NOW

(1) Registration for *Anti-Money Laundering in Real Estate* is online through the UBC Sauder School of Business website.

Have your licence number and UBC Real Estate Division student ID number (if you have one) ready when you register for the course. Find your licence number using our Find a Professional search page.

(2) On the registration page, select a start date that suits your schedule from the list of available

dates. You'll have three days from the start date you select in which to complete the course.

(3) This is an online course that you can take at your own pace over a three day period and should take 3-5 hours to complete.

Once your registration has been processed, you will receive a confirmation email from the UBC Sauder School of Business with details for accessing the online course.

Email Us

Email us for more information about our Continuing Education courses.

Email

Phone Us

Monday to Friday 8:30 AM to 4:30 PM.

Phone: 604.683.9664

Toll-free: 1.877.683.9664

Fax: 604.683.9017

Related Links

Renewing Your Licence →

Legal Update Course →

Ethics for the Real Estate Professional Course →

Appendix 12

We regulate real estate professionals
in the public interest.

Our offices are located on traditional Coast Salish territory of the Musqueam, Squamish, and Tsleil-Waututh Nations.

ABOUT US →

QUICK LINKS

REPORT A CONCERN →

FIND A PROFESSIONAL →

KNOWLEDGE BASE →

CAREERS AT RECBC →

PROFESSIONAL LOGIN →

WHERE WE ARE

Real Estate Council of British Columbia
900-750 West Pender Street
Vancouver, BC V6C 2T8
604.683.9664
Toll-free: 1.877.683.9664

Appendix 13

BCREA – *BCREA Launches FINTRAC Action Plan* – Sept 1, 2018

BCREA Launches FINTRAC Action Plan

Sep 01, 2018

CATEGORY: **Advocacy** **BCREA**
TAGS: **FINTRAC**

Posted by
April van Ert
Communications Manager

BCREA has launched a new action plan in collaboration with member boards to support REALTORS® and managing brokers in better understanding and meeting their FINTRAC reporting duties to help keep the proceeds of organized crime out of the housing market. We have also increased our collaboration with CREA and government partners to prepare for more scrutiny of real estate's vulnerability to criminal activities.

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Advocacy

- COVID-19
- Strata Properties
- Mortgages
- Standard Forms
- Disclosure
- Strata Property Act

Popular posts from BCREA

Applications for

In August, BCREA began working with CREA and FINTRAC to gather more information on where managing brokers and REALTORS® may be falling short of their compliance duties. Using this information, BCREA will develop online and in-person training resources in collaboration with member boards. FINTRAC will also make a presentation at **BCREA Advocacy Exchange: Conference for Managing Brokers** on September 19.

Clarifying myths around FINTRAC compliance is an important element of the action plan. This fall, BCREA will work with member boards to plan and co-host an editorial board meeting with Lower Mainland media to educate them on the steps REALTORS® and managing brokers already take to comply with federal requirements. This is part of a broader campaign to build public confidence in BC's 23,000 REALTORS®.

At the government relations level, BC Attorney General David Eby has indicated he will order a review of money laundering in real estate. BCREA is actively working to

BC Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

ensure that review—when it's ordered—is fair and balanced.

BCREA's action plan is still in the early stages and there is a lot of work ahead to prepare for these coming challenges. BCREA looks forward to working with CREA, member boards, managing brokers and REALTORS® to increase support and be a strong advocate for the profession.

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 1(West Georgia St.
Vancouver, E V6E 3C9

Phone 604.683.7702
Toll Free 1.844.288.7702
Fax 604.683.8601
Emai bcrea@bcrea.bc.ca

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Discounts ▸

About BCREA ▸

Sign up and stay informed

Enter your

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Appendix 13

Appendix 14

BCREA – *Real Estate Transparency to Build Public Confidence* – Nov 1, 2018

Real Estate Transparency to Build Public Confidence

Nov 01, 2018

CATEGORY: Advocacy

TAGS: **Anti-Money Laundering** **Real Estate Practice**

Posted by
Matt Mayers
Policy Analyst

SHARE THIS

PRINT

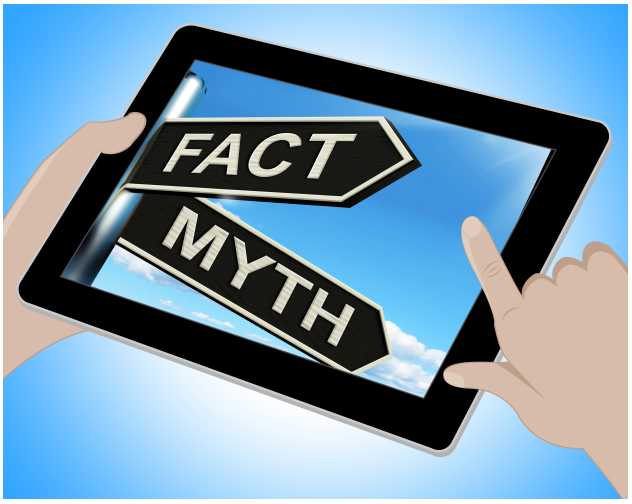
What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

On September 27, Attorney General David Eby and Minister of Finance Carole James announced a two-pronged approach to review money laundering in real estate. BCREA shares the government's concerns about potential vulnerabilities, and we immediately reached out to offer insights into both reviews.

Popular tags within Advocacy

- COVID-19
- Strata Properties
- Mortgages
- Standard Forms
- Anti-Money



For 18 years, REALTORS® have been subject to federal anti-money laundering regulations through the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Real estate offices already take steps to see that proceeds of crime don't enter the real estate market, including:

- appointing compliance officers,
- providing ongoing training to REALTORS®,
- conducting risk assessments every two years at a minimum, and

Popular posts from BCREA

Real Estate Professionals Urged to Stop Open Houses: Regulators and Provincial Association Recommend Virtual Tools

Nov 05, 2020

Applications for BC Emergency Benefit for

- verifying the identities of clients.

To help REALTORS® meet their obligations, the Canadian Real Estate Association has considerable resources, and BCREA recently revised an online course about the federal regulations. We continue to work with FINTRAC to identify opportunities to continue to improve compliance.

Similarly, we look forward to providing input to Peter German and Maureen Maloney as they conduct their investigations, with both initiatives expected to complete in March 2019. Carefully determining whether and where vulnerabilities lie in real estate transactions will help make sure the government makes effective policy decisions and that consumers can have confidence in the market.

Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

The Expert Panel on Money Laundering, led by Maureen Maloney is accepting submissions until December 14. Check out the **consultation website**.

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

Phone 604.683.7702
Toll Free 1.844.288.7702
Fax 604.683.8601
Email bcrea@bcrea.bc.ca

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Benefits ▸

About BCREA ▸

Follow Us

Sign up and stay informed

Enter yo

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Appendix 14

Appendix 15

BCREA - *BCREA Supports BC Government's Money Laundering Investigations* – Nov 27, 2018

BCREA Supports BC Government's Money Laundering Investigations

Nov 27, 2018

CATEGORY: News Releases
TAGS: **Anti-Money Laundering**

Posted by
April van Ert
Communications Manager

Vancouver, BC – November 27, 2018. As the provincial association for BC's 11 regional real estate boards and 23,000 REALTORS®, the British Columbia Real Estate Association (BCREA) is deeply concerned by a recent news report that suggests up to $1 billion may have been laundered through Vancouver luxury real estate in 2016. BCREA continues to support the provincial

government's ongoing efforts to understand money laundering vulnerabilities in real estate transactions.

"Since we learned earlier this summer that BC's real estate sector may be used in money laundering activities, we've been working aggressively with government and other partners to help support investigations into organized crime," said BCREA's Chief Executive Officer Darlene Hyde.

BCREA supports the government's fight against organized crime

In July, BCREA learned that BC brokerages and REALTORS® were having trouble understanding and meeting their reporting duties to Canada's Financial Transactions and Reports Analysis Centre (FINTRAC). BCREA responded quickly to help REALTORS® better meet their compliance responsibilities.

"As the report says, money laundering is a complex problem and recognizing when sophisticated international crime syndicates – who are experts at fraud and deception – are at work behind the scenes takes significant resources," noted Hyde. "At BCREA, we are ready to make our contribution to keeping BC's economy safe from organized crime and we have committed to assisting the government."

Here are the steps BCREA has already taken:

- Invited FINTRAC to speak to more than 250 brokers and REALTORS® about understanding and meeting their compliance obligations at our first ever managing brokers conference.

- Updated the BCREA course on real estate transactions and

Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

FINTRAC reporting.

- Created targeted communications to REALTORS® addressing issues around FINTRAC reporting and compliance.
- Proactively approached the provincial government to assist in their inquiry into real estate's vulnerabilities to organized crime.
- Requested the opportunity to participate in the Ministry of Finance's Expert Panel on Money Laundering in Real Estate.
- Encouraged BC's 23,000 REALTORS® to participate in the government's money laundering investigations through their online and telephone hotlines.

- Promoted the government's request for public participation into its inquiries through our own social media platforms.

BCREA will continue to ensure public trust

While BCREA has not received any reports of REALTORS® being complicit in money laundering, we continue to support the government's investigations into this serious issue. Any REALTOR® found to be knowingly complicit with money laundering should be held accountable to provincial professional standards, criminal codes and to the REALTOR® Code of Ethics. As the voice of BC's REALTORS®, we look forward to continuing to assist the government and ensuring the public can have full confidence in the REALTOR® profession.

-30-

Click here for the PDF.

For more information, please contact:

April van Ert

Communications Manager

Email: **avanert@bcrea.bc.ca**

604.742.2797

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Email bcrea@bcrea.bc.ca

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Benefits ▸

About BCREA ▸

Follow Us

Sign up and stay informed

Enter yo

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Appendix 16

BCREA – *The Role of Realtors in Helping the Government Stop Money Laundering*

British Columbia Real Estate Association

THE ROLE OF REALTORS® IN HELPING THE GOVERNMENT STOP MONEY LAUNDERING

REALTORS® ARE COMMITTED TO HELPING IDENTIFY AND STOP MONEY LAUNDERING.

FACT. REALTORS® and real estate brokerages do their part to support Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) by completing regular training and risk assessments, reporting suspicious transactions, verifying client and third-party identification and flagging any other concerns.

REALTORS® REGULARLY RECEIVE LARGE AMOUNTS OF CASH FROM BUYERS.

FICTION. The only funds REALTORS® ever receive from buyers is the deposit and the majority of BC's real estate brokerages will only accept bank drafts to protect their brokerage from criminal exploitation.

REALTORS® ARE JUST ONE PIECE OF THE PUZZLE WHEN IT COMES TO STOPPING MONEY LAUNDERING.

FACT. REALTORS® help the government fight money laundering by verifying a buyer's identification and meeting other FINTRAC duties, but more needs to be done to understand where real estate may be vulnerable to organized crime.

FINTRAC IMMEDIATELY FOLLOWS UP WITH A REALTOR® WHO REPORTS A SUSPICIOUS TRANSACTION.

FICTION. Once a suspicious transaction report is filed, a REALTOR® will likely never know how FINTRAC uses the report. The information may be used in future investigations, or their suspicions may end up being unjustified.

FINTRAC WILL STOP A SUSPICIOUS REAL ESTATE TRANSACTION ONCE IT'S BEEN REPORTED.

FICTION. After a REALTOR® reports a suspicious transaction, the transaction continues and it is up to FINTRAC to identify the next steps.

REALTORS® AND BROKERAGES HAVE PRECAUTIONS IN PLACE TO HELP PROTECT THEM AND THEIR CLIENTS FROM MONEY LAUNDERING.

FACT. Brokerages have comprehensive compliance programs and in-house compliance officers to make sure they stay on top of their FINTRAC responsibilities. The compliance officer oversees ongoing training for REALTORS® and completes a brokerage risk assessment every two years.

THERE'S A CLEAR UNDERSTANDING OF HOW EFFECTIVE GUIDELINES ARE IN KEEPING ORGANIZED CRIME OUT OF BC REAL ESTATE.

FICTION. BC's government is trying to better understand where real estate may be vulnerable to organized crime. The British Columbia Real Estate Association is working with them to identify opportunities to better protect British Columbians.

Appendix 17

BCREA – *Getting to the Bottom of FINTRAC Compliance* – Jan 16, 2019

Getting to the Bottom of FINTRAC Compliance

Jan 16, 2019

CATEGORY: **Advocacy**
TAGS: **Anti-Money Laundering** **BCREA Managing Brokers' Conference** **Compliance** **FINTRAC** **Managing Brokers** **Proceeds of Crime (Money Laundering) and Terrorist Financing Act**

Posted by
Marianne Brimmell
Communications Specialist

Answers to your burning questions

The wait for responses from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to managing brokers' top questions submitted at the Conference for Managing Brokers is over!

During the conference, attendees

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Advocacy

- COVID-19
- Strata Properties
- Mortgages
- Standard Forms
- Disclosure
- Strata Property Act

Popular posts from BCREA

Applications for

submitted questions to the presenters and voted for the questions they most wanted answered. Responses to three burning questions submitted to FINTRAC are given below. The rest of the responses from FINTRAC can be found **here**.

1. **Why all the FINTRAC pressure on our industry when banks control the flow, not REALTORS®?**
   FINTRAC administers the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its associated Regulations, to which a number of sectors are subject. We provide outreach and assistance to all of these sectors and have developed guidance on each sectors' obligations with respect to the implementation of a compliance program, ascertaining identification, record-keeping, and, as applicable, reporting to FINTRAC.

   That said, the exploitation of real estate by criminals for money laundering purposes is well recognized internationally and underscores the importance of quality reporting on relevant suspicious transactions. Many countries are increasing their efforts to implement

BC Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

counter measures following the Financial Action Task Force (FATF)'s work on this topic indicating that the real estate sector is highly susceptible for many reasons: for example, easy price manipulation and a variety of complex options for selling/purchasing/financing with anonymity.

It is important to recognize that the real estate brokers and sales representatives are uniquely positioned to be able to assess aspects of the transaction that other entities involved may not be aware of. While the actual flow of funds for the purchase of real estate may involve financial entities, it is the real estate brokers and sales representatives that have a relationship with the participants to the transactions. Furthermore, financial institutions may under-report because of an erroneous belief that brokers/agents/developers have already submitted suspicious transaction reports. For example, the suspicions surrounding deposits for a purchase may be primarily visible to and reported by real estate agents,

brokers and developers, whereas those related to loans may be more visible to and reported by financial institutions.

2. **How can we build a proper FINTRAC compliance program if each auditor has a different perspective on many of the grey areas?**
   To ensure that we exercise professional judgement in a consistent manner, we rely on our collective knowledge, experience, training, and standardized assessment approach, while taking into account the nature, size, and complexity of different businesses. Compliance officers strive to provide clear and consistent explanations of the examination findings, and guidance to facilitate your understanding of your legislative obligations, as well as of FINTRAC guidelines, policies, and procedures. Finally, all examination findings go through a peer review and managerial approval process to further ensure consistency.

   As such, what might appear to be different perspectives on grey areas may actually be a result of the

different considerations used – e.g., compliance history, the size of the reporting entity, the way a particular reporting entity sets out responsibilities in its policies and procedures.

3. **How can FINTRAC tell us to not rely on the CREA FINTRAC compliance guidelines and related FINTRAC content? Are they incorrect?**
FINTRAC encourages industries and industry associations to develop products on which the reporting entities within a sector may base their compliance program. However, these products may be intentionally general so as to be applicable, at a high-level, across the industry. As such, a real estate broker or sales representative may be able to use CREA's guidelines and content, but must consider whether it is specific enough for its purposes, and applicable given how its entity functions on a day-to-day basis.

Please click **here** for the rest of the responses from FINTRAC. Thank you to FINTRAC for presenting at the Conference

for Managing Brokers and for providing these great responses!

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 1(West Georgia St.
Vancouver, E V6E 3C9

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Emai bcrea@bcrea.bc.ca

Appendix 18

BCREA – *Understanding Money Laundering Vulnerabilities* – Feb 13, 2019

Understanding Money Laundering Vulnerabilities

Feb 13, 2019

CATEGORY: BCREA

SHARE THIS PRINT

A chain is only as strong as its weakest link

In support of the provincial government's initiatives to curb money laundering in real estate, the British Columbia Real Estate Association (BCREA) has commissioned the consulting firm Deloitte to study residential and commercial transactions. The goal of this study is to identify money laundering vulnerabilities throughout the transaction chain—not just when REALTORS® are involved.

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular posts from BCREA

Real Estate Professionals Urged to Stop Open Houses: Regulators and Provincial Association

Our advocacy actions have earned us a "seat at the table" since July 2018 when Peter German released an independent review of money laundering in Lower Mainland casinos. As the voice of BC's REALTORS®, our commitment to actions such as this study demonstrates the profession's integrity and what REALTORS® are doing to keep the proceeds of organized crime out of real estate. At the same time, we're clearly communicating existing obligations and advocating for careful, meaningful policy changes.

Recommend Virtual Tools
Nov 05, 2020

Applications for BC Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

The vulnerability study will also help identify gaps in federal and provincial regulations and highlight opportunities to improve REALTOR® best practices. Deloitte is assessing vulnerabilities throughout both residential and commercial transactions. From the beginning to the end, Deloitte is considering every transaction stage.

Deloitte has now completed their work, and we'll submit our findings to Peter German's Review of Money Laundering and Maureen Maloney's Expert Panel at the end of February.

As money laundering continues to be in the public eye, we're working hard to provide additional resources that dispel the misconceptions around REALTORS® and money laundering while helping REALTORS® better understand and meet their compliance duties. If you

haven't seen our latest resource showing how REALTORS® help identify and stop money laundering, **click here**.

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Email bcrea@bcrea.bc.ca

Follow Us

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Benefits ▸

About BCREA ▸

Sign up and stay informed

Enter yo

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Appendix 18

Appendix 19

Deloitte Presentation to BCREA – *Assessing Money Laundering Vulnerabilities in the BC Real Estate Sector* – Feb 22, 2019

Deloitte LLP
Bay Adelaide East
8 Adelaide Street West
Suite 200
Toronto ON M5H 0A9
Canada

Tel: +1-416-775-8851
www.deloitte.ca

February 22, 2019

Private and confidential

Ms. Darlene K. Hyde, CEO
British Columbia Real Estate Association
Vancouver B.C.
Canada

Subject: B.C. Real Estate Money Laundering Vulnerability Assessment

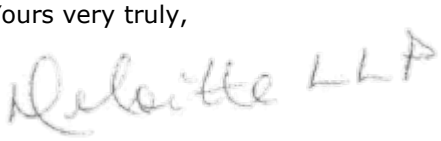
Dear Ms. Hyde:

Attached is our report setting out our observations and recommendations.

Our observations and recommendations are based on the work undertaken as described in the Objectives and Background section of this report and are subject to the restrictions and limitations in scope as set out therein.

Should you have any questions or concerns, please do not hesitate to contact me at 416-775-8851.

Yours very truly,



Christine Ring
Partner
Deloitte LLP

Deloitte.

B.C. Real Estate Association

Assessing Money Laundering Vulnerabilities in the B.C. Real Estate Sector

February 22, 2019

Contents

Introduction

Introduction
Objectives and Background

The British Columbia Real Estate Association ("BCREA") engaged Deloitte LLP ("Deloitte") for assistance in identifying vulnerabilities for money laundering in the B.C. commercial and residential real estate market based on research and interviews. Furthermore, BCREA is seeking recommendations for federal, provincial regulatory improvements, practice changes and opportunities to address the vulnerabilities.

Deloitte's procedures included conducting open source media searches and interviewing a volunteer group of nine B.C. real estate agents and managing brokers from both the residential and commercial sectors, all of whom operate in the B.C. real estate market.

In addition to the restrictions and limitation outlined in this document, the observations and resulting recommendations made were limited to the information provided by the interviewees and research; no attempt was made to corroborate this information with other individuals party to a potential real estate transaction, such as lenders, lawyers or notaries.

The B.C. real estate industry is served by over 23,000 registered REALTORS®. Licensees can become members of the B.C. Real Estate Association (BCREA) and the Canadian Real Estate Association (CREA).

Of B.C.'s 11 real estate boards, Greater Vancouver and Fraser Valley boards have the higher number of unit sales in 2017 and forecasted unit sales in 2018 and 2019[1].

BCREA provides continuing professional education, advocacy, economic research and standard forms for their members.

Except in limited circumstances outlined in the B.C. Real Estate Services Act, sales of real estate in B.C. for or in expectation of remuneration except by licensed REALTORS® is prohibited.

Licensees are typically representatives that are engaged by a real estate brokerage; any business that a representative conducts must be in the name of and on behalf of the brokerage.

[1] BCREA Housing Forecast, Fourth Quarter, November 2018

Introduction

Money Laundering in the B.C. Real Estate Industry

Media reports and public outcry over residential affordability in the Vancouver area in the last few years have raised concerns over the risk of money laundering in the real estate sector, especially in transactions involving foreign funds. While media reports have identified questionable sources of foreign funds which have allegedly fueled price increases, money laundering can occur as well from domestic funds and regardless of whether there are increases to real estate prices.

Canada's 2015 National Risk Assessment[1] assessed real estate agents and developers to be highly vulnerable to money laundering and terrorist financing, due to potential exposure to high risk clients and the ability to obscure beneficial ownership and source of funds.

In September 2016, the FATF[2] issued a mutual evaluation report on Canada's anti-money laundering and counter-terrorist financing measures which identified that real estate agents were "not sufficiently aware of their AML/CFT obligations", which was exhibited through the relatively small number of STRs filed and the perception of low risk "because physical cash is not generally used in real estate transactions."

However, the exposure to money laundering in real estate is not attributable only to realtors; Transparency International identified severe deficiencies or significant loopholes that increased the risk of money laundering in real estate or implementation and enforcement of the law. One of the limitations was that AML provisions do not include lawyers, law firms, or notaries from Quebec, a key role in the closing of real estate transactions.[3]

[1] Department of Finance Canada (2015). *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. Retrieved from https://www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp#

[2] Financial Action Task Force, the inter-government body whose mandate is to examine and develop measures to combat money laundering and terrorist financing.

[3] Transparency International (2017). *Doors Wide Open: Corruption and Real Estate in Four Key Markets.* p.18.

Introduction

Money Laundering in the B.C. Real Estate Industry (continued)

AML Regulations on Real Estate

In Canada, real estate brokers and sales representatives (collectively, "Representatives") are considered to be "Designated Non-Financial Business and Profession" (DNFBP) and reporting entities of FINTRAC[1], Canada's financial intelligence unit. Other DNFBPs include accountants, casinos, dealers in precious metals and stones and B.C. notaries.

The AML legislation requires that Representatives, with the exception of agents acting on behalf of a Broker, are required to implement an anti-money laundering/anti-terrorist financing (collectively, "AML") compliance regime and report certain transactions.[2]

Private real estate sales are not included in the AML legislation and therefore do not require any AML requirements.

FINTRAC reported that of the 130 examinations conducted on the B.C. real estate sector between 2015 and 2017, 88% of those had 'significant' or 'very significant' deficiencies in meeting the legislative requirements.[3] Non compliance with these requirements may result in imprisonment, criminal fines or administrative penalties.

To assist Representatives with complying with the AML legislation, CREA has published several documents. These documents, including templates and forms, require tailoring and completion by the real estate representatives in order to meet the requirements.

[1] Financial Transactions and Reports Centre of Canada

[2] Financial Transactions and Reports Centre of Canada (2019, January). *Real estate developers, brokers and sales representatives*. Retrieved from http://fintrac.gc.ca/re-ed/real-eng.asp

[3] Fumano, Dan (2018, July 29). 'Significant or very significant': Analysis shows money-laundering vulnerabilities in B.C. real estate. *Vancouver Sun.* Retrieved from https://vancouversun.com

Introduction

Money Laundering in the B.C. Real Estate Industry (continued)

B.C. Real Estate Market

Public and media attention in recent years have identified Canada to be a haven for 'snow-washing', the laundering of dirty funds using loopholes in the Canadian regulatory system, including the lack of requirements to disclose the beneficial ownership when incorporating companies. This ability was cited as an opportunity for disguising dirty funds in Transparency International's investigation on the Vancouver luxury real estate, when they identified 46% of the luxury homes were owned by through domestic and offshore shell companies, trusts and nominees.[1]

[1] Transparency International Canada (2017). *TI Canada Investigation Into Vancouver Luxury Real Estate.* Retrieved from http://www.transparencycanada.ca/wp-content/uploads/2017/02/TIC-Infographic-VancouverLuxuryRealEstate-WEB.pdf

Introduction
Key Findings and Observations

Based on our interviews and observations, we noted the following:

- That there is a difference in the perceived available information compared to the actual information available to the real estate agent during a transaction with respect to identifying potential money laundering and/or terrorist financing. As a result, some realtors disagree with the legislative AML responsibilities of the realtor.
- There continues to be a perception by realtors that because they generally do not handle cash, they are therefore not exposed to money laundering, however, the realtor's knowledge of the client purchasing or selling real estate is a crucial piece of information to the real estate transactions process, as it is information that is generally not available to other parties to the real estate process.
- The brokerage's compliance officer relies heavily on real estate agents to fulfill the Know-Your-Client requirements, including the client risk rating and ongoing monitoring in order to meet the AML requirements. In other AML-regulated industries, such as banking or securities, the client risk rating and ongoing monitoring are performed centrally and/or managed by the compliance officer to ensure a consistent approach across the organization.
- With respect to the 'cost' of transacting with a potential money launderer or criminal, realtors that operated in a "community-based" brokerage were generally more concerned about damaging their personal reputation.

Overview

Overview
AML Legislative Requirements

Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) requires Representatives to maintain a "comprehensive and effective compliance program" with the following:

- Appointment of a compliance officer;
- Application of policies and procedures;
- Documented assessment of risks;
- Development of a training program; and
- Review of compliance program every two years.

As part of the compliance program, the Broker also needs to perform the following:

- Know-Your-Client procedures (regardless of whether the realtor is acting for the buyer or seller), as follows:
  - Obtaining certain client details;
  - Verifying the client's identity, such as reviewing ID;
  - Determining the involvement of any third parties; and
  - Conducting ongoing monitoring and client risk rating
- Reporting to FINTRAC, for the following transactions:
  - Suspicious transactions;
  - Terrorist property; and
  - Large cash transactions.

Overview
Our Approach

We were asked to identify the vulnerabilities to money laundering in both the residential and commercial real estate transaction processes. In particular, we were asked to consider the associated vulnerabilities, including:

- The parties involved at different stages of the purchase or sale of property;
- Valuation of the property;
- Methods used to identify the clients;
- Payment methods; and
- Geographic locations.

At the request of BCREA our approach did not include a review of the data from any specific real estate transactions.

As part of our work, we were also asked to:

- Map the real estate transaction process, and identify the vulnerabilities at each stage of the transaction;
- Provide recommendations on practice changes for REALTORS® and other professionals;
- Recommend federal and/or provincial regulatory improvements; and
- Identify opportunities to address the vulnerabilities.

Overview

Real Estate Transaction Process

Our interviews identified that the residential and commercial real estate transaction processes were both similar, generally differing in the use of the property. More subtle and specific differences were identified in the size of the brokerage and geographic client base.

In the client real estate transaction process, the real estate agents AML requirements are primarily during three stages:

- Knowing the client (regardless of whether this is the buyer or seller) – Profile and determine the reasonableness of the client's information.
- Real Estate Purchase/Sale – When acting in a purchase or sale, the client identification record must be completed by verifying the client's identity and obtaining client details, including involvement of third parties, client risk level and business relationship monitoring.
- Deposit – Recordkeeping details and reporting to FINTRAC is required only when the realtor receives cash of $10,000 or more in a single or multiple transactions that total $10,000 or more within a 24-hour period.

Overview

Real Estate Transaction Process

There are multiple parties and professionals in each real estate transaction that have sight on a crucial piece of the process. However a systemic risk in the nature of these transactions is that no single party may be involved in the entire real estate transaction process.

An inherent gap is that besides the client, no single party has sight to the entire real estate transaction, whether that is residential or commercial.

This makes identifying any potential laundering of funds challenging.

Observations and Vulnerabilities

Observations and Vulnerabilities

Real Estate Transaction Process

- Interviewees identified that clients are generally introduced by word-of-mouth and that this is a relationship business with few risks identified. Risks identified are more about the client's ability to purchase; realtors with residential clients are concerned about those that were not serious about a purchase while those with commercial clients indicated that there is risk that the individual they are transacting with does not have approval to make decisions to buy or sell the property. In other cases, realtors mentioned "gut feeling" and the flexibility to walk away from any transaction if it "didn't feel right".

- Realtors with commercial clients identified a more frequent, ongoing relationship where they sometimes performed multiple transactions for the client throughout the years. Accordingly, there is good knowledge and little associated risks with these clients. Some interviewees with residential clients also note instances of higher initial risk due to the client being out of town; these were subsequently rated as low risk when there was knowledge that the client was selling a second home.

- The timing of the client identification and the requirement to "FINTRAC" (to meet the legislative requirements, such as identifying the client) the client varies by brokerage policy and the realtor's preferences; some brokerages require the realtor to complete the KYC (Know-Your-Client) forms and identify the client at the outset, with the chance that the forms are completed and ultimately no transaction is performed. Others mentioned that they saw the requirement to be a good business practice; that hesitation to provide ID would indicate that the client was not serious and was wasting the realtor's time.

Continued on next page

Observations and Vulnerabilities

Real Estate Transaction Process

Continued

- Verification of the individual's ID is primarily in-person, reviewing the individual's government-issued ID, some of which were foreign passports, with a photocopy being taken. In the rare instance where this is not possible due to the client being in B.C. but outside of driving distance, realtors have the client identified through an agent, asking the client to attend a realty brokerage that was close to the individual. Realtors mention that other brokerages, even from another franchisor, were usually cooperative in assisting with identifying a client and sending copies of the information to the realtor. No other client identification methods were mentioned in our discussions.

- With respect to clients from foreign jurisdictions, this is generally not perceived to be a risk as it is understood that "Canada has a good economy and people will generally try to come here." Local market conditions and differences were also understood as well, in one instance, providing examples of clients that are purchasing a second property.

- One interviewee with compliance officer duties indicated that in his experience, they noted that realtors did not ask and/or include in the form whether the transaction was conducted on behalf of a third party.

- However, another realtor mentioned that he always had knowledge as to who the buyer is through their interaction. Examples included a local representative acting on behalf of a foreign head office, representative from an ownership group and housing for a student purchased by a parent or spouse overseas.

Continued on next page

Observations and Vulnerabilities

Real Estate Transaction Process

Continued

- Interviewees indicate that the client risk rating process was understood and none had encountered any medium or high risk clients; however, the process to risk rate clients appear to be used as a measure of working with the client as opposed to the money laundering risk posed by the client. This was further elaborated that if the realtor did not feel comfortable working with the client, the realtor would not accept them, regardless of whether it was an individual or entity.

- Most interviewees recalled the suspicious transaction indicators published by FINTRAC but there were varying views of the usefulness of the indicators: some realtors agreed on the importance of having the indicators to remind them to be aware of money laundering risk where other interviewees disagreed with being "deputized to do the government's job".

Observations and Vulnerabilities

Real Estate Transaction Process

- Residential properties considered to be higher risk were development flips, pre-sale flips, short term re-sales and assignments as those individuals may not be paying tax on the assignment. Realtors that identified this as a risk mitigated their risk by generally not being involved in those types of transactions.
- Commercial realtors noted that higher risk properties were those that included the sale of the operations and business; where buyers are required to conduct their own due diligence, there was a risk on the accuracy of the financial information portrayed, as there were "so many ways to hide money". The realtor we spoke to also noted some small businesses that attempted to increase the value of their business by indicating they paid themselves cash; a potential for undeclared income. This realtor mitigated his risk by not taking on these types of transactions, however, the realtor also shared that the level of experience selling businesses by real estate agents varies, having come across residential realtors with little commercial experience attempting to sell businesses.
- Property valuation was not identified as a risk as a formal appraisal was usually required by the lender.

Observations and Vulnerabilities

Real Estate Transaction Process

- None of the realtors we spoke to identified any instances of non-cash exchange between the buyer and seller, through other assets, such as virtual currency. However, one agent identified instances of homes being exchanged.

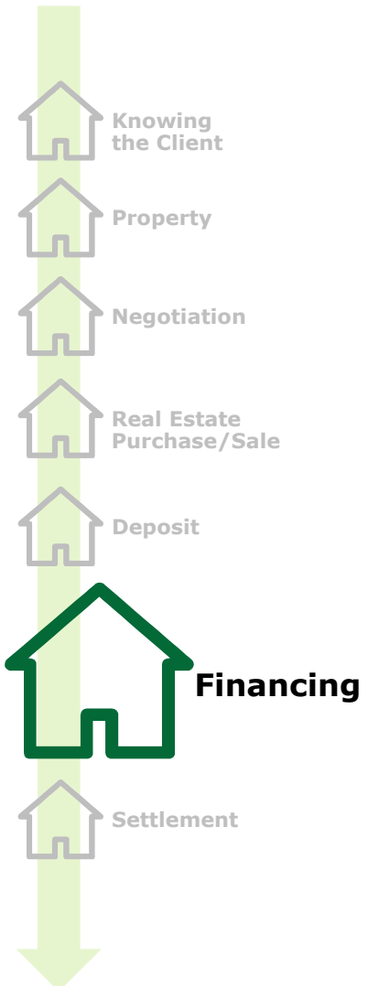
Observations and Vulnerabilities

Real Estate Transaction Process

- Most of the realtors we spoke to indicated that their brokerage has a strict policy to not permit cash. Furthermore, all deposits are required to be paid by certified cheque or bank draft issued by a Canadian financial institution, even if the client is not from Canada. One realtor provided an example where a US cheque was rejected by their managing broker.
- Only in one instance was a realtor approached with $4,000/$5,000 in cash, accordingly there was no requirement to report anything as it did not meet the $10,000 threshold.
- Several interviewees said that it is an unjust requirement for the realtor to identify potential money laundering; the realtor has line of sight to only 5 to 10% of the purchase price (from the deposit) which comes from a Canadian financial institution. The original source of the funds in the financial institution account would be known and better understood from the financial institution's transaction records.
- Interviewees also indicated their expectation on the financial institution to identify the source of funds for the deposit.

Observations and Vulnerabilities

Real Estate Transaction Process



- Interviewees shared that in general, financing of the property is between the client and the lender, which includes mortgage brokers and private lenders. Several realtors mentioned being aware of mortgage brokers or alternative lenders however expectations were mixed: some expected that due to working relationships, they would be notified by a broker if there was something that did not appear consistent or reasonable. Others indicated that it was not their job to arrange funding and did not want or care to know about their clients' income.
- One commercial real estate broker identified that in addition to typical lenders, they identified instances of funding from syndicate loans and crowd funding; in these instances, it was not clear where the money is sourced from. In general, they saw financing as a transactional risk that is not generally inquired about by the realtor.
- It was also mentioned that mortgage brokers and lenders would have better knowledge of the source of funds, if financing is required, which is with most transactions.

Observations and Vulnerabilities

Real Estate Transaction Process

- One realtor observed that "realtors don't sell property, they construct real estate sales" and that the sales is happening at lawyers' and notaries' offices.
- Accordingly, a number of interviewees criticized the lack of regulations on lawyers since the lawyer saw the transaction, the source of the property's funding, the ability to conduct property searches and the ability to detect and report activity within the domain of lawyers.

Observations and Vulnerabilities Groupings

Process and Requirements

These observations and vulnerabilities were identified based on the Representatives' requirements to meet the legislative AML requirements, including the implementation of a compliance program.

Knowledge and Education

We observed and identified gaps in knowledge and education of money laundering risks that exposes the real estate industry to money laundering risk.

Enforcement and Discipline

While it is expected that the large majority of REALTORS® operate ethically and according to the requirements, we identified vulnerabilities that related to enforce~~ment~~ and disciplinary actions.

External to Real Estate

We were informed of and became aware of risks with sectors that were party to the real estate activities but external to the real estate sector.

Observations and Vulnerabilities
Process and Requirements

Appointment of Compliance Officer

Observations

- Interviewees perceived that their respective organization's AML compliance regime was strong, citing attention to detail in the review of documentation, especially as it relates to the KYC (Know-Your-Client) documents.
- In most instances, the compliance officer was the managing broker of the business and therefore was responsible for reviewing and approving all transactions. One interviewee indicated that in her office, the monitoring was supported by junior clerical staff to complete an initial review of the completion of documents.
- While the compliance officer understands his or her responsibilities, in some instances, there was a deferment of responsibility to the individual sales agent. As well, the role appeared to be more focussed on compliance than management of potential money laundering risk. For instance, the review appears to be based on whether the occupation field is completed as opposed to whether it is reasonable based on the transaction.

Potential Vulnerabilities

- The knowledge and experience of the compliance officer varies across organizations, with differing expectations and levels of resources to devote to meeting the requirements. While larger organizations may have more resources to monitor compliance with the requirements, the compliance function does not have the insight of frontline real estate sales and purchase client behaviour and activity. In those instances, inexperienced compliance personnel will rely more heavily on the sales agent to identify high risk transaction, clients and suspicious activity.
- The managing broker has a dual role of ensuring sales growth and managing client risk which places the managing broker in an inherent conflict with their responsibilities.
- Risk of money laundering may not be adequately monitored by the compliance officer.

Observations and Vulnerabilities

Process and Requirements (continued)

Appointment of Compliance Officer (continued)

Observations

- While there were no recollection of any transactions that had been denied by the compliance officer, some individuals identified examples of questions being raised on the parties to the transactions.
- The experience and expectations of the compliance officer varied, with more knowledgeable compliance officers having been previously examined by FINTRAC.

Observations and Vulnerabilities

Process and Requirements (continued)

Application of Policies and Procedures

Observations

- The compliance officers we spoke to used or relied on CREA-prepared AML policies and procedures documentation and client transaction forms.
- An interviewee recalled that at a recent presentation, a FINTRAC representative indicated that the realtor did not require overly-complex AML policies and procedures and that it could be "as simple as one page". The interviewee indicated that, based on this, it wasn't clear why the CREA-prepared document was so long and "unnecessarily complex".
- In most cases, client identification is performed using the face-to-face identification method or through the agency method. Agency was performed through other realtor companies, local to the client.
- The requirement to conduct ongoing monitoring of client transactions is not well understood; CREA documentation has provided guidance but the completion of the monitoring is a 'checklist' process.

Potential Vulnerabilities

- Using a checklist process for ongoing monitoring may not adequately review for and identify high risk and suspicious behaviour.
- While CREA-prepared AML documentation is designed to assist realtors in complying with the requirements, it is not clear whether compliance officers and realtors understand the requirements to tailor the documentation to their brokerage.

Observations and Vulnerabilities

Process and Requirements (continued)

Application of Policies and Procedures (continued)

Observations

- Some interviewees indicated that their company required clients to be identified up-front, while other shared that this was a good measure to ensure that the client was serious about performing a transaction, instead of wasting the realtor's time.
- Compliance officers interviewed did not have a system in place to monitor ongoing client relationships, relying on recollecting the name.
- Based on the CREA forms, most clients are assessed by realtors as low risk. Even where clients posed higher initial risk, such as the nature of their occupation, realtors indicated that the client would be assessed as lower residual risk when they subsequently received satisfactory information. Some interviewees assessed risk interchangeably between money laundering and credit or fraud risk.

Potential Vulnerabilities

- It is technically difficult, if not impossible, for compliance to recall every client name for the purposes of monitoring client relationships.
- CREA-created documentation may not be conducive to identifying more high-risk clients. There is lack of clarity as to whether this is based on inherent risk (that is risk before any controls or further information) or whether this is residual risk, after the performance of mitigating measures (such as making further inquiries).

Observations and Vulnerabilities
Process and Requirements (continued)

Application of Policies and Procedures (continued)

Observations

- Some commercial realtors expressed annoyance that commercial realtors are subject to the same requirements given that it appeared that the problem stemmed from residential real estate.
- One interviewee mentioned that as part of their client screening process, they requested corporate documentation and beneficial ownership information to ensure the individual had the authority to contract property.

Potential Vulnerabilities

- Current requirements treat the residential and commercial real estate sectors as operationally similar; as a result, commercial broker operations may be overlooked to provide relevant money laundering vulnerabilities and suspicious indicators.

Observations and Vulnerabilities

Process and Requirements (continued)

Documented Assessment of Risks

Observations

- Realtors often identified examples of high risk that were unlikely to occur; for example, clients with large amounts of cash.
- When asked about other potential instances of high risk, interviewees frequently identified clients that did not have financing in place and could not afford the property.
- Some realtors identified unusual instances including one example from a few years ago where clients that were particularly interested in basements, alluding to a potential to operate an illegal marijuana grow-op.
- As a DNFBP, the brokerage is required to maintain a documented assessment of risks; it was not clear how day-to-day operations of a brokerage was used to inform the overall assessment of risk, including, for example, whether a brokerage had the same client performing residential and commercial transactions and what the associated risks are (i.e. if they are assessed as a high risk commercial client, are they also assessed as a high risk residential client).

Potential Vulnerabilities

- Lack of understanding of money laundering compared to business risk can result in failure to identify and report suspicious activity.
- Lack of resources to ensure documentation and understanding of money laundering risks specific to the brokerage could result in a failure to implement controls that mitigate risk.

Observations and Vulnerabilities

Process and Requirements (continued)

Development of a Training Program

Observations

- All interviewees indicated that they had good knowledge of the requirements. There were some interviewees that indicated that despite this knowledge, it was not clear to them why realtors were being targeted, especially in light of other sectors such as lawyers and bankers.
- Some interviewees indicated that they had received formal AML training from UBC's Sauder School of Business as well as training sessions by CREA and BCREA. Some compliance officers also indicated that they regularly used the FINTRAC website as refresher of the requirements.
- All interviewees had mentioned they had received training, however training within the realty brokerage varies: Some brokerages provided in-person regular training sessions or regular meetings where compliance is discussed. One brokerage's training consisted of asking realtors to sign an acknowledgement that they had reviewed and understood the AML policies.

Potential Vulnerabilities

- The ability to identify suspicious transactions will vary, depending on the experience of the compliance officer and realtor, as well as the training provided by the brokerage. According to AML legislation, there is also no minimum threshold of training required to be completed by realtors.

Observations and Vulnerabilities

Process and Requirements (continued)

Review of Compliance Program

Observations

- When asked about their last effectiveness review of the brokerage's AML compliance regime, some compliance officer indicated that they had been examined by FINTRAC while in one instance, the compliance officer indicated that there was a process of self-review.
- Some realty brokerages identified that despite having been in operation for a number of years, they had never been examined by FINTRAC.
- However, all interviewees identified that there was a strong AML compliance program, including that there was a review process in place before completion of the transaction.

Potential Vulnerabilities

- Lack of quality effectiveness reviews means that shortcomings in the brokerage's AML compliance regime may not be identified. Furthermore, there is a lack of opportunity to address and continuously improve.

Observations and Vulnerabilities

Process and Requirements (continued)

FINTRAC Reporting

Observations

- All interviewees mentioned that their brokerage had a policy to not accept cash and they have never accepted or been offered cash. Accordingly, none of the interviewees have encountered any requirement to report large cash transactions.
- One interviewee questioned why the realty industry should be tasked with the responsibility to determine whether the client is sanctioned or a terrorist, especially when they received no compensation for "doing the government's job".
- Some interviewees mentioned that there was a concern that reporting suspicious transactions on a client would put them and their family at personal risk: "if I reported and the police show up at the person's door tomorrow, they're going to know who reported".

Potential Vulnerabilities

- Due to the lack of suspicious transaction reporting, it is not clear whether there are no suspicious transactions involving real estate or whether realty professionals are failing to identify and/or report activity that is considered reportable.
- Lack of understanding of the suspicious transaction reporting process leads to realtors not reporting all transactions that should be reported to FINTRAC.

Observations and Vulnerabilities

Knowledge and Education

Observations

- As noted above, a number of realtors struggled to understand why realtors were considered to be a reporting entity, especially when their brokerages were not permitted to receive or ever came across cash payments or saw the entire payment. All realtors indicated that their brokerages restrict fund receipts to deposit funds which were limited to payment by cheque, bank draft or wire transfer from a Canadian financial institution.

- Some realtors indicated that it was "not their job" to catch money laundering, indicating that it was their business to identify property and bring forward offers. When asked who's responsibility it is, some offered that it is the bank's responsibility as they see the source of the funds; or the lawyer, given that they close the transaction and receive the funds.

- A number of interviewees also indicated that there was a difficulty in asking a number of questions they determined were too personal, such as source of funds/wealth.

- Some commercial real estate representatives identified that sale of business is especially high risk, given that some smaller businesses may underreport earnings in the furtherance of evading taxes.

Potential Vulnerabilities

- Different expectations and disagreement over their core responsibilities as a reporting entity can lead to a failure to identify and report suspicious activity, especially if a realtor is looking for extreme examples of abnormal client behaviour as the baseline for suspicious activity.

- Failure to identify potential tax evasion as proceeds of crime leads to underreporting of suspicious transactions.

Observations and Vulnerabilities

Knowledge and Education (continued)

Observations

- One interviewee said that a FINTRAC representative "did not agree" with CREA's approach to the application of the requirements, however, no alternative approach for realtors to meet the requirements has been provided by FINTRAC.
- With respect to real estate peers, the following was mentioned:
  - That language barriers in some communities could lead to a lack of understanding of the requirements.
  - That intentionally "bad" real estate agents were limited to a few individuals.

Potential Vulnerabilities

- Lack of coordination between CREA and FINTRAC leads to confusion in the application of the requirements.
- Perceived or actual unfairness in the real estate marketplace and failure by the Real Estate Council of B.C. to uphold responsibilities.

Observations and Vulnerabilities
Enforcement and Discipline

Observations

- Some interviewees indicated that regulations were focussed on compliance as opposed to risk, and this penalized administrative errors without targeting bad realtors.
- For bad realtors, there was little repercussions from not following the rules and based on the fines, it was simply a cost of doing business.
- It was noted from the discussions that reputational risk varied, depending on the type of realtor; realtors that were community focussed were more concerned about reputational risk and being associated with questionable clients. Larger, commercial realtors did not see this as a concern.

Potential Vulnerabilities

- With the lack of fines and repercussions, there is less incentive to follow the rules and requirements.

Observations and Vulnerabilities
External to Real Estate

Observations

- Interviewees indicated that there were limitations to a realtors' knowledge of their client and the transaction, some of which would be better answered by other parties of the transaction. This limitation would include knowledge by the real estate agent working for the other side of the transaction. Other parties include:
  - Lawyer or notary, who would receive the remaining funds from the client.
  - Lender, which can be a financial institution, such as a bank or credit union that is regulated. Alternatively, the client may utilize mortgage brokers and/or alternative lenders, which may not be regulated by money laundering regulations. If the transaction does not require financing, a lender may not be involved in a transaction.
  - Financial institution, where funds are usually sourced from for the initial deposit.
  - Appraiser, although this is usually an individual determined by the lender.

Potential Vulnerabilities

- The realtor only has access to a part of the real estate transaction process; however, this is not dissimilar from other reporting entities and professionals that nobody has sight to everything. A lack of understanding of the realtor's role in identifying potential money laundering can result the rejection of the requirements.

Observations and Vulnerabilities
External to Real Estate (continued)

Observations

- FINTRAC – some interviewees expressed frustration that it wasn't clear what activity was considered suspicious and therefore reportable.

Potential Vulnerabilities

- Lack of clarity leads to inadequate identification and reporting of suspicious activity.
- Lack of understanding on the regulatory focus can result in realtors focusing their attention on areas that are not high risk. As well, perceived lack of fairness by regulators leads to disregard of the overall regulations.

Recommendations

Recommendations

Practice Changes for REALTORS and Other Professionals

- As a designated FINTRAC-reporting entity, the compliance regime management of the real estate brokerage needs to be enhanced. Specifically, these enhancements should include:
  - Expansion of the compliance officer role to include managing the brokerage's inherent risk for money laundering and terrorist financing. Current processes are focused on ensuring compliance, such that forms are completed and accurate. The risk management role requires the compliance officer to monitor and identify the brokerage's exposure to money laundering risk based on customer, geography, products and services offered, delivery channel and other factors. We recommend the following:
    - That CREA ensure that the AML documentation (i.e. the template compliance regime manual) reflects the expanded role to manage money laundering and terrorist financing risk for the brokerage.
    - That BCREA enhance the local training provided to the managing broker/compliance officers with respect to the money laundering risk management role and updated CREA documentation.
    - For brokerages, to ensure that the role and responsibilities are clearly defined. Compliance officers should also evaluate their companies' resources to manage this risk, which includes ensuring that there is sufficient knowledge to carry out these duties.
  - The compliance officer and managing broker role be separated, where possible, to avoid conflicts of interest. An independent compliance officer will have an unbiased position to review and provide insight. The managing broker is generally tasked with managing the operations of the brokerage and ensuring the profitability whereas the compliance officer's role is to protect and ensure that the brokerage is taking on only acceptable levels of risk; accordingly, there is an inherent conflict of interest in the same individual serving both roles. We recommend the following:
    - That CREA provide guidance on separating these roles; especially for larger and/or higher risk organizations.

Recommendations

Practice Changes for REALTORS and Other Professionals (continued)

- Enhanced collaboration within the realtor sector and with other AML-regulated sectors to allow further collaboration and information-sharing on best practices, regulatory updates and expectations. We recommend that:
  - Local real estate boards establish forums/ periodic meetings for compliance officers of brokerages to meet. Consider inviting local AML experts, regulators and law enforcement to provide insight on recent cases, issues or findings.
  - Compliance officers participate in industry AML knowledge sessions, such as ACAMS (Association of Certified Anti-Money Laundering Specialists), an international, not-for-profit organization devoted to advancing AML knowledge and skills, which can be accessed online or in-person at local ACAMS chapter events.
- Centralize the ongoing monitoring and client risk rating roles to ensure a consistent process. Based on the interviews, compliance officers rely on individual realtors to complete the KYC information, conduct ongoing monitoring and risk rate the clients (e.g. pages 3 and 4 of the Individual Identification Information Record). We recommend that real estate brokerages adopt an approach similar to other AML-regulated industries, where the client risk rating is centrally monitored and managed, based on information and input received from frontline personnel (i.e. the realtor). Similarly, we recommend that the compliance officer centralize the ongoing monitoring process, regardless of who (i.e. the individual agent) is providing services or the nature of services.
- To support the ongoing monitoring process, compliance officers need to enhance their documentation and review process: brokerages should be encouraged to maintain documentation and periodically review their client database and the client activity for patterns of transactions and activity. Where there are higher levels of activities, higher risk activity or transactions considered atypical to the client (or for the brokerage), there needs to be good analysis, review and documentation of the approach by the compliance officer to address the higher levels of risk.

Recommendations

Practice Changes for REALTORS and Other Professionals (continued)

- Enforce the requirement that all attempted suspicious, completed suspicious or unusual activity be reported to the compliance officer. Some interviewees shared examples of potential tax evasion by prospective clients – while these were ultimately rejected by the realtors involved for being high risk, these had not been reported to FINTRAC nor the compliance officer.

- Based on our interviews, we were informed that CREA risk assessment documentation has not been beneficial in meeting the needs to the brokerages and FINTRAC examinations: the AML legislation requires the brokerage to document an assessment of inherent money laundering and terrorist financing risks. The brokerage is also required to identify high risk clients, which is ideally supported using a client risk rating process that is aligned with the inherent risk assessment. Accordingly, to enhance the inherent risk assessment and client risk rating process, we recommend the following:

  - That CREA enhance their standardized template for inherent risk assessment to allow for greater modification. Currently, CREA has provided a standardized template rather than an approach that allows for risk customization and identification of other risks. Modifying the document to provide an approach and delivering training on the modification will increase the brokerages' understanding of money laundering/terrorist financing risks, particularly as it relates to the organization's exposure. As an example, the credit union industry has developed a risk assessment tool that each credit union may choose to adopt that assists the individual credit union with documenting and understanding their exposure to risk .

  - That CREA update the client risk rating process based on the above; the revised process should increase the number of higher risk clients being identified.

  - Furthermore, while individual realtors and representatives can continue to collect client information, the client risk rating process should be centralized with the compliance officer. This will ensure a consistent approach to client risk rating.

Recommendations

Practice Changes for REALTORS and Other Professionals (continued)

- To enhance the realtors' understanding of the legislative AML requirements, CREA should consider updating and providing AML documentation that specifically addresses commercial realtors and how commercial transactions can be used to launder proceeds of crime.
- Based on our interviews, it appears that there are instances where a self-review by the compliance officer is being performed to meet the biennial effectiveness review requirements. As such, we recommend the following:
  - That brokerages engage outside, independent reviews in order to provide more fulsome insight on the quality of their AML compliance programs.
  - Where brokerages have difficulty engaging an outside firm, that BCREA consider developing a review program for brokerages.
- For publicized cases of criminal activity, CREA or BCREA should, as a proactive measure, review and perform case analysis to identify whether there were any shortcomings on related real estate transactions, if applicable.
- Brokerages should also monitor past real estate transactions for known or alleged criminal activity and consider submitting a suspicious transaction report.

Recommendations

Federal and Provincial Regulatory Improvements

- Currently, not all professionals involved in a real estate transaction are regulated by FINTRAC, including lawyers and non-financial institution lenders, such as alternative and private lenders. To ensure that all relevant parties to a real estate transaction are subject to the same AML requirements, we recommend that lawyers, law firms, notaries from Quebec, and non-financial institution lenders be subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

- Furthermore, current legislation does not impose any minimum transaction requirements on private real estate sales (purchase and sales that do not involve a licensed real estate agent). We recommend that private real estate sales be subject to the PCMLTFA.

- We recommend that the Real Estate Council of B.C. (RECBC) conduct AML compliance assessments of brokerages . This could be conducted jointly with FINTRAC based on size, risk and complexity as well or solely by RECBC to increase assessment coverage of the sector. Under a memoranda of understanding, RECBC may also consider informing FINTRAC of potential AML regulatory issues identified as part of RECBC's reviews and investigations. For comparison purposes, we understand that certain provincial deposit insurance regulators will make inquires about a credit union's AML compliance program; their inquiries are used to ensure there is a minimum standard and to inform FINTRAC when a further, more detailed review is required.

- Where possible, CREA and BCREA should host industry dialogue with FINTRAC with the objective of industry information sharing and regime enhancement.

- We recommend that RECBC consider implementing enforcement action on brokerages and realtors that fail to meet AML requirements, such as a financial penalties, follow-up assessments, increased monitoring or license removal.

Recommendations

Education and Skills Development

- In addition to collaborating and interacting with AML professionals from other regulated sectors, as identified above, the compliance officer's training should include insight from experienced AML professionals. This will establish industry best practices and set a baseline for industry expectations.
- Consider providing training in other languages in addition to English, to better ensure realtors' understanding of the AML requirements.
- To increase the quality of licensees and dedication to the real estate profession, realtors should be subject to minimum annual employment hours and a minimum number of AML training hours. From an AML-knowledge perspective, this will ensure that part-time realtors are exposed to sufficient client activity in order to understand and identify suspicious transaction indicators. We note that other professional organizations, such as accountants, also require minimum hours.
- To ensure the understanding of AML requirements, that RECBC implement periodic, such as annual, AML testing. The testing should, at a minimum, focus on the AML requirements and potential risks and red flags for the real estate sector.

Restrictions

Restrictions

- Deloitte assumes no responsibility to update this draft report for events and circumstances occurring after the date of this report. We do not assume any responsibility for losses suffered by any party as a result of circulation, publication, or reproduction of this report contrary to the provisions of this paragraph.
- We reserve the right, but will be under no obligation, to review this report, and if we consider it necessary, to revise our report in light of any information, which becomes known to us after the date of this report.
- This report was prepared at the request of BCREA to assist with BCREA's process to identify vulnerabilities and recommendations. This report is not designed to identify all circumstances of potential inappropriate behaviour, irregularities, vulnerabilities or recommendations, if any, which may exist.
- This report has been based on the information, documents, and explanations that have been provided to us, and therefore the validity of any observations noted rely on the integrity of such information. We have not investigated the accuracy of any third-party information, nor have we performed any investigative procedures to independently verify the accuracy of any third-party information.
- Should any of the information provided to us not be factual or accurate, or should we be asked to consider different information or assumptions, any observations set out in this report could be significantly different.
- The report contains comments and observations based on the information identified in the sources set out herein. It is possible that different observations and comments may be summarized by another service provider. Deloitte cannot assume responsibility for the accuracy of the information obtained from these sources, nor can we guarantee that we will locate all relevant information that might exist regarding a certain subject. Our scope of review and limitations are outlined above.

Deloitte.

Appendix 20

BCREA – *Letter to Expert Panel on Money Laundering re BCREA Submission to Expert Panel* – March 4, 2019

BCrea
British Columbia
Real Estate Association

Suite 1425, 1075 West Georgia St
Vancouver, BC V6E 3C9
bcrea.bc.ca

March 4, 2019

Expert Panel on Money Laundering
Submitted by email: RealEstate.MoneyLaundering@gov.bc.ca

RE: British Columbia Real Estate Association submission to Expert Panel

The British Columbia Real Estate Association (BCREA), the professional association for BC's 11 real estate boards and 23,000 REALTORS®, is committed to supporting the government's efforts to better understand where real estate transactions may be vulnerable to money laundering.

Thank you for giving us extra time to make our final submission. When we met with you in December, we proposed a vulnerability assessment to examine typical residential and commercial real estate transactions, and that work is now complete. With this letter, we offer you the findings of that research plus recommendations.

Vulnerability assessment

BCREA commissioned Deloitte to identify vulnerabilities for money laundering in BC commercial and residential real estate transactions. To understand typical transactions, Deloitte conducted interviews with nine BC REALTORS® and carried out a search of open source media. However, Deloitte did not corroborate the information provided and found.

Key findings:

- There is a difference in the perceived available information compared to the actual information available to the REALTOR® during a transaction with respect to identifying potential money laundering and/or terrorist financing.
- Many REALTORS® perceive that, because they generally do not handle cash, they are not exposed to money laundering; however, the REALTOR®'s knowledge of the client buying or selling real estate is a crucial piece of information to the real estate transaction, because it is information not available to other parties.

- REALTORS® operating in "community-based" brokerages are typically more concerned with the reputational risk of transacting with potential money launderers or criminals than those in brokerages that are less connected to their communities.
- An inherent existing gap is that, besides the client, no single party sees the entire real estate transaction. Real estate transactions involve not just REALTORS® but also notaries, lawyers, appraisers and mortgage brokers. That makes identifying any potential laundering of funds challenging.
- Residential properties considered to be high risk include pre-sale assignments and short-term resales.
- Commercial properties considered to be high risk include the sale of operations and business, especially when one party is unrepresented, because there are many ways to hide money by underreporting income.
- In general, financing of properties is between the client and the lender, which includes mortgage brokers and private lenders. REALTORS® are simply not involved with that aspect of the transaction.
- The fact that lawyers are not subject to Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) requirements is a significant gap.
- The overwhelming majority of brokerages do not accept cash deposits.
- Even though both roles are often performed by the same person, managing brokers are tasked with ensuring sales growth and managing client risk, while FINTRAC compliance officers are focused on monitoring money laundering and terrorist financing risk.
- The real estate brokerage's compliance officer relies on REALTORS® to identify, rate risks and conduct ongoing monitoring of clients to meet anti-money laundering (AML) requirements.
- REALTORS® would benefit from focused training and resources to help them create effective policies and procedures, separate money laundering risks from business risks and identify suspicious transactions.
- Canada's *Proceeds of Crime (Money Laundering) and Terrorist Finance Act* and regulations do not set any minimum threshold of training.
- Inconsistency in FINTRAC examinations causes confusion for REALTORS®.

As a result of the vulnerability assessment and many conversations with REALTORS® and real estate boards, BCREA is placing significant emphasis on training and education.

We are hiring a temporary contractor—an AML specialist—to focus on anti-money laundering issues, including developing resources, liaising with CREA, FINTRAC and

other reporting entities, answering questions from REALTORS® and providing training.

BCREA is already developing training for FINTRAC compliance officers to increasingly foster and maintain a culture of compliance. We understand the Canadian Real Estate Association (CREA) is updating existing resources, which will be incorporated into our training.

Best practices

Through our AML specialist, workshop and other communications methods, we will reinforce best practices. Real estate brokerages vary widely, and the best practices listed below are general in nature. Each brokerage will have to adapt these best practices based on their specific context.

BCREA's 11 real estate boards commit to work towards the following best practices:

- Brokerages avoid accepting cash deposits aside from exceptional circumstances.
- Educating brokerages so they can accurately and effectively report suspicious transactions, according to AML legislation.
- Brokerages engage outside, independent professionals to conduct their two-year reviews.
- Compliance officers participate in AML knowledge sessions, such as the Association of Certified Anti-Money Laundering Specialists.

These were recommended by Deloitte:

- Where possible, the roles of managing broker and FINTRAC compliance officer should be clearly defined and separated, and the role of compliance officer expanded to include managing the brokerage's inherent risk for money laundering and terrorist financing rather than simply ensuring regulatory compliance. Part of the expansion of the compliance officer role should also include centralizing the ongoing monitoring and client risk rating responsibilities and enhancing processes for documentation and review.

  Upon BCREA review, feedback from multiple real estate boards across the province challenged this finding as impractical as a "best practice". The added cost and complexity would not be workable for many brokerages, who already devote significant resources toward complying with an array of legislation at all levels of government.

- Brokerages monitor past real estate transactions for known or alleged criminal activity and consider submitting suspicious transaction reports.

  BCREA board feedback challenged this finding as impractical and setting an expectation that cannot be met. If suspicion wasn't raised at the time of the original transaction, it is unlikely a review in the aftermath would yield any new findings.

Regulatory recommendations

Our investigations have uncovered several opportunities for improvements in federal and provincial regulatory frameworks. BCREA recommends that:

1. The federal government require FINTRAC compliance by lawyers, law firms and non-financial institution lenders, such as alternative and private lenders, and for private real estate transactions.
2. FINTRAC implement its own best practices, including:
   - policies to ensure consistency in its examinations, including immediate, specific suggestions for how a real estate brokerage can improve its compliance system (in early February, FINTRAC published its Assessment Manual, which explains the approach and methods used during examination; consistency has yet to be tested),
   - outreach to sector organizations to create resources—including guidelines to identify suspicious transactions—that reflect real-world situations, and
   - public reporting practices that accurately represent the results of their examinations.
3. The BC Government clarify the role of provincial real estate regulators in the area of anti-money laundering requirements. Ideally, the Real Estate Council of British Columbia will develop required anti-money laundering licensing and relicensing education for REALTORS®.
4. The federal and provincial governments, and their respective agencies, coordinate their actions and policies to create a comprehensive, efficient enforcement regime.

In addition, Deloitte recommends that the Real Estate Council of British Columbia incorporate AML into its brokerage audit program.

BCREA board feedback indicated that FINTRAC already conducts examinations, and the boards considered the above suggestion to be a duplication of efforts.

Thank you for the opportunity to provide input. We always welcome opportunities to provide information and context on this important issue. BCREA also looks forward to future opportunities to comment on draft policies and/or legislation that result from the work of the Expert Panel and Peter German.

BCREA is the professional association for about 23,000 REALTORS® in BC, focusing on provincial issues that impact real estate. Working with the province's 11 real estate boards, BCREA provides continuing professional education, advocacy, economic research and standard forms to help REALTORS® provide value for their clients.

To demonstrate the profession's commitment to improving Quality of Life in BC communities, BCREA supports policies that encourage economic vitality, provide housing opportunities, respect the environment and build communities with good schools and safe neighbourhoods.

Sincerely,

Darlene K. Hyde
Chief Executive Officer

Copies: Hon. Carole James, Minister of Finance and Deputy Premier (FIN.minister@gov.bc.ca)
Hon. David Eby, Attorney General (AG.minister@gov.bc.ca)
Donna Barnett, MLA – Cariboo-Chilcotin (donna.barnett.mla@leg.bc.ca)
Shirley Bond, MLA – Prince George-Valemount (shirley.bond.mla@leg.bc.ca)
Michael Lee, MLA – Vancouver-Langara (michael.lee.mla@leg.bc.ca)
Tracy Redies, MLA – Surrey-White Rock (tracy.redies.mla@leg.bc.ca)
Micheal Noseworthy, Superintendent of Real Estate (micheal.noseworthy@gov.bc.ca)

Erin Seeley, Executive Officer, Real Estate Council of British Columbia
(eseeley@recbc.ca)

Appendix 21

BCREA – *BC Real Estate Sector Submits Anti-Money Laundering Recommendations to Government* - April 15, 2019

BC Real Estate Sector Submits Anti-Money Laundering Recommendations To Government

Apr 15, 2019

CATEGORY: News Releases
TAGS: **Anti-Money Laundering**

Posted by
Trevor Hargreaves
VP Government Relations / Stakeholder Engagement

SHARE THIS

PRINT

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within News Releases

- COVID-19
- Anti-Money Laundering
- Strata Property Act
- Professional Development

Vancouver, BC - April 15, 2019. Organizations representing key professions in the BC real estate sector submitted joint recommendations to the provincial and federal governments today to help protect BC's housing market from money laundering.

The participating organizations include the British Columbia Real Estate Association, the Appraisal Institute of Canada – BC Association, BC Notaries Association, Canadian Mortgage Brokers Association – British Columbia, and the Real Estate Board of Greater Vancouver.

In their submission, these organizations also commit to shared best practices to help keep the proceeds of organized crime out of the economy. Their efforts focus on helping protect the real estate market from unscrupulous operators and ensuring the public can have full confidence in BC's real estate market. All of the organizations have fully supported and participated in the government's investigations into money laundering and real estate.

Popular posts from BCREA

Real Estate Professionals Urged to Stop Open Houses: Regulators and Provincial Association Recommend Virtual Tools

Nov 05, 2020

Applications for BC

A real estate transaction involves multiple professionals. It will take a coordinated effort by all involved, working in collaboration with government, to stop money laundering. The joint recommendations and best practices submitted by these organizations reflect their commitment to the professionals and consumers they serve.

-30-

Read their submission to government:

Real Estate Sector Anti-Money Laundering Statement

As a group of real estate organizations representing industry professionals, we are committed to a transparent real estate market and

Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

to ensuring that the public can continue to have full confidence in the real estate industry. Illegal funds have no place in BC's real estate market. We are supportive of the government's investigations into money laundering and real estate, having actively participated in Peter German's review and the Expert Panel on Money Laundering.

As an industry, we have come together to commit to shared best practices and make recommendations to government. By aligning as an industry and working in collaboration with government, we can help facilitate an environment in which consumers are well-served and industry professionals can thrive.

Anti-money laundering recommendations Our collaboration has resulted in a commitment from the undersigned

organizations to pursue the following shared best practices and recommendations for government:

1. **Accept only verified funds** – For sectors of real estate that are not already required to do so, we recommend that they accept funds only in forms that are verifiable through Canadian financial institutions.

2. **Mandatory anti-money laundering education** – We recommend the introduction of mandatory anti-money laundering education for all real estate professionals subject to the reporting requirements administered by the Financial Transactions

and Reports Analysis Centre of Canada (FINTRAC) to ensure that those professionals are trained in recognizing and reporting suspicious transactions. FINTRAC should work with sector organizations, regulators and the provincial government to improve existing resources so that they better reflect real-world situations and improve compliance.

3. **Smart regulation** – We recommend that the federal government amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to allow FINTRAC intelligence to be made

available to additional regulatory authorities, including the BC Securities Commission and the Financial Institutions Commission (FICOM). Optimally, the federal and provincial governments, as well as their respective agencies, should coordinate their actions, share information, such as the provincial assignment registry, and create a comprehensive, efficient enforcement regime.

4. **Ongoing engagement** – We recommend governments and regulatory agencies, including FINTRAC, better utilize on-the-ground experience of

real estate professionals to develop compliance resources and test policy ideas. This will result in well-crafted, practical regulation and foster a culture of compliance to protect consumers and the economy.

5. **Timely and transparent reporting** – We recommend that FINTRAC implement a framework to identify and report trends on a regular basis and in language that is consistent and understandable to professionals, the public and media. This reporting system should also include consistency in examinations with immediate feedback

designed to help industry professionals improve their compliance systems.

For a backgrounder to the statement, **click here.**

Click here for the PDF.

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Email

bcrea@bcrea.bc.ca

Follow Us

Sign up and stay informed

Enter yo

Appendix 22

BCREA – *Letter to Ministry of Finance re BC Consultation on a Public Beneficial Ownership Registry* – April 29, 2020

BCrea
British Columbia
Real Estate Association

Suite 1425, 1075 West Georgia St
Vancouver, BC V6E 3C9
bcrea.bc.ca

April 29, 2020

Attn: Policy and Legislation Division
BCA Beneficial Ownership
Ministry of Finance
PO Box 9418 Stn Prov Govt
Victoria, BC V8W 9V1
Submitted by email: BCABO@gov.bc.ca

RE: BC Consultation on a Public Beneficial Ownership Registry

The British Columbia Real Estate Association (BCREA) recognizes the need for transparency to ensure confidence in BC's economy. We welcome the opportunity to provide input into this consultation on a potential public corporate beneficial ownership registry.

At a high level, BCREA is looking for senior governments to create and implement smart policies, laws and regulations. Coordination is required to effectively identify and address money laundering. We expect the provincial and federal governments to use common language, thresholds and data standards so that registries and other systems can be linked.

BCREA also expects that privacy will continue to be a significant concern, and that governments build assessment and accountability into their approaches.

Our specific feedback on the consultation paper is organized into the five categories articulated in the Background section: business impacts, efficient collection of data, public access, scope and role of government.

Business Impacts
To simplify implementation, we recommend using the existing Corporate Registry, which is already available through BC OnLine. This will help reduce the administrative burden for companies and should be financially and operationally efficient for the government.

Additional reporting requirements, such as transparency registers, represent higher costs for corporations through legal and consulting fees. Therefore, we ask that the registration and access fees for the Corporate Registry not be increased.

Transparency registers are a new process for REALTORS®, and so BCREA recommends flexibility for those whose registers are found lacking. A heavy-handed approach to enforcement would negatively impact the business and also their customers/ clients, so please consider all possible consequences of a heavy-handed approach. To help ensure compliance, please provide support to corporations in the form of best practices and information to help them understand why these systems are needed.

Efficient Collection of Data

To ensure efficiency, we urge the government to create a system that does not duplicate efforts. Specifically, if information is gathered for the Land Owner Transparency Registry, then do not require the same information to be gathered for the corporate beneficial ownership registry. Aside from being time efficient for the public and private sectors, a single point of data entry reduces the chance for errors and also makes it more likely that the information remains current.

As noted above, we expect the provincial registry will be linked to the national registry, assuming both are created.

Please explain why a provincial registry was not contemplated in Bill 24 (2019). By introducing transparency registers and then consulting on a provincial registry, the government's approach to corporate beneficial ownership seems inefficient from the start.

Public Access

We firmly believe that transparency needs to be balanced with privacy. BCREA urges the government to consider a broad approach to privacy and anti-money laundering measures. That is, please clearly articulate anti-money laundering goals, and then determine the minimum information that needs to be made public to accomplish those goals. Then that approach can be used as a starting point for all government anti-money laundering initiatives.

To prevent a misuse of data, we recommend safeguards against the misuse of registry information. Please see section 77 of the *Land Owner Transparency Act*, which prohibits people from using publicly accessible data for solicitation or harassment.

Scope

BCREA strongly recommends using a 25 per cent threshold to determine beneficial ownership, because it is consistent with the federal government's approach. For further consistency, we also recommend the definition of "significant number of shares" in the *Land Owner Transparency Act* be changed from 10 per cent to 25 per cent. Differences from one initiative to another are likely to cause confusion and result in mistakes.

Aside from potential privacy issues for family trusts, we have no concerns about requiring trusts and limited partnerships to participate in this initiative. The challenge comes from the fact that there is no existing registry for trusts, and the current partnership registry would need to be enhanced. If they are included, then all three registries should be linked together.

Role of Government
We prefer government take a reactive approach to verifying the accuracy of information in the registry. By that we mean that the government only takes steps to verify information when alerted by another party that information might be incorrect.

Please contact me directly (dhyde@bcrea.bc.ca; 604.790.4855) if you have any questions or want to discuss further.

BCREA is the professional association for about 23,000 REALTORS® in BC, focusing on provincial issues that impact real estate. Working with the province's 11 real estate boards, BCREA provides continuing professional education, advocacy, economic research and standard forms to help REALTORS® provide value for their clients.

To demonstrate the profession's commitment to improving Quality of Life in BC communities, BCREA supports policies that encourage economic vitality, provide housing opportunities, respect the environment and build communities with good schools and safe neighbourhoods.

Sincerely,

Darlene K. Hyde
Chief Executive Officer

Copies: Hon. Carole James, Minister of Finance and Deputy Premier (FIN.minister@gov.bc.ca)
Hon. David Eby, Attorney General (AG.minister@gov.bc.ca)
Shirley Bond, MLA – Prince George-Valemount (shirley.bond.mla@leg.bc.ca)
Stephanie Cadieux, MLA – Surrey South (stephanie.cadieux.mla@leg.bc.ca)
Michael Lee, MLA – Vancouver-Langara (michael.lee.mla@leg.bc.ca)

Appendix 23

BCREA – *Backgrounder to the Real Estate Sector Anti-Money Laundering* Statements – April 15, 2019

Backgrounder To The Real Estate Sector Anti-Money Laundering Statement

April 15, 2019

In September 2018, Attorney General David Eby commissioned former RCMP Deputy Commissioner Peter German to study whether there is evidence that BC real estate, luxury car sales and horse racing industries are being used for money laundering. In parallel, the Ministry of Finance set up the Expert Panel on Money Laundering to assess legislative and regulatory gaps that could contribute to risks of money laundering and administrative non-compliance in the real estate and financial services sector.

Since then, professional organizations representing BC REALTORS®, appraisers, notaries and mortgage brokers have been working to support the government with their investigations, while learning more about the challenges the professionals they represent face in identifying and reporting suspicious activities.

One thing has become clear. Given that real estate transactions involve multiple professionals, it will take a coordinated effort and collaboration with government to strengthen anti-money laundering measures in BC's real estate market.

That's why the following organizations came together in early 2019 to commit to shared best practices and propose recommendations to government that will help ensure the public can have full confidence in BC's real estate market:

- British Columbia Real Estate Association
- Appraisal Institute of Canada - BC Association
- BC Notaries Association
- Canadian Mortgage Brokers Association - British Columbia
- Real Estate Board of Greater Vancouver

Read their press release and submission to government.

About the organizations:

British Columbia Real Estate Association (BCREA): Working with the province's 11 real estate boards, BCREA provides continuing professional education, advocacy, economic research and standard forms to help REALTORS® provide value for their clients. To demonstrate the profession's commitment to improving Quality of Life in BC communities, BCREA supports policies that help ensure economic vitality, provide housing opportunities, preserve the environment, protect property owners and build better communities.

Appraisal Institute of Canada – BC Association (AIC-BC): AIC-BC is the provincial association of the Appraisal Institute of Canada (AIC) within British Columbia and Yukon Territory. Established in 1973, AIC-BC represents approximately 1,200 members and delivers AIC's member programs and services within the region. AIC-BC's objective is to serve the profession and the public by implementing policies and programs to ensure the appraisal profession is advanced and the public is protected.

BC Notaries Association: BC Notaries are a select group of legal professionals commissioned by the Supreme Court of British Columbia, trained in the provision of non-contentious services including real estate transfers, personal planning and authentications. Throughout history, notaries have been recognized as individuals of integrity practising in a Tradition of Trust. The BC Notaries Association promotes and supports BC Notaries Public in all communities of the province.

Canadian Mortgage Brokers Association – British Columbia (CMBA-BC): CMBA-BC represents the province's mortgage industry. It exists to support and enhance professionalism and ethical standards within the mortgage industry. CMBA-BC offers educational and networking events designed to enhance professional development and relationship building within the industry and among clientele.

Real Estate Board of Greater Vancouver (REBGV): REBGV is a member-based professional association of more than 14,000 REALTORS® who live and work in communities from Whistler to Maple Ridge to Tsawwassen and everywhere in between. They provide structure and services that help their members excel and foster public confidence in the real estate profession.

For more information:

British Columbia Real Estate Association
April van Ert
Communications Manager
avanert@bcrea.bc.ca
604.742.2797

Appraisal Institute of Canada – BC Association
Christina Dhesi, BA, DULE
Executive Director
christina@appraisal.bc.ca
604.284.5515

BC Notaries Association
Jacqui Mendes
Chief Executive Officer
jmendes@society.notaries.bc.ca
778.327.6390

Canadian Mortgage Brokers Association – British Columbia
Samantha Gale, LLB
Chief Executive Officer
samanthagale@cmbabc.ca
604.408.9989

Real Estate Board of Greater Vancouver
Craig Munn
Manager, Communications
cmunn@rebgv.org
604.730.3146

Appendix 24

BCREA – *eBulletin: Anti-Money Laundering; Opportunities for Action* – May 2019

Link to *BCREA eBulletin:* **Online version** or **Mobile version**.

BCrea eBULLETIN

May 2019

Anti-Money Laundering

Opportunities for action

A public inquiry into money laundering has now been ordered. This has been a media favourite for a long time, and certainly since the reports of Peter German and the Expert Panel on Money Laundering in BC Real Estate were published on May 9. Here's a quick summary of BCREA's actions, analysis and how we're supporting REALTORS®.

In recent months, BCREA participated in both of the provincial government reviews, commissioned a vulnerability assessment of residential and commercial transactions and worked with four other real estate sector organizations on joint AML best practices and recommendations.

Both Peter German and the Expert Panel criticize REALTORS® for not filing many suspicious transaction reports and for poor compliance statistics with FINTRAC. To be clear, they also criticize FINTRAC for not providing the best feedback, data and resources. And both reports call out many other professions and the provincial and federal governments. The Expert Panel also explains that real estate is complex and it can be difficult to identify criminal activity in a context where most people are legitimate. While some media reports have focused on REALTORS® and “real estate firms,” the reports don't.

The Expert Panel makes 29 recommendations (Peter German only reports his findings and observations), and BCREA's perspective is reflected in 16 of them. We agree with the Expert Panel that lawyers and other professionals involved in potentially vulnerable aspects of real estate transactions should become part of the anti-money laundering monitoring and compliance system. We also strongly support coordination among governments and government agencies, the need for regulators to educate professionals about their reporting obligations and improved public reporting by FINTRAC.

Here are a few more Expert Panel recommendations that haven't been reported (the following language has been simplified):

> 6. The BC government should implement the recommendations of the Perrin report to improve BC's real estate regulatory framework. The Perrin report recommends a single regulator under the Financial Institutions Commission (instead of the dual system we have now), and the government is already moving in that direction
>
> 7. Individual real estate licensees—rather than managing brokers—should be responsible for their own compliance with the *Real Estate Services Act* and the [federal] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. This is a new direction.
>
> 8. Developers should be licensed under the *Real Estate Services Act* and the exemption from the Act for developers' employees should be eliminated. BCREA's always been on record that people who work for developers should be licensed; the biggest question we have about licensing developers is how that would impact our own regulatory system.

We're optimistic that, if implemented, the Expert Panel's recommendations will help create an efficient, comprehensive system to keep the proceeds of crime out of real estate. But that could take a long time, since many of the recommendations are complicated and require legislative changes at the federal and provincial levels.

In the meantime, BCREA is representing the REALTOR® voice as the government considers these recommendations. We're also working with member boards on resources to help REALTORS® meet their FINTRAC

compliance requirements. More information will be available soon, and we welcome feedback and suggestions at any time.

Find the Expert Panel and Peter German reports below, as well as BCREA's submission to the Expert Panel and our response following the release of the two reports:

- **Expert Panel report – *Combatting Money Laundering in BC Real Estate***
- **Peter German report – *Dirty Money – Part 2: Turning the Tide – An Independent Review of Money Laundering in BC Real Estate, Luxury Vehicle Sales & Horse Racing***
- **BCREA submission to the Expert Panel (March 4, 2019)**
- **BCREA news release (May 13, 2019)**

Click **here** to visit the *BCREA eBulletin* archive, available on REALTOR Link®.

View BCREA's Facebook Profile View BCREA's Twitter Profile View BCREA's LinkedIn Profile
View BCREA's YouTube Channel

British Columbia Real Estate Association Suite 1425, 1075 West Georgia Street, Vancouver, BC, V6E 3C9
Phone: 604.683.7702 | Email: **bcrea@bcrea.bc.ca**

Appendix 25

BCREA – *New Anti-Money Laundering Initiatives in Development* – Dec 5, 2019

New Anti-Money Laundering Initiatives in Development

Dec 05, 2019

CATEGORY: **Advocacy**
TAGS: **Anti-Money Laundering**

SHARE THIS

The issue of money laundering continues to be one of ongoing governmental and public concern. BCREA have taken an active role in the Cullen Commission of Inquiry into Money Laundering In BC, having applied and received formal standing to partake in the process and represent provincial real estate interests.

We have also been attending the initial public hearings which presented a mixed bag of public testimony, very little of which has thus far involved real estate. The most compelling testimony presented focused

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Advocacy

- COVID-19
- Strata Properties
- Mortgages
- Standard Forms
- Disclosure
- Strata Property Act

Popular posts from BCREA

Applications for

around issues tied to the casino sector and practices that are alleged to have resulted in the laundering of funds.

Internally, we are developing an array of new resources to support REALTORS® and managing brokers, such as infographics, podcasts, FAQs and regional training workshops.

In addition, the Real Estate Council of BC are amidst development of a mandatory anti-money laundering online course which will debut in early 2020.

In short, there is a great deal of work taking place behind the scenes to assure more robust education, better access to information and new services. Expect to hear more on the above in coming weeks.

Photo courtesy of The Globe and Mail

BC Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

GET IN TOUCH

Suite 1425, 1(West Georgia St.
Vancouver, E V6E 3C9

Phone 604.683.7702
Toll Free 1.844.288.7702

Fax 604.683.8601

Emaibcrea@bcrea.bc.ca

Follow Us

Sign up and stay informed

Enter your

Appendix 26

BCREA – *Get Ready for Mastering Compliance: Anti-Money Laundering Training for Brokers* – August 13, 2020

Get Ready for Mastering Compliance: Anti-Money Laundering Training for Brokers

Aug 13, 2020

CATEGORY: Education
TAGS: **Anti-Money Laundering** **Compliance** **FINTRAC**

Posted by
Marianne Brimmell
Communications Specialist

This fall, BCREA is launching *Mastering Compliance: Anti-Money Laundering Training for Brokers*, a nine-week program created to support managing brokers and compliance officers in meeting anti-money laundering and FINTRAC requirements.

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Education

- COVID-19
- Standard Forms
- Anti-Money Laundering
- Property Disclosure

This comprehensive program will provide learners with the knowledge, skills and resources to:

- navigate an audit or examination with confidence,
- implement effective brokerage compliance training,
- conduct an audit of potential risks and vulnerabilities,
- identify gaps and opportunities in brokerage policies and procedures,
- guide agents on when and how to file Suspicious Transaction Reports,
- adapt to upcoming changes in compliance standards,
- and more!

▸ Real Estate Practice
▸ Property Disclosure Statement

Popular posts from BCREA

Real Estate Professionals Urged to Stop Open Houses: Regulators and Provincial Association Recommend Virtual Tools
Nov 05, 2020

Applications for BC

Appendix 26

Mastering Compliance: Anti-Money Laundering Training for Brokers will run from October 5 to December 4 and will require approximately 1-3 hours each week. It will be a blended model, with both online and virtual classroom components, and will be eligible for accredited PDP hours.

The program will be facilitated by Jacqueline Shinfield, one of Canada's leading financial services regulatory lawyers.

Stay tuned for registration information in the next *Resources for REALTORS®* newsletter.

To subscribe to receive BCREA publications, or to update your email address or current subscriptions, **click here**.

Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Discounts ▸

About BCREA ▸

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

twitter youtube

GET IN TOU

Suite 1425, 1C
West Georgi :.
Vancouver, E /6E
3C9

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Email bcrea@bcrea.bc.ca

Follow Us

Sign up and stay informed

Enter yo

Appendix 27

BCREA – *Mastering Compliance: Anti-Money Laundering Trainihng for Brokers Program* – December 16, 2020

Mastering Compliance: Anti-Money Laundering Training for Brokers Program

Mastering Compliance: Anti-Money Laundering Training for Brokers is a nine-week program combining online, self-paced learning with virtual classes. Learners must successfully complete all content modules and attend all the virtual classes during the nine-week period to earn their completion certificate.

This comprehensive program provides learners with the knowledge, skills, and resources necessary to master FINTRAC compliance, including:

- how to foster a culture of compliance;
- what roles the compliance officer, managing broker, brokerage, Realtors, and support staff play in establishing and maintaining compliance;
- what FINTRAC's requirements are for reporting and record-keeping and how to ensure the brokerages' policies and procedures are compliant;
- why identifying business risks in the context of money-laundering and terrorist financing is important and how to implement a risk-based approach;
- when to report a suspicious transaction and how to file a suspicious transaction report;

- how to develop and maintain a compliance training program;
- who conducts an effectiveness review and what should be included; and
- how to be prepared for a FINTRAC examination and address deficiencies.

The online, self-paced modules are complemented by three virtual classes hosted by BCREA and facilitated by lawyer Jacqueline Shinfield. These virtual classes provide a communal environment for networking, trading stories, collaborative problem solving, and peer support.

Upon completion of this program, learners will be able to implement effective brokerage compliance training; navigate a FINTRAC examination with confidence, identify and mitigate business risks related to money laundering, identify gaps and opportunities to improve brokerage policies and procedures, guide agents on how to file suspicious transaction reports, and adapt to upcoming compliance standards.

Return to Previous Page

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Benefits ▸

About BCREA ▸

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Phone 604.683.7702

Toll Free 1.844.288.7702

Fax 604.683.8601

Email bcrea@bcrea.bc.ca

Follow Us

Sign up and stay informed

Enter you

Appendix 28

BCREA – *Signs You Should File a Suspicious Transaction Report* – Sept 3, 2020

Signs You Should File a Suspicious Transaction Report

Sep 03, 2020

CATEGORY: **Practice Tips**
TAGS: **Anti-Money Laundering** **FINTRAC** **Suspicious Transaction Report**

Posted by
April van Ert
Communications Manager

SHARE THIS

Filing a Suspicious Transaction Report (STR) can seem like a tough call – what's considered suspicious? And how do they help anyways? The truth is STRs are an easy and important way for REALTORS® to help protect BC's economy from money laundering. They also play a key role in helping law enforcement identify money launderers and bring them to justice. If you experience any of these signs during a transaction, it's time to file one.

Know thy client

Anytime a client uses a name other than their own (or a spouse's) on documents or uses different names on offers to purchase,

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Practice Tips

- COVID-19
- Strata Properties
- Liability
- Deposits
- Disclosure
- Anti-Money Laundering

Popular posts from BCREA

closing documents or deposit receipts, you need to file an STR. Likewise, if your client remains anonymous and all your dealings are with a lawyer and cheques drawn on a lawyer's trust account, that's a sign something might be wrong.

Caginess about using their own name isn't the only sign something might be wrong. If your client is conducting a transaction on behalf of someone who doesn't seem like they could afford it (like someone who is underage) or is painting their own financial situation in a way that seems unrealistic, then it's time to submit an STR.

And while BC has lots of out-of-country buyers, if your client is a non-resident for tax purposes and is buying a property as an investment with no intention of living in it, it's worth considering an STR, especially if there are other indicators that something's off.

Easy come, easy go

If a client seems unconcerned about the financial risks (like losing a deposit) or costs of a transaction, warning bells should go off. Another warning sign is when a client seems unconcerned about the value

Applications for BC Emergency Benefit for Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

of the property itself. For example, they're planning to build a luxury house in a non-prime location; they resell the property shortly after buying it at a significantly different price although local market values haven't changed; or they buy multiple properties in a short period of time and seem unconcerned about the location, condition or any future repair costs.

Follow the money

Any unusual ways of paying a deposit is a clear sign something's not quite right. This could include your client asking for the deposit to be divided into smaller parts with a short interval between them or even paying the deposit with a cheque from a third-party other than a spouse or parent. Another telltale warning sign is when a client pays a substantial down payment in cash and the balance is financed by an unusual source or offshore bank.

So I filed an STR. What happens next?

From your perspective as a Realtor, not much. The transaction completes and most likely you will never know how that

information was used. Identifying and prosecuting money launderers is a long process and often takes years of law enforcement officers piecing together a complex puzzle of financial and other data. But by submitting an STR, Realtors can contribute a piece of the puzzle – and it just might be the piece that helps bring a criminal to justice.

To subscribe to receive BCREA publications such as this one, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 1(West Georgia St.
Vancouver, E V6E 3C9

Phone 604.683.7702
Toll Free 1.844.288.7702
Fax 604.683.8601
Email bcrea@bcrea.bc.ca

BCrea British Columbia Real Estate Association

What We Do ▸

Want to Be a REALTOR®?

REALTOR® Education ▸

Professional Discounts ▸

About BCREA ▸

Sign up and stay informed

Enter your

OUR PODCAST

TAX CALCULATOR

PDP LOGIN

Appendix 29

BCREA – *Anti-Money Laundering Resources* – Sept 25, 2020

Anti-Money Laundering Resources

Sep 25, 2020

CATEGORY: Advocacy
TAGS: **Anti-Money Laundering**

Posted by
Marianne Brimmell
Communications Specialist

SHARE THIS

PRINT

Background Resources Advocacy

Last updated: November 25, 2020

Ensuring REALTORS® have the resources to meet anti-money laundering requirements is an important step towards keeping money from criminal activity out of

What we do

- Advocacy
- Economics
- Education
- Standard Forms
- Legally Speaking
- Media Relations
- Podcast

Popular tags within Advocacy

- COVID-19
- Strata Properties
- Mortgages
- Standard Forms
- Anti-Money

BC's housing market. BCREA has created this dedicated page to help Realtors access BCREA's anti-money laundering resources. Throughout the fall, we'll add to these resources with new blog, podcast and video content on anti-money laundering topics.

Background

Money laundering is an issue of significant concern for all British Columbians. At BCREA, we take the issue very seriously. We continue to be active participants in the Cullen Commission of Inquiry into Money Laundering in British Columbia, where we have been providing information, documentation, and expertise. We are scheduled to give public testimony in early spring 2021. BCREA is committed to ongoing sectoral efforts that foster increased awareness, understanding and best-practice

Popular posts from BCREA

Real Estate Professionals Urged to Stop Open Houses: Regulators and Provincial Association Recommend Virtual Tools

Nov 05, 2020

Applications for BC Emergency Benefit for

compliance around money laundering as a strategic priority. By strengthening our practices, we can assist government in assessing and minimizing this issue while also better protecting our communities.

We recently introduced a new educational initiative called *Mastering Compliance: Anti-Money Laundering Training for Brokers*, a blended learning program focused on best-practices and anti-money laundering compliance. The program launched on Monday, October 5. **Click here** to learn more.

Below, Realtors can access BCREA's resources, communications and advocacy materials related to this issue.

Resources

News Releases

Workers Now Open
May 01, 2020

First-Time Home Buyer Incentive Launches in September
Aug 22, 2019

- **BCREA Calls for Increased Federal/Provincial Cooperation to Tackle Money Laundering in BC** (February 26, 2020)
- **BC's REALTORS® Welcome Government Recommendations** (May 13, 2019)
- **BC Real Estate Sector Submits Anti-Money Laundering Recommendations to Government** (April 15, 2019)
- **BCREA Supports BC Government's Money Laundering Investigations** (November 27, 2018)
- **BCREA Supports Government's Reviews of BC Real Estate** (September 28, 2018)

Blog Posts

- **How REALTORS® Help Prevent Money Laundering in Real Estate: Setting the Landscape** (November 25, 2020)
- **New Form Helps Brokerages Meet Anti-Money Laundering Requirements** (October 20, 2020)
- **Transparency Registers Effective October 1** (September 8, 2020)
- **Signs You Should File a Suspicious Transaction Report** (September 2, 2020)
- **Register Now for Mastering Compliance: Anti-Money Laundering Training for Brokers** (August 26, 2020)

- **BCREA Combats Money Laundering Through Participation in Cullen Commission** (May 28, 2020)

- **New Anti-Money Laundering Initiatives in Development** (December 5, 2019)

- **BCREA Brings REALTOR® Perspective to Inquiry into Money Laundering** (November 18, 2019)

- **Real Estate Professions Taking the Lead to Curb Money Laundering** (May 17, 2019)

- **Anti-Money Laundering: Opportunities for Action** (May 17, 2019)

- **Anti-Money Laundering in Real Estate Sector** (May 1, 2019)

- **FINTRAC Compliance? There's an App for That!** (March 7, 2019)
- **Focus on Anti-Money Laundering** (March 1, 2019)
- **Understanding Money Laundering Vulnerabilities** (February 13, 2019)
- **The Role of REALTORS® in Helping the Government Stop Money Laundering** (January 4, 2019)
- **Real Estate Transparency to Build Public Confidence** (November 1, 2018)

Media Coverage

- **British Columbia Real Estate Association calls for co-ordinated effort to tackle money laundering** (Real Estate Magazine, March 11, 2020)

- **What BCREA wants the government to do about money laundering** (Canadian Real Estate Magazine, February 28, 2020)

- **Canada must expose hidden company owners to end 'snow washing,' inquiry hears** (CBC, February 27, 2020)

- **Acceptance of cash deposits rare in real estate, money laundering inquiry hears** (BNN Bloomberg, February 26, 2020)

- **B.C. money laundering inquiry to begin amid hopes for answers, accountability** (CBC, February 23, 2020)

- **Mandatory anti-money laundering course rolls out for B.C. realtors** (CBC, January 1, 2020)

- **Darlene Hyde: Realtors are part of the solution to fighting money laundering** (Vancouver Sun, May 24, 2019)

- **'Swiss cheese' regulatory system allows dirty money into real estate: BCREA CEO** (Vancouver Courier, May 15, 2019)

- **Joint statement on anti-money laundering commitments by real estate industry** (BC Gov News, April 15, 2019)

- **Real estate groups issue recommendations on money laundering** (The Globe and Mail, April 15, 2019)

- **Real estate sector proposes changes to fight money laundering** (Vancouver Sun, April 15, 2019)

- **B.C.'s real estate professionals on what they need to stop money laundering in housing** (CBC, April 15, 2019)

Advocacy

Submissions

In 2019, BCREA actively participated in Peter German's review of money laundering in gambling, luxury cars and real estate and Maureen Maloney's Expert Panel on Money Laundering. View our submissions below:

- **BCREA submission to Expert Panel on Money Laundering** (March 4, 2019)

- **BCREA submission to Peter German** (March 4, 2019)

BCREA also monitors the BC Government's various anti-money laundering initiatives and provides

feedback on behalf of Realtors, as necessary. See the following recent documents for more information:

- **Letter to Minister of Finance Carole James regarding the Land Owner Transparency Registry** (August 13, 2020)

- **Response to consultation on proposed corporate beneficial ownership registry** (April 29, 2020)

Recommendations

In 2019, BCREA brought together four other real estate sector partners to combat the issue of money laundering. This collaboration resulted in a commitment from all organizations involved to pursue shared best practices and recommendations for government, which you can find **here**.

To follow BCREA's advocacy work on anti-money laundering and other issues, contact **gr@bcrea.bc.ca** to subscribe to the Advocacy Update, published every two weeks.

To subscribe to receive BCREA publications, or to update your email address or current subscriptions, **click here**.

GET IN TOUCH

Suite 1425, 10
West Georgi
Vancouver, E /6E
3C9

Phone 604.683.7702
Toll Free 1.844.288.7702
Fax 604.683.8601
Email bcrea@bcrea.bc.ca

Follow Us

BCrea
British Columbia Real Estate Association

What We Do ▸
Want to Be a REALTOR®?
REALTOR® Education ▸
Professional Benefits ▸
About BCREA ▸

Sign up and stay informed

Enter yo

OUR PODCAST
TAX CALCULATOR
PDP LOGIN

Appendix 30

AML Resources Identified by Local Real Estate Boards

AML Resources identified by Local Real Estate Boards

Boards flagged the following resources available to real estate agents for education on the topic of money laundering in real estate:

1. Canadian Real Estate Association sources. Members have access to resources through CREA Education Hub on REALTORLink. There is a page dedicated to FINTRAC within the portal and it includes:
    a. FINTRAC FAQ document, titled “FINTRAC Information for REALTOR® Members”;
    b. Template FINTRAC documents:
        1. FINTRAC - Receipt of Funds Record;
        2. FINTRAC - Office Policy Template;
        3. FINTRAC - Template Consent Letter;
        4. FINTRAC - Risk Assessment Form;
        5. FINTRAC - Individual Identification Information Record;
        6. FINTRAC - Identification Mandatory/Agent Agreement;
        7. FINTRAC - Corporation/Entity Identification Information Record;
    c. names of companies that offer anti-money laundering services to real estate professionals;
2. CREA-created courses, including:
    a. Introduction to Canada’s FINTRAC Regime;
    b. CREA Lite M3: Legal.
3. BCREA’s resources, including:

a. FINTRAC: Compliance for REALTORS®, Brokers and Broker Managers;

b. FINTRAC presentation at BCREA Advocacy Exchange: Conference for Managing Brokers, held September 19th, 2018;

4. FINTRAC:

a. FINTRAC's webpage;

b. FINTRAC's online webinar (http://video.isilive.ca/fintrac/2016-03-21.html);

5. Newsletters repeating information from 3rd party sources.

Appendix 31

CMBA-BC – *News Release; Mortgage Brokers Association Recommends Stronger Enforcement of Existing Regulations to Control use of Mortgages for Money Laundering* – February 20, 2018

NEWS RELEASE

Mortgage Brokers Association recommends stronger enforcement of existing regulations to control use of mortgages for money laundering

Vancouver, B.C. – (February 20, 2018) – The Canadian Mortgage Brokers Association - British Columbia (CMBA-BC) is urging Attorney-General David Eby to increase enforcement of regulations that prohibit unlicensed brokers from lending money. The association representing licensed mortgage brokers in British Columbia is responding to Mr. Eby's announced intention to close loopholes allowing lenders to launder money through mortgages. Mortgage brokers arrange funding with private lenders.

"There are no loopholes to close," says CMBA-BC Chief Operating Officer Samantha Gale. "We need to distinguish between private lenders who are licensed under the Mortgage Brokers Act and criminals who lend money as part of a money laundering scheme. Criminals do not comply with regulations and criminal law while trying to fly under the radar."

There are already strict penalties under the Criminal Code of Canada that prohibit money laundering, excessive interest rates and fraud. "These laws need to be understood and enforced," she says.

As well, private lenders are required to obtain licensing under the BC Mortgage Brokers Act (MBA) if they are in the business of lending money or lend on 10 or more mortgages a year. The MBA authorizes regulatory action against those who do not obtain the required licensing. The MBA already enables the Registrar to require annual financial reporting for its licensees, conduct investigations and audits of both licensed and unlicensed lenders and issue orders to remedy non-compliant conduct.

"Current financial reporting can be made more robust under existing legislative provisions," Gale says. "We urge the government to have more robust financial reporting to better understand private lending activity."

She points out the Mortgage Brokers Act dates to 1972 and has been on the legislative agenda for review since 2012, with little or no action taken by the provincial government.

"We have urged the government to proceed with its legislative review, as the legislation needs to be modernized," Gale says. "Many smaller jurisdictions across Canada including Nova Scotia, Manitoba, New Brunswick and Saskatchewan now have modernized legislation to more effectively regulate the mortgage industry."

Private lenders who raise capital from the public, which include mortgage investment corporations and many syndicators are also regulated under securities legislation.

“Their capital raising activities are already governed by the BC Securities Commission, which has a comprehensive regulatory scheme in place to ensure that investors are protected,” Gale says.

The public should always access private lenders through licensed mortgage brokers and are welcome to contact CMBA-British Columbia for more information.

Canadian Mortgage Brokers Association - British Columbia provides information, education, advocacy and support for approximately 1,500 members throughout British Columbia. It is a member of the national Canadian Mortgage Brokers Association, which unites provincial mortgage broker associations together under one umbrella.

For more information **http://www.mbabc.ca**

Samantha Gale

CEO, Canadian Mortgage Brokers Association – British Columbia

Ph: 604-408-9989

Email: Samantha Gale samanthagale@mbabc.ca

Appendix 32

CMBA-BC – *Letter to Expert Panel on Money Laundering re Submissions from the Canadian Mortgage Brokers Association* – BC – March 21, 2019

March 21, 2019

Expert Panel on Money Laundering

Via email

Attn: Expert Panel Members:

Submissions from the Canadian Mortgage Brokers Association- BC

Thank you for meeting with representatives from the Canadian Mortgage Brokers Association – BC to discuss measures which could be undertaken by the government of BC to help combat money laundering and abuses in the housing sector and mortgage transaction process.

Please know we are committed to a transparent real estate market and to ensuring the public can continue to have full confidence in the mortgage lending and brokering industry. Illegal funds have no place in BC's real estate market. We are supportive of the government's investigations into money laundering and real estate, including Peter German's review and the Expert Panel on Money Laundering.

I understand the mandate of the Expert Panel, which has been commissioned by the BC Minister of Finance, is to look at ways of improving the BC regulatory system to prevent money laundering and market abuse related to the real estate industry. In furtherance of this goal, we can make the following recommendations for potential actions for your consideration. The recommendations focus on the Mortgage Brokers Act ("MBA"), which is the statue which creates a licensing or registration regime for mortgage brokers and private mortgage lenders. I attach a brief note on the MBA to give you some background on the statute.

Mandatory Anti-Money Laundering Education

The Registrar currently requires registrants to complete courses to qualify to obtain their renewal of registration; registration must be renewed every two years. We recommend the introduction of mandatory anti-money laundering education for all registrants under the MBA at the time of registration renewal. This will ensure MBA registrants are better trained to recognize and report suspicious transactions.

Amendments to the MBA to create a "Designated Individual" Registration Category

Currently the MBA has no licensing or registration category for designated individuals, submortgage brokers who are responsible to manage a mortgage brokerage. The management responsibilities include overseeing the brokerage's and its team members' compliance with regulatory and legal requirements.

Most modern licensing statutes create a managing broker or designated individual licensing category. Having a person designated with compliance responsibility enables regulators to create standards and policy specifically geared for the position's unique brokerage management functions. As a band-aid solution to this legislative gap in the MBA, the Registrar of Mortgage Brokers has created a simple "DI" policy; our view is that the policy is not supported by legislation and is therefore not enforceable. A designated individual licensing category would also enable the Registrar to require designated individuals to undertake specific, higher level courses which address market abuses and money laundering issues.

Amendments to the MBA to resolve licensing/registration gaps

There are discrepancies between substantive sections of the MBA and its enforcement provisions. Section 1 of the MBA defines mortgage brokers to include a person who in any one year receives $1,000 or more for arranging mortgages for other persons; such a person is required to obtain registration. However, section 21(1)(a) makes it an offence to "carry on business as a mortgage broker or submortgage broker" without registration. The BC Supreme Court in AZTA Management v. Croft Agencies Ltd. BCSC 1462 declined to find that a person who arranged a mortgage for $6 million was needing registration under the MBA. The Court, in applying the enforcement provision, said the person was not carrying on business as a mortgage broker as, among other things, the subject transaction was an isolated incident. The Court accordingly said that the person was not required to be registered and awarded the person a fee of $90,000.

The MBA is a public protection statute; the public is at risk if its enforcement provisions do not properly support the registration requirements. The absurd inconsistency in the MBA needs to be addressed by amending its enforcement sections.

Amendments to the MBA to plug loopholes for bank brokers

Bank employees who broker third party mortgages come within the scope of the MBA. They act as intermediaries between borrowers and third party lenders (other than the bank that employs them). We estimate that approximately one half of all brokered mortgages are arranged by brokers employed by banks, who are not licensed under the MBA or any similar mortgage broker licensing statute in another province.

Section 11 of the MBA provides: "(1) The registration provisions of this Act do not apply to any of the following while acting as mortgage brokers or submortgage brokers under

their proper names: (b) savings institutions . . .” It further states that the “The registration provisions of this Act do not apply to any of the following: (a) an employee, or director, of a person exempted from registration under subsection (1) (a) or (b) . . ..”

In a nutshell, the MBA only exempts bank brokers from having to register as a mortgage broker or submortgage broker. It does not exempt them from any other provisions of the MBA.

The result is that there are critical provisions of the MBA with which bank brokers in B.C. are required to comply, such as providing conflict of interest disclosure, private lender disclosure, and cost of credit disclosure. It is improper to expose the public to undue risk by not enforcing these and other protections provided in the MBA, which include public discipline by an independent government regulator for engaging in prejudicial conduct, undertaking continuing education, and submitting required periodic filings. However, bank brokers without consequence do not appear to comply with any provisions of the MBA or any comparative protections in the federal regulatory regime.

This gap poses significant risk to members of the public. In addition, it enables unscrupulous borrowers trying to push fraudulent mortgages through the system to shop mortgage applications through the softer, less strict bank broker system after experiencing rejection from the mortgage broker channel. We therefore urge the Panel to plug this loophole and ensure that bank brokers obtain registration under the MBA.

We want to thank you for the opportunity to speak to members of the Expert Panel and provide this written submission in follow up. Please know we are available to provide further information or clarification, if needed or desired.

Yours truly,

Samantha Gale
CEO, Canadian Mortgage Brokers Association-BC

Appendix 33

Mortgage Brokers Institute of BC – *Available Courses* – December 16, 2020

AVAILABLE COURSES

Online

Course Details	Course Price	
Name: Anti Money Laundering **Details:** Real estate and mortgage brokers are	$59.95	Add To Cart

significant targets of money launderers. The law, including regulators, requires mortgage brokers to not be engaged in money laundering. What is money laundering? How can you recognize it? When is even a little or peripheral involvement in money laundering enough to get you in trouble? What can you do to not, even carelessly, be part of the problem? What can you do to be part of the solution?		
Name: Ethics: A Practical Approach **Details:** What standard of conduct must a broker meet to keep their registration/licence? What do ethics have to do with it? Who determines ethical standards for mortgage brokers, when the standards are breached, and the consequences of being unethical? How do ethics relate to legal/regulatory requirements and morals?	$0.00	Already enrolled
Name: Limitation Periods **Details:** The borrower won't pay back your mortgage. The client won't pay your outstanding fees. You made an error and the client wants to sue you for negligence. These are just examples of lawsuits you might start or have started against you; the possible cases are endless. How long do you have to start the lawsuit before you lose the right to do so? How long does someone have to start a lawsuit against you before they lose the right to do so? When does the time start? When does the allowed time end? What can you do to extend the time? What can you do to avoid extending the time? This course will equip you to better protect yourself and your clients concerning limitation periods.	$59.95	Add To Cart
Name: Module 1 - Recordkeeping **Details:** This module covers record keeping bulletin, client files/contents, office files, electronic records, confidentiality, who owns records/files, duties around record keeping, privacy issues.	$125.00	Add To Cart
Name: Module 11 - Mortgage Application Fraud by Mortgage Brokers **Details:** Mortgage Application Fraud by Mortgage Brokers	$125.00	Add To Cart
Name: Module 12 - Form 10 Interest Disclosure **Details:** Form 10 Interest Disclosure	$125.00	Add To Cart
Name: Module 2 - Advertising **Details:** This module covers name requirements, web site use, misleading information, MBA requirements, BPCPA requirements, false advertising and false statements.	$125.00	Add To Cart
Name: Module 3 - Form 9 **Details:** This module covers the investor/lender disclosure statement.	$125.00	Add To Cart

Name: Module 4 - Real Estate Appraisal **Details:** This module covers Appraisal concepts and different approaches to appraising property, how to read an appraisal, the review process, how appraisals can be used to perpetrate mortgage fraud	$125.00	Add To Cart
Name: Module 5 - Marketing **Details:** This module is divided into two major sections: I. Understanding the Paradigm shift in marketing II. Theory and Practice Integration	$125.00	Add To Cart
Name: Module 6 - Arranging Mortgages **Details:** This module is to explain what constitutes mortgage brokering activity under the Mortgage Brokers Act (the Act), and when a person will require registration under the Act in order to perform those activities.	$125.00	Add To Cart
Name: Module 7 - Contract Law - Part 1 **Details:** An introduction to contract law for mortgage brokers.	$125.00	Add To Cart
Name: Module 8 - Contract Law - Part 2 **Details:** An introduction to contract law for mortgage brokers	$125.00	Add To Cart
Name: Module 9 - Suitability **Details:** This module covers the topic of Suitability as it applies to a Mortgage Broker's application for license or renewal.	$125.00	Add To Cart
Name: Regulatory Update (approved for publication April 13, 2018) **Details:** Regulatory Update (approved for publication April 13, 2018)	$135.00	Add To Cart
Name: Second Mortgage Strategies **Details:** Second mortgages are common place. Registering them requires informed broker advice and client decisions. Does a borrower have the right to take out a second mortgage or can doing so cause the first mortgage to become due? What can a second mortgage lender do to take priority over later advances made by a first mortgage lender? What can a first mortgage lender do to better protect priority? The answers to these and related questions may surprise you, as may how easy (but rarely taken) the steps are to better protect your client and you.	$59.95	Add To Cart
Name: The Essentials of Commercial Lending **Details:** This module provides an overview of lending in the Industrial / Commercial / Investment market.	$59.95	Add To Cart

For more information please email education@mbibc.ca or contact us at: Suite 902 - 777 West Broadway, Vancouver, B.C. V5Z 1J5 * 877-371-2916 or through our Contact Page All prices are in Canadian dollars.


BC
mbi
MORTGAGE
BROKERS
INSTITUTE

Appendix 34

CMBA-BC – *Event; Dialed-in With CMBA-BC: FINTRAC Reporting* – Feb 14, 2019

DIALED-IN WITH CMBA-BC: FINTRAC REPORTING

Title:	Dialed-In with CMBA-BC: FINTRAC reporting
Location:	Conference Call
Start date:	14 February, 2019
Cost:	$0.00 for members

REGISTER NOW

The BC Provincial government has commissioned an investigation into money laun
with a particular focus on mortgage brokering and lending (see recent press releas

CMBA-BC will be hosting a round table discussion on this topic, and Members are ir
views with us.

DATE: THURSDAY, FEBRUARY 14

TIME: **** CHANGED TO 3:00PM START ****

- Are there challenges in identifying the problem?
- Is this about “unexplained income” or “cleaning money”.
- What do you see as solutions, which may be both specific and broad in scope?

We will follow up with registrants to provide conference call connection detai

Appendix 35

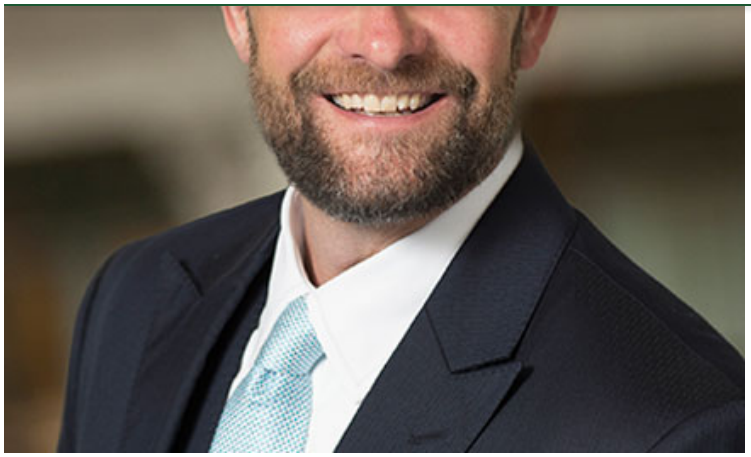
CMBA-BC – *Expert Speaker Series; Taking Action Against Money* Laundering – April 4, 2019

EXPERT SPEAKER SERIES – BURNABY, APRIL 4, 2019

Title:	Expert Speaker Series - Burnaby
Location:	
Start date:	04 April, 2019
Cost:	$39.00 for members or $59.00 for non-members

REGISTER NOW

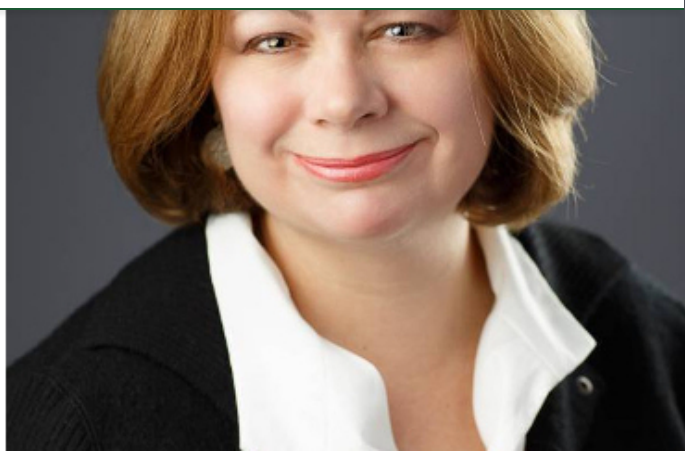
FEATURED SPEAKERS WILL INCLUDE:



TIM LACK

Lawyer at Bridgehouse Law LLP

Legal Hot Topics in Mortgage Lending



SAMANTHA GALE

CEO, CMBA-BC

Taking Action Against Money Laundering

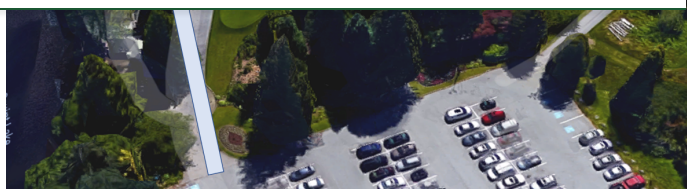
Learn about the issues that real estate lawyers are seeing in their practices and the emerging legal trends that are shaping the mortgage industry, including:

- Penalties, real penalties and deemed penalties
- Renewals Discharges
- Unconscionable Mortgages
- GST super priority
- Lending to an estate

Samantha's presentation will focus on the role that policy makers expect our members play in mitigating money laundering activities. She will also outline the initiatives that other real estate sector associations a industry groups have proposed.

7600 Halifax St, Burnaby, BC

PRICE: only $39 for CMBA-BC Members



Appendix 36

CMBA-BC – *Expert Speaker Series: An Update on BC AML Policies* – May 30, 2019

EXPERT SPEAKER SERIES – VANCOUVER MAY 30, 2019

Title:	Expert Speaker Series - Vancouver
Location:	Chateau Granville Hotel & Suites, 1100 Granville Street, Vancouver
Start date:	30 May, 2019
Cost:	$39.00 for members or $59.00 for non-members

REGISTER NOW

May 30, from 9:00am – 11:

Join us in Vancouver to he
topics that matter to mor

- ***Foreclosures and Mortg***
  Who's on First?
  With Andrew Bury, QC
- ***Assisting Credit Challe***
  With Bill Macklem, Mortg
- ***An Update on BC Anti M***
  With Samantha Gale, CE(

ANDREW BURY, QC

Lawyer at Gowling WLG

Foreclosures and Mortgage Priorities;

Who's on First?

Times may be getting tougher and more foreclosures may be on the horizon. Are you prepared?

You are a lender-broker. Your borrower won't pay you – what can you do, what can't you do in the foreclo

You are a broker advising a lender or a borrower. How can you structure the deal to minimize later probl possibly develop a returning client?

What amounts can you collect in the foreclosure? Can you foreclose on just one of two registered owners between guarantors and covenantors when it comes to foreclosure? How long do you have before the rig Ask your questions of expert Andrew Bury, QC.

If you have a question concerning foreclosure, Andrew is the right person to ask! If you don't have a ques
valuable lender and broker contacts.

BILL MACKLEM

Mortgage Broker

Dominion Macklem Mortgages

Assisting Credit Challenged Borrowers

Legendary BC mortgage broker Bill Macklem will discuss how you can assist credit challenged mortgage b
your delinquent borrowers back on track. This is your opportunity to ask an industry veteran about your
origination challenges and receive some practical, detailed advice.

Bill has been a mortgage broker since 1987, beginning in Edmonton and moving to B.C. in 1994. He move
RE/MAX Western Canada asked him to develop a mortgage broker program in the Fraser Valley. He joine
in 2007, establishing the Dominion Macklem Mortgages franchise with offices in the Lower Mainland and
office in White Rock and you will be surrounded by sports memorabilia from the 1972 Russia v. Canada w
Lions Grey Cup Championship, Jon Montgomery's Gold Medal victory in the 2010 Olympic Skeleton event
well over one billion dollars of mortgage funding in his career and is a member of the CMBA MB Funding
Tier.

SAMANTHA GALE

CEO, CMBA-BC

An Update on BC Anti Money Laundering Policies

Samantha will deliver an overview of the two new government reports on money laundering, and explain
mortgage brokers and mortgage lenders in BC.

Appendix 37

CMBC-BC – *Briefing Note: Mortgage Brokers Act Consultation: Independence in the Adjudication Process* – April 20, 2020

CANADIAN MORTGAGE BROKERS ASSOCIATION BRITISH COLUMBIA

April 20, 2020

BRIEFING NOTE

Mortgage Brokers Act Consultation: Independence in the Adjudication Process

On behalf of the Canadian Mortgage Brokers Association - BC (CMBA-BC), I thank you for the opportunity to make submissions in response to the consultation by the Ministry of Finance on proposed amendments to the Mortgage Brokers Act (the "MBA").
In this brief, we are reviewing independence in the adjudication process for determining breaches of the MBA and disciplining registrants.

Current Status

Under the MBA, the Registrar, who is appointed by the Lieutenant Governor in Council, adjudicates disciplinary matters, which are pursued by the Registrar's staff under a Notice of Hearing. Generally, his staff will investigate suitability issues or suspected breaches of the MBA and collect relevant facts and evidence which are assembled into a hearing brief. Lawyers for the Attorney General act to represent the interests of the Registrar, and if warranted, will assist in a negotiation process to attempt to resolve the matter by way of consent, in the form of a Consent Order which is granted by the Registrar and signed by the opposing party. If matters cannot be resolved by consent, they proceed to a hearing, wherein, the Registrar will sit as an adjudicator. In several past hearings, another person has been appointed (presumably by the Registrar) to act as an adjudicator in his place.

Whether by consent or following a hearing, the Registrar can make various orders pursuant to the provisions of the MBA, which include:

a. Suspending or cancelling a person's registration;
b. Paying monetary penalties and costs; and
c. Directing a person to cease certain activities or perform certain activities.

Challenges with the Current Status

An all too frequent criticism of the MBA adjudication process by registration subjects is that it lacks fairness, as the adjudicator governs all aspects of the regulatory program under the MBA, including its staff, and the very investigative process which brings the subject before the Registrar for adjudication of allegations against him or her. Even if the BCFSA erect internal information firewalls on specific investigations between investigators and the ultimate adjudicator, there is still a clear perception of institutional bias. In the infamous English case of R. v. Sussex Justices, which concerned the impartiality and recusal of judges, the court found that the mere appearance of bias is sufficient to overturn a decision, as it is "of fundamental importance that justice should both be done and be manifestly seen to be done."

We know that disciplinary hearings conducted pursuant to the MBA need to meet the requirements of natural justice or the duty to act fairly. The Supreme Court of Canada in *Baker v. Canada (Minister of Citizenship and Immigration (1999)* set out a list of non-exhaustive factors that impact the nature of the duty of fairness required to be dispensed by a tribunal. Those factors include the nature of the decision being made and the process followed in making it, the statutory scheme under which the decision-maker operates, the importance of the decision to the person challenging it, the person's legitimate expectations, and the choice of procedure made by the decision-maker.

Professional disciplinary proceedings have been found to be quasi-judicial proceedings, requiring regulatory bodies to maintain independence in the decision-making process. In *Lim v. Assn. of Professional Engineers of Ontario*, 2011 ONSC 106, for instance, the discipline committee was found to lack independence from the staff who were tasked with providing it with logistical and administrative support. This lack of independence ultimately resulted in the extraordinary remedy of the committee's decision being quashed.

Ensuring that regulatory bodies both act impartiality and are seen to act impartially helps to instill confidence in them - not only from the industry members who they regulate but also from the public. This is critical requirement in building and maintaining a culture of compliance, within which proactive industry members believe in the value of regulation and its enforcement. Efforts to fight money laundering will be challenged when industry members do not have faith in the fairness and impartiality of a regulator – they may adopt an "us vs them" approach filled with distrust and extreme caution.

Other BC regulatory bodies, such as the BC Real Estate Council, which is soon to be incorporated under the BCFSA umbrella, have ensured that they have detailed, robust and clearly laid out adjudication processes which satisfy the rules of natural justice and procedural fairness.

For instance, the Real Estate Council has published a 9-page document, "*A Guide to RECBC's Consent Order Process,* which sets out the process for entering into consent orders with industry members. The rational for the detailed Consent Order process is set out in the beginning of the document:

> "Consent orders (COs) are not informal settlements of discipline matters; they result in formal discipline orders. COs are published and become part of a licensee's public discipline record**."**

Real Estate Council consent orders are reviewed by formal Consent Order Review Committees, which are comprised of a "combination of members of Council and possibly non-Council members appointed from approved rosters of lawyers and real estate industry professionals." Likewise, for hearings, the *Real Estate Services Act* (RESA) sets out detailed requirements for constituting hearing committees with permitted members including RESA licensees, lawyers or other persons with industry expertise sufficient to sit on a disciplinary panel.

Recommended Changes

In order to ensure the impartiality and the appearance of impartiality in the discipline process which is a fundamental component of natural justice and procedural fairness, the MBA should be amended to ensure that all license suitability matters and disciplinary proceedings are adjudicated by persons who are not paid BCFSA staff or contractors. In addition, adjudication should be undertaken by a panel or a committee which is comprised of lawyers, mortgage licensees or other related industry experts who have knowledge of the mortgage industry and compliance requirements. This will help instill confidence in the regulator amongst industry members and the public, which is essential to building a culture of compliance and tackling wide scale problems such as money laundering.

Yours truly,

Samantha Gale
CEO, Canadian Mortgage Brokers Association-BC