

Overview Report: Legal Professionals and Accountants Publications

A. Scope of Overview Report

1. This overview report sets out information related to works published by the Financial Action Task Force (“FATF”), FATF-style regional bodies, the Federation of Law Societies of Canada (“FLSC”) and certain regulatory bodies on the subject of money laundering through lawyers and accountants. Its purpose is to provide background and contextual information to those records as they may be referred to in *viva voce* evidence during Commission hearings.

B. Legal Professionals

2. The FATF *Guidance for a Risk-Based Approach for Legal Professionals* (2019) is attached as Appendix “A”.
3. The FATF *Professional Money Laundering* (2018) is attached as Appendix “B”.
4. The FATF *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (2013) is attached as Appendix “C”.
5. The FATF *Risk Based Approach Guidance for Legal Professionals* (2008) is attached as Appendix “D”.
6. The International Bar Association *A Lawyer’s Guide to Detecting and Preventing Money Laundering* (2014) is attached as Appendix “E”.
7. The Solicitors Regulation Authority *Anti-Money Laundering Report* (2016) is attached as Appendix “F”.
8. The Solicitors Regulation Authority *Preventing Money Laundering and Financing of Terrorism, A Thematic review* (2018) is attached as Appendix “G”.
9. The Solicitors Regulation Authority *Risk assessment Anti-money laundering and terrorist financing* (2018) is attached as Appendix “H”.

10. The Solicitors Regulation Authority *Guidance The Money Laundering, Terrorist Financing and Transfer of Funds* (March 2018, updated in November 2019) is attached as Appendix “I”.

11. The Legal Sector Affinity Group *Anti-Money Laundering Guidance for the Legal Sector* (2018) is attached as Appendix “J”.

C. FLSC Reports

12. The FLSC *Final Report on the Model Rules* (Amended October 1, 2018) is attached as Appendix “K”.

13. The FLSC *Guidance for the Legal Profession* (2019) is attached as Appendix “L”.

14. The FLSC *Model Rule on Cash Transactions* (2018) is attached as Appendix “M”.

15. The FLSC *Model Rule on Client Identification and Verification Requirements* (2018) is attached as Appendix “N”.

16. The FLSC *Model Trust Accounting Rule* (2018) is attached as Appendix “O”.

17. The FLSC *Guidance on Monitoring Obligations: Client Identification and Verification* (2020) is attached as Appendix “P”.

18. The FLSC *Guidance on Using an Agent* (2020) is attached as Appendix “Q”.

19. The FLSC *Risk Assessment Case Studies for the Legal Profession* (2020) is attached as Appendix “R”.

20. The FLSC *Risk Advisories for the Legal Profession* (2019) is attached as Appendix “S”.

D. Accountants

21. The FATF *Guidance for a Risk-Based Approach for the Accounting Profession* (2019) is attached as Appendix “T”.

22. The Chartered Professional Accountants Canada *Guide to Comply with Canada's Anti-Money Laundering (AML) Legislation* (2014) is attached as Appendix "U".



GUIDANCE FOR A RISK-BASED APPROACH

LEGAL PROFESSIONALS



JUNE 2019



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 (2019), *Guidance for a Risk-Based Approach for Legal Professionals*, FATF, Paris, www.fatf-gafi.org/publications/documents/Guidance-RBA-legal-professionals.html

© 2019 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredits coverphoto ©Getty Images

TABLE OF CONTENTS

Acronyms	3
Executive Summary	4
Section 1- Introduction and key concepts.....	5
Background and context.....	5
Purpose of the Guidance.....	6
Target audience, status and content of the Guidance	7
Scope of the Guidance: terminology, key features and business models.....	8
Terminology.....	8
Services provided by legal professionals and their vulnerabilities for ML/TF.....	12
Services performed by notaries.....	17
FATF Recommendations applicable to the legal professionals	17
Section II- The RBA to AML/CFT	19
What is the RBA?	19
The rationale for the RBA	19
Application of the RBA	20
Challenges	21
Allocating responsibility under a RBA	24
Identifying ML/TF risk.....	24
Assessing ML/TF risk.....	25
Mitigating and managing ML/TF risk.....	25
Developing a common understanding of the RBA.....	26
Section III – Guidance for legal professionals	27
Risk identification and assessment.....	27
Country/Geographic risk.....	29
Client risk.....	30
Transaction/Service risk.....	35
Variables that may influence risk assessment	38
Documentation of risk assessments.....	41
Risk management and mitigation.....	42
Initial and ongoing CDD (R.10 and 22)	43
Ongoing monitoring of clients and specified activities (R.10 and 23).....	47
Suspicious transaction reporting, tipping-off, internal control and higher-risk countries (R.23)	49
Section IV- Guidance for supervisors	54
Risk-based approach to supervision.....	54
Supervisors and SRBs’ role in supervision and monitoring.....	55
Background: national frameworks and understanding ML/TF risk- the role of countries	55
Mitigating and managing ML/TF risk.....	57
Supervision of the RBA	58

Licensing or Registration.....	58
Monitoring and supervision	61
Enforcement.....	62
Guidance	62
Training.....	63
Endorsements	63
Information exchange.....	63
Supervision of beneficial ownership and source of funds/wealth requirements.....	64
Sources of funds and wealth	66
Nominee arrangements	66
Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom a legal professional provides services	69
Annex 2: Sources of further information	74
Annex 3: Glossary of terminology	79
Annex 4: Supervisory practices for implementation of the RBA	82
Annex 5: Examples of Red flags highlighting suspicious activities or transactions for legal professionals	92
Annex 6: Members of the RBA Drafting Group	94

Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client ¹ due diligence
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

¹ In some jurisdictions or professions, the term “customer” is used, which has the same meaning as “client” for the purposes of this document.

Executive Summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that competent authorities, supervisors and legal professionals should identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which legal professionals are exposed, and implement appropriate mitigation measures. This approach enables allocation of resources where the risks are higher.
2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a [general presentation](#) of the RBA and provides [specific guidance](#) for legal professionals and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the profession.
3. The Guidance acknowledges that legal professionals operate within a wide range of business structures - from sole practitioners to large, multi-national firms and provide a variety of services in different jurisdictions. Given the diversity in scale, activities and risk profile, there is, therefore, no one-size-fits-all approach.
4. The development of the ML/TF risk assessment is a key starting point for the application of the RBA. It should be commensurate with the nature, size and complexity of the law firm. The most commonly used risk criteria are country or geographic risk, client risk and service/transaction risk. The Guidance provides [examples of risk factors](#) under these risk categories.
5. The Guidance highlights that it is the responsibility of the senior management of legal professionals to foster and promote a culture of compliance. They should ensure that legal professionals are committed to manage ML/TF risks when establishing or maintaining relationships.
6. The Guidance highlights that legal professionals should design their policies and procedures so that the level of initial and ongoing CDD measures addresses the ML/TF risks to which they are exposed. The Guidance thus explains the obligations for legal professionals regarding identification and verification of [beneficial ownership information](#) and provides examples of standard, simplified and enhanced CDD measures based on ML/TF risk.
7. The Guidance has a [section for supervisors](#) of legal professionals and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the RBA to supervision as well as supervision of the RBA by providing specific guidance on licensing or registration requirements for the profession, mechanisms for on-site and off-site supervision, enforcement, guidance, training and the value of information-exchange between the public and private sector.
8. The Guidance highlights the importance of [supervision of beneficial ownership](#) requirements and [nominee arrangements](#). It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained and made available in a timely manner.

Section 1- Introduction and key concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org.

- a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the FATF Glossary
- b) Other relevant FATF Guidance documents such as:
 - The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
 - FATF Guidance on Transparency and Beneficial Ownership (October 2014)
 - FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs) (June 2019)
 - FATF Guidance on the Risk-Based Approach for Accountants (June 2019)
- c) Other relevant FATF reports such as:
 - FATF Report on Money Laundering and Terrorist Financing: Vulnerabilities of Legal Professionals (June 2013)
 - The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

Background and context

9. The RBA is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012². The FATF has reviewed its 2008 RBA Guidance for Legal Professionals, in order to bring it in line with the new FATF requirements³ and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to legal professionals when they prepare for, or carry out, transactions for their clients concerning certain specified activities⁴.

² [FATF \(2012\)](#).

³ The FATF Standards are comprised of the [FATF Recommendations](#), their Interpretive Notes and applicable definitions from the Glossary.

⁴ The services provided by legal professionals include those provided by both lawyers and notaries, and these services are included under bullet (e) of the definition of “Designated non-financial businesses and professions” in the FATF Glossary. For details about specified activities of legal professionals under R.22 and other FATF Recommendations applicable to the legal professionals, please refer to paragraph 20 of this Guidance.

10. This Guidance was drafted by a project group comprising FATF members and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 5.

11. The FATF adopted this updated RBA Guidance for legal professionals at its June 2019 Plenary.

Purpose of the Guidance

12. The purpose of this Guidance is to:

- a) Assist legal professionals in the design and implementation of a RBA to AML/CFT compliance by providing guidelines and examples of current practice, with a particular focus on providing guidance to sole practitioners and small firms;
- b) Support a common understanding of a RBA for legal professionals, financial institutions and designated non-financial businesses and professions (DNFBPs)⁵ that maintain relationships with legal professionals (e.g. through pooled or client accounts or for trust and company accounts) and competent authorities and self-regulatory bodies (SRBs)⁶ responsible for monitoring the compliance of legal professionals with their AML/CFT obligations;
- c) Outline the key elements involved in applying a RBA to AML/CFT applicable to legal professionals;
- d) Assist financial institutions and DNFBPs that have legal professionals as clients in identifying, assessing and managing the ML/TF risk associated with legal professionals and their services;
- e) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to legal professionals, particularly R.22, 23 and 28;
- f) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;
- g) Support the effective implementation of action plans of national risk assessments (NRAs) conducted by countries; and
- h) Support the effective implementation and supervision by countries of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

⁵ Including both legal and natural persons, see definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary.

⁶ See definition of the term 'Self-regulatory body' in the FATF Glossary.

Target audience, status and content of the Guidance

13. This Guidance is aimed at the following audience:
- a) Legal professionals;
 - b) Countries and their competent authorities, including AML/CFT supervisors of legal professionals, AML/CFT supervisors of banks that have legal professionals as customers, and Financial Intelligence Units (FIUs); and
 - c) Practitioners in the banking sector, other financial services sectors and DNFBPs that have legal professionals as customers.
14. The Guidance consists of four sections. Section I sets out introduction and key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific guidance to legal professionals (Section III) and guidance to supervisors of legal professionals on the effective implementation of a RBA (Section IV). There are six annexes on:
- a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom a legal professional provides services (Annex 1);
 - b) Sources of further information (Annex 2);
 - c) Glossary of terminology (Annex 3);
 - d) Supervisory practices for implementation of the RBA (Annex 4);
 - e) Red flag indicators highlighting suspicious activities or transactions for legal professionals (Annex 5); and
 - f) Members of the RBA Drafting Group (Annex 6).
15. This Guidance recognises that an effective RBA will take into account the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile a country's legal professionals and the risk profile of individual legal professionals operating in the sector and their clients. The Guidance sets out different elements that countries and legal professionals could consider when designing and implementing an effective RBA.
16. This Guidance is non-binding and does not overrule the purview of national authorities⁷, including on their local assessment and categorisation of legal professionals based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and legal professionals to implement effectively applicable FATF Recommendations. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. Legal professionals should also refer to relevant legislation and sector guidance of the country where their clients are based.

⁷ National authorities should however take the Guidance into account when carrying out their supervisory functions.

Scope of the Guidance: terminology, key features and business models

Terminology

Legal professionals

17. The FATF Recommendations apply to all legal professionals when they carry out specified transactional activities for third parties (see below) and do not apply to all activities carried out by legal professionals. Most notably, litigation is not a specified activity, and a legal professional representing a client in litigation will not be subject to the FATF Recommendations; unless during the course of such representation the legal professional additionally engages in one or more specified activities, in which case the Recommendations will apply to this specified activity or activities only. The FATF Recommendations do not apply where a person provides legal services 'in-house' as an employee of an entity that does not provide legal services.

18. The legal sector comprises a broad spectrum of practitioners and is not a homogenous group, from one country to another or even within a country. For the purposes of this Guidance, legal professionals include barristers, solicitors and other specialist advocates and notaries. In addition to obligations they may owe through the contracting of their services, legal professionals owe special duties both to their clients (e.g. duties of confidentiality and loyalty), as well as public duties to the legal institutions of their jurisdictions (e.g. through roles such as 'officers of the court'). These duties are designed to assist in the administration of justice and promote the rule of law, and generally set legal professionals apart from other professional advisors. In many jurisdictions, these duties and obligations are enshrined in law, regulations or court rules pursuant to historic and well established practices.

19. Titles given to different legal professionals vary among countries and legal systems, with the same title not always having the same meaning or area of responsibility. Although some common elements may exist based on whether the country has a common law or civil law tradition, even these generalisations will not always hold true. As the range of services provided and carried out by legal professionals is diverse and varies widely from one country to another, it is important to understand the specific roles undertaken by different legal professionals within their respective countries when assessing the AML/CFT obligations of the legal profession sector, as well as how these services interact with those of other professionals. Many legal professionals are required to comply with specific national legislation, rules and regulations adopted by professional associations or other SRBs.

20. R.22 provides that the customer due diligence and record-keeping requirements of the Recommendations apply to legal professionals when they prepare for and carry out certain specified activities for their clients, namely:

- a) Buying and selling of real estate;
- b) Managing of client money, securities or other assets;
- c) Management of bank, savings or securities accounts;
- d) Organisation of contributions for the creation, operation or management of companies; and
- e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

21. The FATF Recommendations set an international standard, which countries should implement through measures adapted to the circumstances of their particular jurisdictions. In general terms, jurisdictions have closely followed the FATF Recommendations but differences exist and legal professionals need to carefully consider the laws, rules and regulations of the relevant jurisdictions as implemented in such jurisdictions. The overarching concept of the obligations applying to certain specified activities (as set out in paragraph 20) is considered to be common across all jurisdictions.

22. Some legal professionals and law firms may accordingly be able to conclude that based on the services they provide, they do not have any specific AML/CFT obligations as they do not prepare for, or carry out any of the specified activities. Even though specific AML/CFT obligations may not apply to a legal professional or a law firm, it is consistent with the overall ethics and best practices of the profession for all legal professionals to ensure that their services are not being misused, including by criminals. Accordingly, legal professionals and law firms should carefully consider what they need to do to guard against that risk irrespective of the application of specific AML/CFT obligations in order not to be unwittingly involved in ML/TF.

23. Legal professionals provide advisory services and representation to members of society, companies and other entities to

- a) understand their increasingly complex legal rights and obligations;
- b) facilitate business transactions;
- c) assist their clients to comply with laws; and
- d) provide access to justice and judicial redress.

24. They may provide these services alone, in collaboration with other independent legal professionals or as partners or as members of a law firm. A firm may consist of a sole practitioner or a few practitioners or thousands of legal professionals spread throughout numerous offices around the globe. There are also alternative business structures in which legal professionals combine with non-legal professionals to form partnerships. Most legal professionals practise alone or with other legal professionals in small firms.

25. Legal professionals include barristers, solicitors and other types of specialist advocates, however called. Typically, these legal professionals represent clients in court and also, in some countries, provide advisory services that might include one of the specified activities in R.22 and, as set forth above, they will therefore need to comply in respect of such services.

26. Services provided globally by legal professionals include advising on clients' financial transactions and legal structures that involve financial or business arrangements. As a result of their regulated status and to assist clients in transactions, legal professionals may also hold clients' funds in designated accounts or agree to act on behalf of clients (e.g. under a power of attorney) in relation to specific aspects of transactions. However, the counselling and advisory roles of legal professionals, especially in an increasing regional and global marketplace, do not generally involve handling funds. Legal professionals frequently work in collaboration with other professional advisors on transactions, such as accountants, TCSPs, escrow agents and title insurance companies and may refer their clients to particular professionals for services. Flows of funds are also often dealt with and facilitated exclusively by financial institutions.

27. The work of legal professionals is fundamental to promoting adherence to the rule of law. Legal professionals are typically regulated by laws, professional standards and codes of ethics and conduct. Breaches of the obligations imposed upon them can result in a variety of sanctions, including civil, contractual, disciplinary and criminal sanctions.

Legal professional privilege and professional secrecy

28. The actions and behaviours discussed in this Guidance are subject to applicable professional privilege and professional secrecy. Privilege/professional secrecy is a protection to the client, and a duty of the legal professional. Privilege (a common law concept existing in jurisdictions such as England and Wales and the United States) and professional secrecy (a civil law concept existing in jurisdictions such as Germany and France) aim to protect client information or advice from being disclosed. Though the two concepts differ in scope and purpose, both are founded on the nearly universal principle of the right of access to justice and the rationale that the rule of law is protected where clients are encouraged to communicate freely with their legal advisors without fear of disclosure or retribution. R.23 and the accompanying INR.23 recognise concepts of privilege and professional secrecy.

29. The degree and scope of legal professional privilege or professional secrecy and the consequences of a breach of these principles vary from one country to another and are determined by the relevant national laws.

30. In some jurisdictions, the protections against non-disclosure may be overridden by the consent or waiver of the client or by express provisions of law. Most jurisdictions seek to balance the right of access to justice and the public interest in investigating and prosecuting criminal activity. Accordingly, legal professional privilege or professional secrecy does not protect a legal professional from knowingly facilitating a client's illegal conduct.⁸ Moreover, the protections against non-disclosure may not exist where the "crime/fraud" exception applies. Under the "crime/fraud" exception to privilege, privilege is not created where there is an illegal purpose whether or not the legal professional is aware of the illegality or is complicit in the illegality. The extent of that exception is a matter of national law.

31. Each country needs to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover some information that legal professionals receive from or obtain through their clients: (a) in the course of ascertaining the legal position of their clients, or (b) in performing their task of defending or representing their clients in, or concerning judicial, administrative, arbitration or mediation proceedings. There may be cases in which these professionals conduct activities that are clearly covered by the legal privilege (i.e. ascertaining the legal position of their client or defending or representing their client in judicial proceedings) alongside activities that may not be covered by it. In addition, within a single matter, privilege may attach to some but not all communications and advice.

32. A number of the DNFBP sectors, including legal professionals, are already subject to regulatory or professional requirements (including as promulgated by SRBs) that complement AML/CFT measures. For example, by virtue of their professional codes of conduct, many legal professionals are already subject to an obligation to identify their clients

⁸ Also see IBA and the secretariat of the OECD: Report of the Task Force on the Role of Lawyers and International Commercial Structures (May 2019): Full Report and Executive Summary.

(e.g. to check for conflict of interest) and the substance of the matter submitted to them by such clients, to appreciate the consequences that their advice may have. If a legal professional provides legal advice to a client that helps the client commit an offence, that legal professional may, depending on the legal professional's state of knowledge, become an accomplice to the offence.

33. This Guidance must be considered in the context of these professional and ethical codes of conduct. In situations where legal professionals are claiming legal professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules. For example, it is important to distinguish between legal advice, which generally is subject to robust protections, and underlying facts, which in many cases are not protected by privilege.

Role of notaries as a legal professional

34. Both civil and common law countries have notaries, but the main difference between them is the roles that they play in their respective jurisdictions. In some common law countries, a notary public is a qualified, experienced practitioner, trained in the drafting and execution of legal documents. In other common law countries, a notary public is a public servant appointed by a governmental body to witness the signing of important documents (such as deeds and mortgages) and administer oaths. Notaries provide legal advice in the context of documenting transactions and legal arrangements, and do not necessarily direct this advice to a specific party. In some common law countries, such as the UK, the notary is no longer required for documenting transactions.

35. Most civil law notaries are members of autonomous legal professions (regulated by law) and qualified public officials, as they are appointed by the State through a selective public competition among law graduates. Civil law notaries, who are bound by an obligation of independence and impartiality with respect to parties to a transaction, must be regarded, in matters of real estate property (conveyancing), family law, inheritance and corporate legal services (e.g. the formation of companies, sale of shares, capital increases, liquidation and dissolution of companies), as practising non-adversarial activities. They act as gatekeepers by drafting and ensuring the legality and certainty of the instruments, and the authenticity of the content of the instrument and in some jurisdictions, also provide a public fiduciary function by performing the role of trusted third parties. Civil law notaries are obliged by law to remain impartial, fair and independent as between the parties they are advising, including bearing in mind any disparity of power between the parties. For this reason, civil law notaries are assigned functions of a public nature as part of their legal assignments and typically do not act for one of the parties in an advisory capacity.

36. In civil law jurisdictions, as notaries are entrusted with public functions, they act as public office holders in accordance with the principles of impartiality, legality, certainty and independence. In these jurisdictions, the involvement of notaries in transactions includes the notaries' responsibility and the specific legal value of the notarial form established by law. This legal framework for civil law notaries ensures a high degree of legal certainty and enhances the traceability and transparency of transactions between the parties. Notarial deeds as authentic instruments are recognised as a particular form of evidence, which is taken to be authoritative and in certain cases, as judicially enforceable as court orders and judgments and, sometimes, are an indispensable step in order to obtain other effects such as *traditio*, right of first refusal, third-party effectiveness and registration in substantive and administrative registries. State powers are therefore effectively delegated to civil law

notaries so that they can assign “public authority” to the authentic instruments they establish and are responsible for. The obligations of fairness and public office mean that services performed by civil law notaries are often very different in nature to the services provided by other legal professionals.

37. Notaries are subject to a duty of professional secrecy, as well as generally being subject to a duty to respect rights to confidentiality. Notaries are the party to interpret these duties in the light of their overarching obligation to ensure the common good and the general interests of society. Therefore, in practice, professional secrecy is not an absolute duty and is often subordinated to the public interest. Notaries may also be required to disclose the contents of their archives and communications in criminal proceedings or when required by law. In the context of ML/TF, notaries are obliged to co-operate with law enforcement, and to disclose all the relevant information to the competent authorities, in accordance with the laws of the jurisdiction. Notification to public authorities of any suspicious transactions should not be considered as an infringement of the notary’s duty of professional secrecy. Information received by the civil law notaries in respect of a client and which is being transferred to the competent FIU in conformity with the AML/CFT legislation still remains confidential information.

38. This Guidance does not cover some common law notaries when those notaries perform merely administrative acts such as witnessing or authenticating documents, as these acts are not specified activities.

Services provided by legal professionals and their vulnerabilities for ML/TF

39. Legal professionals provide a vast range of services to a diverse range of clients. For example, services may include (but are not restricted to):

- a) Advising on the purchase, sale, leasing and financing of real property;
- b) Tax advice;
- c) Advocacy before courts and tribunals;
- d) Representing clients in disputes and mediations;
- e) Advice in relation to divorce and custody proceedings;
- f) Advice on the structuring of transactions;
- g) Advisory services on regulations and compliance;
- h) Advisory services related to insolvency/receiver-managers/bankruptcy;
- i) Administration of estates and trusts;
- j) Assisting in the formation of entities and trusts;
- k) Trust and company services⁹;
- l) Acting as intermediaries in the trade of citizenship and residency or acting as advisors in residence and citizenship planning;

⁹ For such activities, refer also to the guidance on risk-based approach for Trust and Company Service Providers (TCSPs).

- m) Providing escrow services and token custody services in connection with legal transactions involving an initial coin offering or virtual assets;
- n) Legitimising signatures by confirming the identity of the signatory (in the case of notaries); and
- o) Overseeing the purchase of shares or other participations (also in the case of notaries).

40. While some of these services may involve activities that fall within the scope of the specified activities under R.22, not all (e.g. representing clients in disputes and mediations; providing advice in relation to divorce and custody proceedings; or providing advisory services on regulations) will do so. When considering the range of tasks undertaken by legal professionals only specified activities under R.22 are subject to the AML/CFT regime.

41. The specifics of the risk-based processes should accordingly be determined based on the activities undertaken by the legal professional, the ethical and existing supervisory structure for legal professionals and the susceptibility or vulnerability of activities of a legal professional to ML/TF. Firms with offices in multiple jurisdictions should apply a consistent approach across all of its offices with a general compliance tone from the top.

42. A RBA requires legal professionals to mitigate the risks that they face and with due regard to the resources available. Mitigating practices will invariably include initial CDD and ongoing monitoring, as well as a range of internal policies, training and systems to address the vulnerabilities faced in the particular practice setting of the legal professional. This section does not attempt to exhaustively list the mitigating practices that may be employed by legal professionals. For information on ways in which legal professionals might mitigate their vulnerabilities to ML/TF, see “Section 2 – Guidance for Legal professionals and Notaries” and chapters III and IV of the separate publication: “*A Lawyer’s Guide to Detecting and Preventing Money Laundering*” published in October 2014 by a collaboration of the International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe¹⁰.

Client funds

43. Most legal professionals can hold funds of clients. Client accounts are accounts held by legal professionals with a financial institution. In some civil law countries, a professional body holds the funds of clients, rather than legal professionals. For example, in France, where funds are held in CARPA (see Annex 4 “France”). Operating client accounts does not automatically require a legal professional to observe AML/CFT obligations. These obligations apply when the accounts are used in conjunction with a specified activity under R.22.

44. In most countries, legal professionals are required to hold client funds in a separate account with a financial institution and use the funds only in accordance with their client’s instructions. In countries where client accounts are used, legal professionals are required to hold client funds separate from their own. The purpose of these accounts is to hold client funds in “trust” for or for a purpose designated by the client. Funds will also be

¹⁰ The full publication is available at:
www.ibanet.org/Article/NewDetail.aspx?ArticleUid=f272a49e-7941-42ee-aa02-eba0bde1f144

held or received for payment of costs incurred by the legal professional on behalf of the client. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the legal professional is required to account for these funds.

45. The use of client accounts has been identified as a potential vulnerability, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional. Legal professionals can seek to limit their exposure to this risk by developing and implementing policies on the handling of funds (e.g. currency value limits) as well as restricting access to the account details of the client account in order to prevent unsanctioned deposits into the client account.

Advising on the purchase and sale of real property

46. Real estate, both commercial and residential, accounts for a high proportion of confiscated criminal assets, demonstrating that this as a clear area of vulnerability. In many countries, legal professionals are either required by law to undertake the transfer of property or their involvement is a matter of tradition, custom or practice. However, the specific role of legal professionals in real estate transactions varies significantly from country to country, or even within countries. In some countries, legal professionals will customarily hold or control (e.g. through a financial institution) and transfer or control the transfer of the relevant funds for the purchase of the real estate assets. In other countries this will be done by other parties, such as a title insurance company or escrow agent. Even if legal professionals are not handling the funds, they will typically be aware of the financial details and in many cases will be in a position to inquire about the transaction where appropriate.

47. Some criminals may seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership of the real estate. Alternatively, criminals may seek to obscure the ownership of real property by using false identities or title the property in the names of family members, friends or business associates, or purchase property through an entity or a trust. Legal professionals should consider carefully who they are acting for at the outset of a real estate transaction, especially where there are multiple parties involved in a transaction. In some cases, legal professionals may also opt to apply specific checks on the settlement destinations of transactions (i.e. performing limited diligence on the seller of real property, when acting for the buyer and the seller and the buyer appear to be related parties).

Formation of companies and trusts¹¹

48. In some countries, legal professionals (in civil law jurisdictions this will usually be a notary) must be involved in the formation of a company. In other countries members of the public are able to register a company themselves directly with the company register, in which case a legal professional's advice is sometimes sought at least in relation to initial liability management, corporate, tax and administrative matters.

49. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of

¹¹ The illustrations could also apply to other legal persons and arrangements.

the assets. Companies and often trust and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies¹², which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies¹³ formed by legal professionals by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

Management of companies and trusts

50. In some cases, criminals will seek to have legal professionals involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude a legal professional from acting as a trustee or as a company director, or require a disclosure of directorship positions to ensure independence and transparency is maintained. In countries where this is permitted, there are diverse rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will determine whether any funds relating to activities by the company or trust can go through the relevant legal professional's client account. In addition, in some countries, the non-legal counsel of a legal professional acting in a business capacity for formation or management of companies or trusts may not be protected by the legal professional privilege.

Acting as nominee

51. Individuals may sometimes have legal professionals or other persons hold their shares as nominees, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to 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. Legal professionals should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where legal professionals are asked to act as nominees, they should understand the reason for this request and ensure that they are able to verify the identity of the beneficial owner of the shares and that the purpose is legitimate.

General management of client affairs

52. In some jurisdictions, legal professionals may undertake a range of 'management' activities for clients permitted in limited circumstances by some professional rules. In some European jurisdictions, this is sometimes referred to as 'man of affairs work'.

¹² A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

¹³ A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

Situations where a legal professional may be undertaking these activities legitimately may involve a client who has limited capacity to manage his/her own affairs, or in other circumstances where the client has a clear legitimate rationale for seeking the continuing assistance from the 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. While ordinarily this type of activity should give the legal professional access to sufficient information to make considered assessments of a client's legitimacy under a RBA, it is possible that criminals will seek to use such ancillary services, in addition to legal services, to minimize the number of advisors and third parties who have access to the client's financial and organizational details. Legal professionals should carefully scrutinize any request to take on additional obligations for a client beyond their primary services and consider the justification of such a request in the totality of the circumstances and its overall legitimacy.

Other services that might indicate ML/TF activity

53. Legal professionals possess a range of specialised legal skills that 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 and arrangements, 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 encounter 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 funds 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 or creditor. Where these circumstances involve legal professionals engaging in a specified activity, legal professionals must carefully consider their AML/CFT obligations. Legal professionals should also consider the ML/TF risk in such circumstances.

54. Many aspects of this Guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply a RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. Legal professionals may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this Guidance, legal professionals and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.¹⁴

¹⁴ For example, legal professionals may be subject to mandatory disclosure rules, requiring them to report arrangements that have the hallmarks of tax evasion to the tax authority. Legal professionals may also commit an offence where they facilitate the commission of tax evasion. These initiatives require legal professionals and supervisors to take many of the steps outlined in this Guidance to ensure they fulfil their obligations under applicable law.

Services performed by notaries

Overseeing the purchase of shares or other participations

55. Notaries are often involved in reviewing the documentation for the transfer of shares and/or for transactions that enable participation in a company's equity. It is possible for criminals to use fictitious or misleading accounting methods to distort the apparent value of a company, including by diminishing it in order to hide or obscure transfers of value. Although a notary is generally not responsible for verifying the 'true' value of companies, notaries may encounter information in the course of their duties that is at odds with the presented valuation of a company.

Legitimisation of identities of signatory

56. In certain situations, the intervention of a notary is required to legitimise the execution of a private document. Although this technically relates only to verifying the identity of the signing parties, notarisation can often lend an impression of credibility to the content of the document. Criminals may use this form of notarisation service to lend credibility, in particular, to information contained in such documents that asserts the identity of the owners of assets, thereby potentially hiding its true owners.

Legalisation of old documents

57. In certain situations, the intervention of a notary is required for the legalisation of private documents drafted several years before the time of notarisation. The purpose of this service is to provide certainty in relation to the validity of old documents. Criminals may seek to use such services in relation to documents that falsely assert that transactions occurred many years ago, in circumstances that cannot otherwise be verified.

Opening of safe deposit boxes

58. Notaries may be present at the opening of a safe deposit box held at a bank that is opened in the name of a deceased person. This service is to certify the contents of the safe deposit box. Criminals may fraudulently place contents that were not the property of the deceased person in such a deposit box in order to ensure that the title to this property passes in an apparently legitimate and 'clean' transfer from the estate of the deceased to the same criminal enterprise as the beneficiaries of the estates.

FATF Recommendations applicable to the legal professionals

59. The basic intent behind the FATF Recommendations as it relates to legal professionals is to ensure that their operations and services are not abused for facilitating criminal activities and ML/TF. This is consistent with the role of legal professionals, as guardians of justice and the rule of law namely to avoid knowingly assisting criminals or facilitating criminal activity. The requirements of R.22 regarding CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R.10, 11, 12, 15 and 17 should apply to legal professionals in certain circumstances.

60. R.22 mandates that the requirements for CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R. 10, 11, 12, 15 and 17 apply to legal professionals in certain circumstances. R.22 applies to legal professionals when they prepare

for and carry out certain specified activities. Unless legal advice and representation consist of preparing for or carrying out one or more of these specified activities, legal professionals are not subject to the FATF Recommendations. This Guidance has been prepared to assist in situations where legal professionals prepare for and carry out transactions for the clients concerning the specified activities. For example, FATF Recommendations would not be applicable if a legal professional only provides litigation advice or routine advice at legal aid or other legal help clinics.

61. Where more than one law firm or legal professional prepares for or carries out a transaction, each firm or legal professional must comply with the applicable CDD, record-keeping and other AML/CFT obligations. Where permitted, legal professionals may rely on third parties in accordance with R.17 to perform elements (a)-(c) of the CDD measures set out in R.10 or to introduce business. Where not all legal professionals are preparing for or carrying out the transaction, those legal professionals providing advice or services (e.g. a general legal opinion on the applicability of a local law) peripheral to the transaction need not be subject to the AML/CFT obligations.

62. R.23 requires that measures set out in R.18 (Internal controls and foreign branches and subsidiaries), 19 (Higher-risk countries), 20 (reporting of suspicious transactions) and 21 (tipping-off and confidentiality) should apply to legal professionals subject to certain qualifications.

63. R.23 applies to legal professionals when they engage in a financial transaction on behalf of a client, in relation to the specified activities under R.22. If legal professionals suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to TF, they should be required to promptly report their suspicions to the FIU. Subject to certain limitations, legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege, as recognised by INR.23. The lawyer-client relationship is protected in many countries, including in some instances by constitutional provisions.

64. The FATF Recommendations set the international standards on combating ML and the financing of terrorism and proliferation, which jurisdictions implement taking into consideration their national context including their legal framework. In general terms jurisdictions have closely followed the FATF Recommendations but differences do exist and legal professionals need to carefully consider these differences in their own jurisdictions. The overarching concept of the obligations only applying to certain specified activities is common across all jurisdictions. Section III provides further guidance on the application of obligations in R.22 and R.23 to legal professionals.

65. Even though individual legal professionals or law firms may be able to conclude that specific AML/CFT obligations do not apply to them, ethical standards require them to ensure that their services are not being misused, including by criminals, and they should carefully consider what they need to do to guard against that risk.

66. Countries should establish the most appropriate regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for legal professionals.

Section II- The RBA to AML/CFT

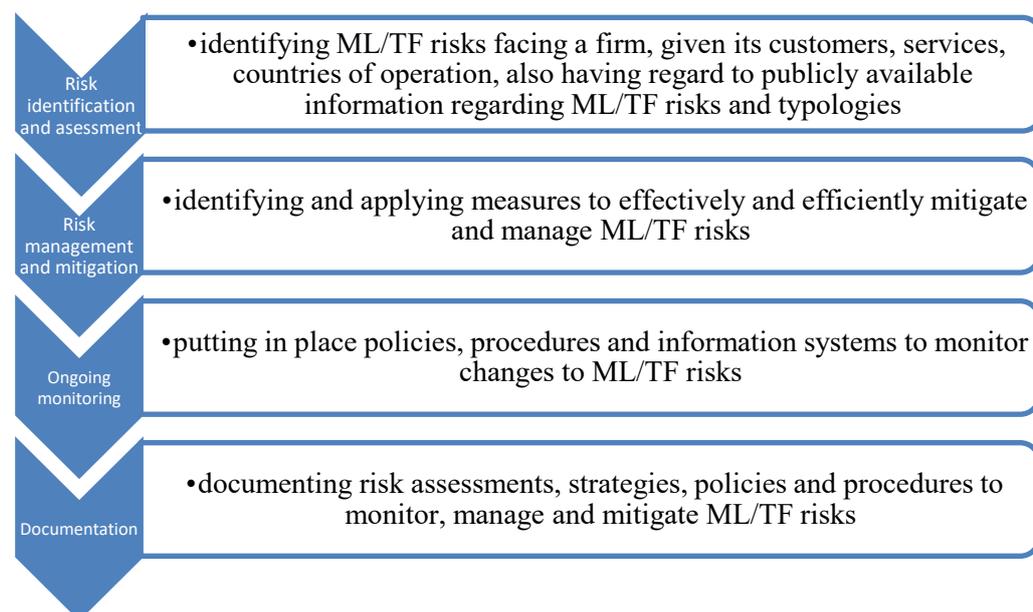
What is the RBA?

67. The RBA to AML/CFT means that countries, competent authorities and DNFBPs, including lawyers, notaries and other legal professionals should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures effectively and efficiently to mitigate and manage the risks.

68. For legal professionals, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions where they operate, and the effectiveness of their controls in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

69. The RBA is not a “zero failure” approach; there may be occasions where a legal professional has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML/TF in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that legal professionals must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

70. Key elements of a RBA can be summarised as follows:



The rationale for the RBA

71. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

72. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the

application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.¹⁵

73. The RBA allows countries, within the framework of the FATF Recommendations, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are reasonable and proportionate to the nature of risks.

74. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and legal professionals.¹⁶

Application of the RBA

75. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors, including services, products, customers, geography, preventive measures and the strength of the entity's compliance program.

76. R.1 sets out the scope of application of the RBA as follows:

a) **Who should be subject to a country's AML/CFT regime?**

- In addition to the sectors and activities already included in the scope of the FATF Recommendations¹⁷, countries should extend their regime to additional institutions, sectors or activities if they pose a higher ML/TF risk. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.¹⁸

b) **How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime**

- Supervisors should ensure that legal professionals are implementing their obligations under R.1. AML/CFT supervisors should consider a legal professional's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.

c) **How should those subject to the AML/CFT regime be required to comply**

- The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls

¹⁵ R.1.

¹⁶ The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take into account the risks and the flexibility allowed by the RBA, when determining whether there are deficiencies in a country's AML/CFT measures, and their importance (*FATF, 2013f*).

¹⁷ See FATF Glossary, definitions of "Designated non-financial businesses and professions" and "Financial institutions".

¹⁸ See INR.1.

conducted should be stronger in higher risk scenarios. Legal professionals are required to apply each of the following CDD measures¹⁹: (i) identification and verification of the client's identity; (ii) identification of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner; (iii) understanding the purpose and nature of the business relationship; and (iv) on-going due diligence on the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

d) **Consideration of the engagement in client relationships**

- Legal professionals are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to ML/TF risks based on risk assessment, it does not mean that all legal professionals and all their clients or services pose a higher risk when taking into account the risk mitigating measures that have been put in place.

e) **Importance of legal professional services to overall economy**

- Legal professionals often play significant roles in the legal and economic life of a country. The role of legal professionals in supporting the negotiation of business and other agreements is vital. The risks associated with any type of client group are not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium-low, medium, medium-high or high risk (see section 3.1 below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

77. Implementing a RBA can present a number of challenges for legal professionals. A RBA requires resources and expertise, both at a country and sector level, to gather and interpret information on risks, to develop policies and procedures and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing such policies and procedures.

Box 1. Particular RBA challenges for legal professionals

Culture of compliance and adequate resources. Implementing a RBA requires that legal professionals have a sound understanding of the ML/TF risks and are able to exercise good professional judgement. Above all, legal professionals and the leadership of law firms should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organisation. This requires the building of expertise including, for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on ML/TF risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will

¹⁹ See R.10

benefit from information sharing by relevant competent authorities, supervisors and SRBs. The provision of good practice guidance by competent authorities, supervisors, legal professionals and SRBs is valuable and encouraged.

Significant variation in services and clients. Legal professionals will vary substantially in the breadth and nature of services provided and the clients they serve, as well as the size, focus, geographic reach and sophistication of the firm and its employees. In implementing the RBA, legal professionals should make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices. Legal professionals should thus tailor their RBA based on their unique characteristics and practice profile.

Appropriate mitigation measures will also depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those who are engaged for distinct purposes. Where these services involve tax laws and regulations, legal professionals also have additional considerations related to a country's or jurisdiction's permissible means to structure transactions and entities or operations to legally avoid and/or minimise taxes.

Transparency of beneficial ownership on legal persons and arrangements. Legal professionals can be involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person may be able to perform these activities. Where legal professionals do play this "gatekeeper" role, they may encounter challenges in keeping current and accurate beneficial ownership information depending upon the nature and activities of their client. Other challenges may arise when on-boarding new clients with minimal economic activity associated with the legal entity and/or its owners, controlling persons, or beneficial owners, established in another jurisdiction. Finally, whether the source is a public registry, another third party source, or the client, there is always potential risk in the correctness of the information, in particular where the underlying information has been provided by the client.²⁰ Those risks notwithstanding from the outset the legal professional should seek answers from the immediate client in determining beneficial ownership (having first determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company). The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the legal professional is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

²⁰ For further information legal professionals can refer to the FATF Guidance on Transparency and Beneficial Ownership.

Risk of criminality. Although the implementation of a RBA should not impair a client's right of access to justice, legal professionals and their firms must be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of a substantive offence of ML/TF. There have been examples of unwitting involvement of or negligence on the part of legal professionals or complicit professionals intentionally enabling the laundering of proceeds of crime. Legal professionals and firms should protect themselves from misuse by criminals and terrorists. This may include restricting the method and source of payments (e.g. cash payments above a monetary threshold, unexplained third party payments) for the services being provided, dictating greater focus on monitoring and reporting of clients and their funds for unusual or suspicious activity.

Interplay between the requirement to comply with AML/CFT obligations and the principle of legal professional privilege and professional secrecy as applicable. Where legal professional privilege does apply, many countries provide exceptions in law that allow legal professionals to make disclosures of suspicion of ML/TF without incurring penalties or liability or breaching ethical obligations and in others to provide an exception to disclosure if the information is directly encompassed by a legitimate claim of privilege. However, legal professionals may be cautious of making disclosures that would otherwise breach privilege or confidentiality rules due to uncertainties in the application of these exceptions, lack of adequate information or training in relation to these rules, the complexities of their clients' situations or a combination of these factors. Criminals may misperceive that legal professional privilege and professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional. Criminals may also seek out legal professionals (over other non-legal professions) to perform the services listed in R.22 with the specific criminal intent of concealing their activities and identity from authorities through professional privilege/secrecy protections.

Allocating responsibility under a RBA

78. An effective risk-based regime builds on and reflects a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector and its risk profile. Legal professional should identify and assess their own ML/TF risk taking account of the NRAs in line with R.1, as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. Legal professionals are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.²¹ Where ML/TF risks are higher, legal professionals should always apply enhanced CDD, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

79. Strategies adopted by legal professionals to mitigate ML/TF risks should take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which legal professionals can take measures to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal and supervisory frameworks are still developing may determine that legal professionals are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until the understanding and experience of the sector is strengthened.²²

80. Legal professionals should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resources on higher risk entities.

Identifying ML/TF risk

81. Access to accurate, timely and objective information on ML/TF risks is essential for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and legal professionals. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share relevant information on ML/TF risks and threats, or where access to information is restricted by censorship or data protection provisions, it will be difficult for legal professionals to correctly identify ML/TF risk.

82. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

²¹ R.1 and IN.1.

²² This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or Financial Sector Assessment Program (FSAP) evaluations.

Assessing ML/TF risk

83. Assessing ML/TF risk requires countries, competent authorities and legal professionals to determine how the ML/TF threats identified will affect them. They should analyse the information to understand the likelihood of these risks occurring, and the impact that these would have, on the individual legal professionals, the entire sector and on the national economy. As a starting step, ML/TF risks are often classified as low, medium-low, medium, medium-high and high. Assessing ML/TF risk goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.²³

84. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. Legal professionals and law firms that are required to routinely conduct a high volume of enquiries when on-boarding clients, e.g. because of the size and geographic footprint of the firm, may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such law firms are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist law firms in this regard.

85. Law firms should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. Law firms should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

86. The FATF recommendations require that when applying a RBA, legal professionals should appropriately mitigate and manage the risks that they identify. Mitigating practices will invariably include initial and ongoing CDD, internal policies, training, and procedures to address the vulnerabilities faced in the legal professional's particular context. Legal professional should take enhanced measures to manage the ML/TF risks identified. This section does not attempt to exhaustively list the mitigating practices that may be employed by legal professionals. Instead, it provides select examples to illustrate how legal professionals might choose to address particular risks under the RBA.²⁴

87. The FATF Recommendations require that, when applying a RBA, legal professionals, countries, competent authorities and SRBs decide on the most appropriate and

²³ [FATF \(2013a\)](#), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk. Also refer to The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013).

²⁴ For information on ways in which legal professionals might mitigate their ML/TF vulnerabilities, see Section 2 of this Guidance and chapters III and IV of the separate publication: "A Lawyer's Guide to Detecting and Preventing Money Laundering" published in October 2014 by a collaboration of the International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe.

effective way to mitigate the ML/TF risk they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied:²⁵

- a) Countries may decide not to apply some of the FATF Recommendations requiring DNFBSs to take certain actions, provided (i) 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 DNFBS or (ii) a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6.
- b) Countries looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of clients or services, establish a threshold for the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.²⁶

Developing a common understanding of the RBA

88. The effectiveness of a RBA depends on a common understanding by competent authorities and legal professionals of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, legal professionals should deal with the risks they identify. Following a consultative process, competent authorities should issue RBA guidance to legal professionals on meeting and managing their legal and regulatory AML/CFT obligations. Supporting ongoing and effective communication between competent authorities and legal professionals is essential.

89. Competent authorities should acknowledge that not all legal professionals will adopt identical AML/CFT controls in a risk-based regime. On the other hand, legal professionals should understand that a RBA does not exempt them from applying effective AML/CFT controls.

²⁵ Subject to the national legal framework providing for Simplified CDD.

²⁶ For example, R.22 on CDD.

Section III – Guidance for legal professionals

Risk identification and assessment

90. Potential ML/TF risks faced by legal professionals will vary according to many factors including the activities undertaken by them, the type and identity of the client, and the nature and origin of the client relationship. When applying the RBA, legal professionals and firms should bear in mind that specified activities have been found to be more susceptible to ML/TF activities because they involve the movement or management of client assets; this susceptibility may be heightened when these activities are conducted on a cross-border basis. These specified activities include:

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

91. Although a client's right of access to advice and justice should not be adversely affected by the implementation of the RBA, legal professionals and their firms must remain alert to ML/TF risks posed by the services they provide to avoid unwittingly committing or becoming an accessory to the commission of a ML/TF offence. Legal professionals and law firms must protect themselves from unwitting involvement in ML/TF; such involvement not only presents reputational risk to the individuals concerned, the law firm and the legal profession at large, it is also unacceptable for the legal profession to allow itself to be misused by criminals.

92. Legal professionals should perform a risk assessment of the client at the inception of a client relationship. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in legal services/sector, risk reports in other jurisdictions where the legal professional is based, and any other information which may be relevant to assess the risk level particular to their legal practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Legal professionals may also draw references to FATF Guidance on indicators and risk factors²⁷. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important. Competent authorities should consider how they can best alert legal professionals to the findings of any national risk assessments, the supra-national risk assessments and any other information that may be relevant to assess the risk level particular to a legal practice in the relevant country.

93. Due to the nature of services that a legal professional generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most legal professionals. The legal professional's knowledge of the client

²⁷ FATF Report on Vulnerabilities in the Legal Sector (2013), Chapters 4 and 5.

and its business will develop throughout the duration of a longer term and interactive professional relationship (in some cases, such relationships may exist for short term clients as well, e.g. for property transactions). Although individual legal professionals are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationship. Legal professionals should consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g. one-off client relationship involving simple transactions). Legal professionals should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

94. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients in a single transaction, those involved in a long term advisory relationship and those who are engaged for distinct and discrete purposes including, for example, civil law notaries and local counsel engaged in a specific jurisdiction within a transaction.

95. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A legal professional may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring legal professional).

96. Legal professionals may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling legal professionals, where required, to subject each client to reasonable and proportionate risk assessment.

97. The most commonly-used risk categories are:

- a) country or geographic risk;
- b) client risk; and
- c) risk associated with the particular service offered.

98. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the legal professional and/or law firm. These criteria, however, should be considered holistically and not in isolation. Legal professionals, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

99. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller law firms and sole practitioners, it is advisable to look at the services they offer (e.g. providing company management services may entail greater risk than other services).

100. Criminals deploy a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common

mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. Legal professionals may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

101. A practical starting point for law firms (especially smaller firms) and legal professionals (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

- a) **Client acceptance and know your client policies:** identify the client and its beneficial owners and the true “beneficiaries” of the transaction. Obtain an understanding of the source of funds and source of wealth of the client where required, its owners and the purpose of the transaction.
- b) **Engagement acceptance policies:** understand the nature of the work. Legal professionals should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where a legal professional does not have the requisite expertise, the legal professional should not undertake the work.
- c) **Understand the commercial or personal rationale for the work:** legal professionals need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Legal professionals however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.
- d) **Be attentive to red flag indicators:** exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. Subject to qualifications set forth in this Guidance, these cases would trigger reporting obligations. Documenting the thought process may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion.
- e) **Then consider what action, if any, needs to be taken and have an action plan:** the outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm’s CDD/EDD procedures (including evidence of source of wealth or funds).
- f) **Documentation:** legal professionals should adequately document and record steps taken under a) to e).

Country/Geographic risk

102. There is no universally agreed definition by competent authorities, SRBs or legal professionals that prescribes whether a particular country or geographic area (including the country within which the legal professional practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information on ML/TF risks. Geographic risks of ML/TF may arise in a variety of circumstances, including from the

domicile of the client, the location of the transaction or the source of the wealth or funds. Factors that are generally agreed to place a country in a higher risk category include:

- a) Countries/areas identified by credible sources²⁸ as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
- b) Countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
- c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.
- d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.²⁹

Client risk

103. Determining the potential ML/TF risks posed by a client or category of clients is critical to the development and implementation of an overall risk-based framework. Based on their own criteria, law firms and legal professionals should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of clients whose activities may indicate a higher risk include:

- a) PEPs and persons closely associated with or related to PEPs, are considered as higher risk clients (Please refer to the FATF Guidance (2013) on PEPs for further guidance on how to identify PEPs).

²⁸ “Credible sources” refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

²⁹ www.oecd-ilibrary.org/taxation/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews_2219469x

Box 2. Particular considerations for PEPs and source of funds and wealth

If a legal professional is advising a PEP client, or where a PEP is the beneficial owner of assets in a transaction, appropriate enhanced CDD is required if a specified activity under R.22 is involved. Such measures include, obtaining senior management (e.g. senior partner, managing partner or executive partner) approval before establishing a business relationship, taking reasonable measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs, and conducting enhanced ongoing monitoring on that relationship.

The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust). Source of funds relates directly to the economic origin of funds to be used in a transaction. This is likely to be received via a bank account. Generally, this would be evidenced by bank statements or similar documentation showing from where funds in an account originated such as receipt of salary. Source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). Source of wealth is the origin of the accrued body of wealth of an individual. Understanding source of wealth is about taking reasonable steps, commensurate with risk to be satisfied that the funds to be used in a transaction appear to come from a legitimate source.

While source of funds and wealth may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, legal professionals should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is reasonable and proportionate to the risk profile of the client.

Relevant factors that influence the extent and nature of CDD include the particular circumstances of a PEP, PEPs separate business interests and the time those interests prevailed in relation to the public position, whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts, the PEP's home country, the type of activity that the PEP is instructing the legal professional to perform or carry out, whether the PEP is domestic or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

If a PEP is otherwise involved with a client, then the nature of the risk should be considered in light of all relevant circumstances, such as:

- a) the nature of the relationship between the client and the PEP: If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary

beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) the nature of the client (e.g. where it is a public listed company or regulated entity who is subject to and regulated for a full range of AML/CFT requirements consistent with FATF Recommendations, the fact that it is subject to reporting obligations will be a relevant factor.

c) the nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration. Higher risks may exist where a legal professional is involved in the movement or transfer of funds/assets, or the purchase of high value property or assets.

- b) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).
- c) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:
 - i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company formation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.
 - ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
 - iii. Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the legal professionals' understanding of the client's business and economic purpose.
- d) Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- e) Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks. These may include, for example:
 - i. Money or Value Transfer Services (MVTs) businesses (e.g. remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities).

- ii. Operators, brokers and others providing services in virtual assets.
 - iii. Casinos, betting houses and other gambling related institutions and activities.
 - iv. Dealers in precious metals and stones.
- f) Businesses that while not normally cash intensive appear to have substantial amounts of cash.
 - g) Businesses that rely heavily on new technologies (e.g. online trading platform) may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.
 - h) Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
 - i) Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SRBs.
 - j) Clients who appear to be acting on somebody else's instructions without disclosing the identity of such person.
 - k) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected.
 - l) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the legal professionals to perform a proper risk assessment.
 - m) Clients with previous convictions for crimes that generated proceeds, who instruct legal professionals (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.
 - n) Clients who have no address, or who have multiple addresses without legitimate reasons.
 - o) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).
 - p) Clients who change their settlement or execution instructions without appropriate explanation.
 - q) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

- r) Clients who insist, without reasonable explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.
- s) Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where legal professionals may receive a significant premium for a successful representation, should not be considered a risk factor.
- t) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.
- u) Where there are certain transactions, structures, geographical location, international activities or other factors that are not consistent with the legal professional's understanding of the client's business or economic situation.
- v) The legal professional's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent³⁰.
- w) Clients who apply for residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction.
- x) Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.
- y) The relationship between employee numbers/structure and nature of the business is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses).
- z) Client seeking advice or implementation of an arrangement that has indicators of a tax evasion purpose, whether identified as the client's express purpose, in connection with a known tax evasion scheme or based on other indicators from the nature of the transaction.
- aa) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies that might be used to obscure beneficial ownership.
- bb) Sudden activity from a previously dormant client without clear explanation.
- cc) Client that start or develop an enterprise with unexpected profile or abnormal business cycles or client that enters into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

³⁰ See the FATF Report on Money Laundering and Terrorist Financing: Vulnerabilities of Legal Professionals (June 2013).

- dd) Indicators that client does not wish to obtain necessary governmental approvals/filings.
- ee) Reason for client choosing the firm is unclear, given the firm's size, location or specialisation.
- ff) Frequent or unexplained change of client's professional adviser(s) or members of management.
- gg) The client is reluctant to provide all the relevant information or legal professionals have reasonable suspicion that the provided information is incorrect or insufficient.
- hh) Clients seeking to obtain residents rights or citizenship in the country of establishment of the legal professional, in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

Transaction/Service risk

104. An overall risk assessment of a client should also include determining the potential risks presented by the services offered by a legal professional, given the nature of such services, noting that legal professionals provide a broad and diverse range of services. The context of the services being offered or delivered is always fundamental to a RBA. Any one of the factors discussed in this Guidance alone may not itself constitute a high-risk circumstance but the factors should be considered cumulatively and holistically. When determining the risks associated with the provision of services related to specified activities, consideration and appropriate weight should be given to such factors as:

- a) Services where legal professionals, effectively acting as financial intermediaries, handle the receipt and transmission of funds through accounts they control in the act of facilitating a business transaction.
- b) Services that allow clients to deposit/transfer funds through the legal professional's trust account that are not tied to a transaction for which the legal professional is performing or carrying out activities specified in R.22.
- c) Services where the client may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client) (e.g. through the firm's general account and/or a personal or business account held by the legal professional himself/herself).
- d) Services where legal professionals may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.
- e) Services that are capable of concealing beneficial ownership from competent authorities.³¹

³¹ For further details on the difficulties presented by arrangements which conceal beneficial ownership see joint FATF and Egmont group report "Vulnerabilities Linked to the Concealment of Beneficial Ownership" published in July 2018.

- f) Services requested by the client for which the legal professional does not have expertise excepting where the legal professional is referring the request to an appropriately trained professional for advice.
- g) Services that rely heavily on new technologies (e.g. in relation to initial coin offerings or virtual assets) that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.
- h) Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.³²
- i) Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment.
- j) Transactions where it is readily apparent to the legal professional that there is inadequate consideration, especially where the client does not provide legitimate reasons for the amount of the consideration.
- k) Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes.
- l) The use of shell companies, companies with ownership through nominee shares or bearer shares and control through nominee and corporate directors without apparent legal, tax, business, economic or other legitimate reason.³³
- m) Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including changes of name/corporate seat or on establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.³⁴
- n) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the legal professional.
- o) Settlement of default judgments or alternative dispute resolutions is made in an atypical manner (e.g. if satisfaction of a settlement or judgment debt is made too readily).

³² See the FATF Typologies report [Money Laundering and Terrorist Financing through the Real Estate Sector](#).

³³ See also the FATF typologies report "[The Misuse of Corporate Vehicles, including Trust and Company Service Providers](#)" published 13 October 2006.

³⁴ See also the FATF typologies report "[The Misuse of Corporate Vehicles, including Trust and Company Service Providers](#)" Annex 2 on trusts, for a more detailed description of "potential for misuse" of trusts.

- p) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.
- q) Transactions using unusual means of payment (e.g. precious metals or stones).
- r) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.
- s) Unexplained establishment of unusual provisions in credit arrangements that do not reflect the commercial position between the parties. Arrangements that may be abused in this way might include unusually short/long amortisation periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.
- t) Transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for the type of client, transaction or with the legal professional's normal course of business, such as a transfer to a corporate entity, or generally without any appropriate explanation.
- u) Successive capital or other contributions in a short period of time to the same entity with no apparent legal, tax, business, economic or other legitimate reason.
- v) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.
- w) Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.
- x) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.
- y) Legal persons that, as a separate business, offer TCSP services should have regard to the TCSP Guidance,³⁵ even if such legal persons are owned or operated by legal professionals. Legal professionals, however, who offer TCSP services should have regard to this Guidance, and should consider customer or service risks related to TCSPs such as the following:
 - i. Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices.
 - ii. Provision of registered office facilities and nominee directorships without proper explanations.
 - iii. Unexplained use of discretionary trusts.

³⁵ See the FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers, published in July 2019

- iv. In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
- z) In the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries
- aa) Services where the legal professional acts as a trustee/director that allows the client's identity to remain anonymous.
- bb) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.
- cc) Unexplained use of pooled client accounts or safe custody of client money or assets or bearer shares, where allowed, without justification.
- dd) Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.
- ee) Suspicion of fraudulent transactions or transactions which are improperly accounted for. These might include:
 - i. Over or under invoicing of goods/services.
 - ii. Multiple invoicing of the same goods/services.
 - iii. Falsely described goods/services
 - iv. Over or under shipments (e.g. false entries on bills of lading).
 - v. Multiple trading of goods/services.

Variables that may influence risk assessment

105. While all legal professionals should follow robust standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst legal professionals, as well as the nature of the clients they serve. As a result, consideration must be given to these factors when creating a RBA that complies with the existing obligations of legal professionals. Certain notaries, for example, are subject to an array of duties as public officeholders. By contrast, legal professionals do not have such extensive public duties, but are nearly universally subject to duties of professional secrecy and an obligation to uphold their clients' rights of legal professional privilege to their communications. Legal professionals with distinct "public" roles within national legal systems should carefully consider the interaction of their particular duties with the RBA outlined in this Guidance.

106. The particular responsibilities, status and role of the legal professional will, in general, have a significant influence on what is appropriate for risk assessment. For example, in many civil law jurisdictions, notaries do not represent parties to a contract and are not intermediaries. They are obliged to be impartial and independent, advising both parties bearing in mind any disparity of power between them. Notaries carry duties as public office holders. These duties will influence the scope of what the notary must do to assess the ML/TF risk and how to act based on that assessment. Notaries should be conscious of the

respectability they can add to documents, and the value this can add to those whose motives are nefarious.

107. Consideration should be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. It may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large law firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may also be regarded by criminals as more of a target for money launderers than large law firms. Legal professionals in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

108. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular legal professional. This factor must be considered in the context of the legal professional's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice. A legal professional's RBA methodology may thus take account of risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause a legal professional to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, legal professionals should always adhere to the minimum requirements as set out in national legislation. These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

- a) The nature of the client relationship and the client's need for the legal professional to prepare for or carry out specified activities.
- b) The level of regulation or other oversight or governance regime to which a client is subject. For example, a client that is a financial institution or legal professional regulated in a country with a satisfactory AML/CFT regime poses less risk of ML/TF than a client in an industry that has ML/TF risks and yet is unregulated for ML/TF purposes.
- c) The reputation and publicly available information about a client. Legal persons that are transparent and well known in the public domain and have operated for a number of years without being convicted of proceed generating crimes may have low susceptibility to money laundering. This may not be the case where such a legal person is in financial distress or in a situation of liquidation/insolvency.
- d) The regularity, depth or duration of the client relationship may be a factor that lowers or heightens risk (dependant on the nature of the relationship).

- e) The familiarity of the legal professional with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a legal professional's own activities.
- f) The proportionality between the magnitude or volume and longevity of the client's business and its legal requirements, including the nature of services sought.
- g) Subject to other factors (including the nature of the services and the source and nature of the client relationship), providing limited legal services in the capacity of a local or special counsel may be considered a low risk factor. This may also, in any event, mean that the legal professional is not "preparing for" or "carrying out" a transaction for a specified activity identified in R.22.
- h) Significant and unexplained geographic distance between the legal professional and the location of the client where there is no nexus to the type of activity being undertaken.
- i) Where a prospective client has instructed the legal professional to undertake a single transaction-based service (as opposed to an ongoing advisory relationship) and one or more other risk factors are present.
- j) Where the legal professional knows that a prospective client has used the services of a number of legal professionals for the same type of service over a relatively short period of time.
- k) Risks that may arise from non-face-to-face relationships and could favour anonymity. Due to the prevalence of electronic communication between legal professionals and clients in the delivery of legal services, non-face-to-face interaction between legal professionals and clients would not be considered a high risk factor on its own. The treatment of non-face-to-face communications should always be subject to the approach taken by legislation and regulators in the relevant jurisdiction.
- l) The nature of the referral or origin of the client. A prospective client may contact a legal professional in an unsolicited manner or without common or customary methods of introduction or referrals, which may indicate increased risk. By contrast, where a prospective client has been referred from another trusted source or a source regulated for AML/CFT purposes (e.g. from another legal professional), the referral may be considered a mitigating risk factor.
- m) The structure of a client or transaction. Structures with no apparent legal, tax, business, economic or other legitimate reason may increase risk. Legal professionals often design structures (even if complex) for legitimate legal, tax, business, economic or other legitimate reasons, in which circumstances there may not be an indicator of increased risk of ML/TF. Legal professionals should satisfy themselves of a reasonable need for such complex structures in the context of the transaction.
- n) Trusts that are pensions may be considered lower risk.

Documentation of risk assessments

109. Several jurisdictions mandate various documentation requirements in connection with AML/CFT.³⁶ Legal professionals must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments to be able to demonstrate their basis. However, 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.³⁷

110. Legal professionals may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner has become more important as legal professionals are now obliged in various jurisdictions to conduct a documented risk assessment for each client and share it with supervisory authorities when required.

111. A documented risk assessment may cover a range of specific risks by breaking them down into the three common categories highlighted above: (a) geographic risks, (b) client-based risks and (c) service-based risks. These three risk categories have been identified and explained in the guide: “*A Lawyer’s Guide to Detecting and Preventing Money Laundering*”.³⁸ The guide also provides graphic illustrations and case studies of how to assess risk under these three categories. In practice, risk factors could be categorised differently in different jurisdictions. However, all relevant risk factors should be considered.

112. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan³⁹ (if required) should then be outlined to accompany the assessment and dated. Action plans can help identify potential red flags, facilitate risk assessment and decide on CDD measures to be applied. A simple template of risk assessment may be as below, for instance:

Geographic risk	Client-based risk	Service-based risk
Low/medium/high risk	Low/medium/high risk	Low/medium/high risk
Explanation	Explanation	Explanation
Overall assessment: Low/Medium/High risk		
Action plan		

113. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, as required, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the

³⁶ For example, the European Union law places an obligation on legal professionals working in an AML-regulated service to document risk assessments and ensure they are kept up to date (Article 8 of the Fourth Anti-Money Laundering Directive (EU) 2015/849).

³⁷ Paragraph 8 of INR.1

³⁸ *A Lawyer’s Guide to Detecting and Preventing Money Laundering*, is a collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, published in October 2014.

³⁹ “Action plans” are described in some jurisdictions as the “document your thought process” form.

client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties. Proper safeguards should be put in place to ensure privacy of clients.

114. Where legal professionals are involved in longer term transactions, risk assessments should be undertaken at suitable intervals across the life of the transaction, to ensure no significant risk factors have changed in the intervening period (e.g. new parties to the transaction, new sources of funds etc.). See [3.4.2] *Ongoing monitoring of clients and special activities*.

115. A final risk assessment should be undertaken before a transaction has completed, allowing time for any required STR to be filed and any authority to move or transfer assets to be obtained from law enforcement (in countries where this is applicable).

Risk management and mitigation

116. Identification and assessment of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those who are engaged for distinct purposes including, for example, civil law notaries. In high risk scenarios, legal professionals must consider the extent to which they might be involved in unwittingly enabling the substantive offence of ML/TF by providing a legal service even with the application of enhanced CDD measures. Under such scenario, legal professionals should consider not to provide services or establish/continue business relationship with the client.

117. Legal professionals should implement appropriate measures and controls to mitigate the potential ML/TF risks for those clients that, as the result of a RBA, are determined to be higher risk. These measures should be tailored to the specific risks faced, both to ensure the risk is adequately addressed and to assist in the appropriate allocation of finite resources for CDD. Paramount among these measures is the requirement to train legal professionals and appropriate staff to identify and detect relevant changes in client activity by reference to risk-based criteria. These measures and controls may include:

- a) General training on ML/TF methods and risks relevant to legal professionals.
- b) Targeted training for increased risk awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work.
- c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain evidence and record source of wealth and beneficial ownership information if required.
- d) Periodic review of the services offered by the legal professional and/or law firm, and the periodic evaluation of the AML/CFT framework applicable to the law firm or legal professional and the law firm's own AML/CFT procedures, to

determine whether the ML/TF risk has increased and adequate controls are in place to mitigate those increased risks.

- e) Reviewing client relationships on a periodic basis to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

118. CDD measures should allow a legal professional to establish with reasonable certainty the true identity of each client. The legal professional's procedures should apply in circumstances where a legal professional is preparing for or carrying out⁴⁰ the specified activities listed in R.22 and include procedures to:

- a) Identify and appropriately verify the identity of each client on a timely basis.
- b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner on risk-sensitive basis such that the legal professional is reasonably satisfied that it knows who the beneficial owner is. The general rule is that clients should be subject to the full range of CDD measures, including the requirement to identify the beneficial owner in accordance with R.10. The purpose of identifying beneficial ownership is to ascertain those natural persons who exercise effective influence or control over a client, whether by means of ownership, voting rights or otherwise. Legal professionals should have regard to this purpose when identifying the beneficial owner. They may use a RBA to determine the extent to which they are required to verify the identity of beneficial owner, depending on the type of client, business relationship and transaction and other appropriate factors in accordance with R.10 and INR.10 as articulated in the following box. This information is in many circumstances critical to helping legal professionals avoid conflicts of interest with other clients.

Box 3. Beneficial ownership information obligations (see R.10, R.22 and INR.10)

R.10 sets out the instances where legal professionals will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. Legal professionals should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk.⁴¹

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. Legal professionals can

⁴⁰ See paragraphs 17-22 above for further information on when a legal professional would or would not be considered engaged in "preparing for" or "carrying out" transactions for clients, and hence when the requirements of R.22 would apply.

⁴¹ For more information and guidance relating to beneficial ownership information please refer to AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. Legal professionals can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the legal professional is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client and may include conducting public searches as well as by seeking information directly from the client. Legal professionals will likely need to obtain the following information for a client that is a legal entity:

- a) the name of the company;
- b) the company registration number;
- c) the registered address and/ or principal place of business (if different);
- d) the identity of shareholders and their percentage ownership;
- e) names of the board of directors or senior individuals responsible for the company's operations;
- f) the law to which the company is subject and its constitution; and
- g) the types of activities and transactions in which the company engages.

To verify the information listed above, legal professional may use sources such as the following:

- a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
- b) details from company registers;
- c) shareholder agreement or other agreements between shareholders concerning control of the legal person; and
- d) filed audited accounts.

Legal professionals should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure.

The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

- c) Obtain appropriate information to understand the client's circumstances and business depending on the nature, scope and timing of the services to be provided including, where necessary, the source of funds of the client. This

information may be obtained from clients during the normal course of their instructions to legal professionals.

- d) Conduct ongoing CDD on the business relationship and scrutiny of transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with legal professional's knowledge of the client, its business and risk profile, including where necessary, the source of funds. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of STRs to an FIU where required, or to respond to requests for information from an FIU and law enforcement agencies.

119. The starting point is for legal professionals to assess the risks that the client may pose taking into consideration any appropriate risk variables (and any mitigating factors) before making a final determination to accept the client, reject the client, or request additional information. In many situations and in many jurisdictions this risk assessment is required to be documented and kept in the client's file. The legal professional should review this file as necessary, especially in a situation where the client looks to engage in a one-off or atypical transaction or where new red flags arise. The legal professional's risk assessment should inform the overall approach to CDD and appropriate verification. Legal professionals should reasonably determine the CDD requirements appropriate to each client, which may include:

- a) **Standard CDD:** A standard level of CDD, generally to be applied to all clients to whom specified services are provided.
- b) **Simplified CDD:** The standard level being reduced after consideration of appropriate risk variables, and in recognised lower risk scenarios, such as:
 - i. Publicly listed companies traded on certain exchanges (and their majority owned subsidiaries). Although it should not be assumed that all publicly listed companies will qualify for simplified CDD, for example appropriate levels of reporting to the market will be a factor to take into account, as well as geographic risk factors.
 - ii. Financial institutions and other businesses and professions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.
 - iii. Public administration or enterprises (other than those from countries that are being identified by credible sources as having inadequate AML/CFT systems, being the subject of sanctions, embargos or similar measures issued by the United Nations, having significant levels of corruption or other criminal activity or providing funding or support for terrorist activities, or having designated terrorist organisations operating within their country).
- c) **Enhanced CDD:** An increased level of CDD for those clients that are reasonably determined by the legal professional to be of higher risk. This may be the result of the client's business activity, ownership structure, particular service offered including work involving higher risk countries or defined by applicable law or regulation as posing higher risk.

120. Where the legal professional is unable to comply with the applicable CDD requirements, they should not carry out the transaction nor commence business relations, or should terminate the business relationship and consider filing an STR in relation to the client.

121. A RBA means that legal professionals should perform varying levels of work according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or natural persons exercising effective control; and an indication of the purpose of the trust. Legal professionals will need to obtain a reasonable level of comfort that the declared purpose of the trust is in fact its true purpose.

122. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

Box 4. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the legal professional is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- 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 business and risk profile of the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity

- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional client information, such as the client's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the client risk profile
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of legal professionals should enable them to disregard source documents, data or information, which is perceived to be unreliable)
- Where appropriate, undertaking further searches on the client or beneficial owner to specifically understand the risk that the client or beneficial owner may be involved in criminal activity
- Obtaining additional information about the client's source of wealth or funds involved to seek to ensure they do not constitute the proceeds of crime. This could include obtaining appropriate documentation concerning the source of wealth or funds
- Seeking additional information and, as appropriate, substantiating documentation, from the client about the purpose and intended nature of the transaction or the business relationship
- Increasing the frequency and intensity of transaction monitoring.
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of such holders.

Ongoing monitoring of clients and specified activities (R.10 and 23)

123. The degree and nature of ongoing monitoring by a legal professional will depend on the type of legal professional, and if it is a law firm, the size and geographic 'footprint' of the law firm, the ML/TF risks that the law firm has identified and the nature of the specified activity and services provided. In many instances, client information must already be monitored in this fashion to satisfy legal professionals' other obligations (e.g. legal, professional, or ethical) to both their clients and as part of their general regulatory

obligations. For example, legal professionals may need to have a full and up-to-date understanding of their clients' business to fully satisfy fiduciary duties towards their clients. In some jurisdictions, ethical or professional obligations may require a legal professional to discontinue their representation of a client on learning/knowing certain adverse information or in case of reasonable grounds to suspect that the client is involved in an ML/TF offence. Monitoring is often best achieved by individuals having contact with the client (either face-to-face or by other means of communication).

124. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that legal professionals are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information.

125. In larger law firms serving clients with a wide range of operations, legal professionals with regular contact with the client may be narrowly focused on one aspect of the client's business and/or need for specific advice. In these circumstances, it may be more effective to have screening processes and tools to identify potential risks that are generic to the client's overall business, and that can then be flagged for the attention of legal professionals who have the most client contact. However, monitoring does not require legal professionals to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis the client. It rather refers to maintaining awareness throughout the course of work for a client to the possibility of ML/TF activity and/or changes in the clients activities/personnel and/or other changing risk factors.

126. Monitoring of these advisory relationships cannot be achieved solely by reliance on automated systems and whether any such systems would be appropriate will depend in part on the nature of a legal professional's practice and resources reasonably available to the legal professional. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate monitoring systems and a RBA proportionate to the scope and nature of the practitioner's practice. A legal professional's advisory relationships may well be best monitored by the individuals having direct client contact being appropriately trained to identify and detect changes in the risk profile of a client. Where appropriate this should be supported by systems, controls and records within a framework of support by the firm (e.g. tailored training programs appropriate to the level of staff responsibility, the role each staff member plays in the AML/CFT process at the firm and the types and volumes of clients and transaction for which the firm provided services).

127. Legal professionals should assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs should fall within the system and control framework developed to manage the risk of the firm. Certain jurisdictions may require that the results of the monitoring be documented.

128. The civil law notaries do not generally represent parties to a contract and therefore must maintain a fair position with regard to any duty to both parties.

Suspicious transaction reporting, tipping-off, internal control and higher-risk countries (R.23)

129. R.23 sets out obligations for legal professionals on reporting and tipping-off, internal controls and higher-risk countries as set out in R.20, R.21, R.18 and R.19.

Suspicious transaction reporting and tipping-off (R.20, R.21 and 23)

130. R.23 requires legal professionals to report suspicious transactions set out in R.20, when on behalf of, or for a client, they engage in a financial transaction in relation to the activities described in R.22. Subject to certain limitations, such reporting is not required if the relevant information is directly encompassed within a legitimate claim of professional secrecy or legal professional privilege. Legal professionals should be alert to these obligations in addition to separate requirements in their jurisdictions regarding tipping-off. These obligations, where they apply, can carry serious penalties when not properly complied with. As specified under INR.23, where legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

131. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly and, therefore, a RBA for the reporting of the suspicious activity under these circumstances is not applicable. STRs are not part of risk assessment, but rather reflect a response mechanism – typically to an FIU or SRB once a suspicion has been formed. Legal professionals have an obligation not to facilitate illegal activity, so if there are suspicions, they could contact their FIU or SRB for guidance, obtain independent legal advice, if necessary and do not provide services to that person/company and report the transaction or the attempted transaction. Legal professionals may be asked to advise a client on the client's own obligation to report suspicious activity. In doing so, the legal professional may become aware of the subject matter giving rise to the suspicion. In these circumstances, the legal professional will need to consider whether it should file an STR where required. In the context of an international law firm, which may have a global Money Laundering Reporting Officer (MLRO), where a reportable suspicion arises in relation to a client, the MLRO need not necessarily make a report to the FIU in each jurisdiction where a client has a relationship but, rather, in the jurisdictions with a nexus to the matter giving rise to the suspicion.

Internal controls (R.18 and 23)

132. Legal professionals differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of legal professionals have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against ML/TF. For a number of legal professionals, a single person may be responsible for the functions of front office, back office, reporting, and senior management. This dimension of a legal professional's practice environment should be taken into account in designing a risk-based framework for internal controls systems. INR.18 specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size, nature and risk profile of the business.

133. The risk-based process must be a part of the internal controls of the legal professional or law firm. Legal professionals operate within a wide range of differing business structures, from sole practitioners to large, multi-national partnerships. In smaller legal practices, legal professionals' businesses tend to have a flat management structure and

accordingly, most or all of the principals (or partners) of the firm hold ultimate management responsibility. In other organisations, legal professionals employ corporate style organisational structures with tiered management responsibility. In both cases the principals or the managers are ultimately responsible for ensuring that the organisation maintains an effective internal control structure; regardless of the size of the legal practice, legal professionals are generally responsible for the actions of their partners and staff. Engagement by the principals and managers in AML/CFT is an important aspect of the application of the RBA since such engagement reinforces a culture of compliance, ensuring that staff adheres to the legal professional's policies, procedures and processes to manage effectively ML/TF risks.

134. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

- a) the nature, scale and complexity of a legal professional's business.
- b) the diversity of a legal professional's operations, including geographical diversity.
- c) the legal professional's client, service and activity profile.
- d) the degree of risk associated with each area of the legal professional's operations.
- e) the services being offered and the frequency of client contact (either by face-to-face meetings or by other means of communication).

135. Subject to the size and scope of the legal professional's organisation, the framework of risk-based internal controls should:

- a) have appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP;
- b) provide for adequate controls for higher risk clients and services as necessary (e.g. additional due diligence, obtaining information on the source of wealth and funds of a client, escalation to senior management or additional review and/or consultation by the legal professional or within a law firm);
- c) provide increased focus on a legal professional's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;
- d) provide for periodic review of the risk assessment and management processes, taking into account the environment within which the legal professional operates and the services it provides;
- e) designate personnel at an appropriate level who are responsible for managing AML/CFT compliance;
- f) provide for an AML/CFT compliance function and review programme as appropriate given the scale of the organisation and the nature of the legal professional's practice;
- g) inform the principals of compliance initiatives, identified compliance deficiencies and corrective action taken;

- h) provide for programme continuity despite changes in management or employee composition or structure;
- i) focus on meeting all regulatory measures for AML/CFT compliance, including record-keeping requirements and provide for timely updates in response to changes in regulations;
- j) implement risk-based CDD policies, procedures and processes, including review of client relationships from time to time to determine the level of ML/TF risks;
- k) provide for adequate supervision and support for staff activity that forms part of the organisation's AML/CFT programme;
- l) incorporate AML/CFT compliance into job descriptions of relevant personnel;
- m) for legal professionals that share a common arrangement in some way (e.g. alliances of law firms), to the extent possible, provide a common control framework;
- n) adhere to country specific legislative requirements (such as residence requirements);
- o) provide for policies and procedures to ensure staff awareness of STR filing requirements; and
- p) implement a documented program of ongoing staff AML/CFT awareness and training.

136. Same measures and controls may often address more than one of the risk criteria identified, and it is not essential that a legal professional establish specific controls targeting each risk criterion.

137. Legal professionals should consider using reputable technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the legal profession as they continue to develop, this may be particularly important for smaller law firms that may be less able to commit significant resources of time to these activities. Under R.17, the ultimate responsibility for CDD measures should remain with legal professionals relying on the technology-driven solutions utilized.

138. At larger law firms, senior management should have a clear understanding of ML/TF risks to manage the affairs of the law firm and to ensure adequate procedures are put in place to identify, manage, control and mitigate risks effectively. The RBA to AML/CFT needs to be embedded in the culture of law firms and the legal profession generally.

Internal mechanisms to ensure compliance

139. Legal professionals (and where relevant senior management and the board of directors (or equivalent body)) should monitor the effectiveness of internal controls. If they identify any weaknesses in those internal controls, improved procedures should be designed.

140. The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member who may have a good working knowledge of the law firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to

challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the law firm's procedures.

141. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the law firm is acting on those recommendations.

142. Legal professionals should review their firm-wide risk assessments regularly and make sure that policies and procedures continue to target those areas where the ML/TF risks are highest.

Vetting and recruitment

143. Legal professionals should consider the skills, knowledge and experience of staff for AML/CFT both before they are appointed to their role and on an ongoing basis. The level of assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

144. R.18 requires that legal professionals provide their staff with AML/CFT training. For legal professionals, and those in smaller law firms in particular, such training may also assist with raising awareness of monitoring obligations, and may also satisfy some jurisdictions' continuing legal education obligations. A legal professional's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant legal professionals with at least general information on AML/CFT laws, regulations and internal policies.

145. Firms should provide targeted training for increased awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work. Training should also be targeted towards the role that individual legal professionals perform in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

146. Training is not necessarily resource-intensive and it can take many forms. Training can include group study where one member of staff outlines to other staff, relevant guidance, credible sources of information on legal sector risk or firm policies and/or provides regular email updates.

147. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Legal professionals must also be alert to the interaction with, and importance of legal professional privilege and professional secrecy in relation to AML/CFT laws in their particular jurisdictions.⁴² Likewise, legal professionals should be aware of the scope of application of the legal professional

⁴² See also the [FATF Report on Vulnerabilities in the Legal Sector](#) (2013), Chapter 4 "ML Typologies".

privilege and professional secrecy in their jurisdictions, i.e. the cases and scenarios that fall under its application and those outside its scope.

148. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in the legal professional's own practice. In addition, competent authorities, SRBs and representative bodies for both common and civil law notaries and law societies should work with educational institutions to ensure that the curriculum addresses ML/TF risks. The same training should also be made available for students taking courses to train to become legal professionals. For example, law societies and bar associations should be encouraged to produce jurisdiction-specific guidance based on this Guidance (such as the ABA's Voluntary Good Practices Guidance), offer continuing legal education programs on AML/CFT and the RBA and large law firms should be encouraged to conduct in-house training programs on AML/CFT and the RBA.

149. The overall RBA and the various methods available for training and education gives legal professionals flexibility regarding the frequency, delivery mechanisms and focus of such training. Legal professionals should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

- a) tailored to the relevant staff responsibility (e.g. client contact or administration);
- b) at the appropriate level of detail (e.g. considering the nature of services provided by the legal professional);
- c) at a frequency suitable to the risk level of the type of work undertaken by the legal professional; and
- d) used to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

150. Consistent with R.19, legal professionals should apply enhanced CDD measures (also see box in paragraph 102 above), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV- Guidance for supervisors

151. The RBA to AML/CFT aims to develop prevention or mitigation measures, which are commensurate with the risks identified. This applies to the way supervisory authorities allocate their resources. R.28 requires that legal professionals are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs have different roles across jurisdictions and this section should be read in the context of what is applicable for a specific jurisdiction. Whichever model of supervision (i.e. by a designated supervisor or a SRB) is adopted by a country, it should be effective.

152. In many jurisdictions, supervisors and SRBs take an active role in identifying ML/TF risks and may take a direct approach to regulating legal professionals' obligatory responsibilities both generally and with regards to AML/CFT. Supervisors or SRBs should identify the particularities of the sector, assess its risks, controls and procedures in order to efficiently allocate its resources. In particular, supervisors for legal professionals should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas.

153. Although a country may have a legal framework that does not fully accommodate the supervision of legal professionals in the manner described in this Section, the supervision of legal professionals in that country should nonetheless include as a minimum:

- a) A requirement that legal professionals perform risk assessment at firm, client and transactional level.
- b) A requirement that legal professionals perform appropriate risk-based CDD.
- c) Procedures that ensure the system for licensing legal professionals prevents criminals from becoming legal professionals.
- d) Procedures determined to ensure prompt investigation of legal professional misuse of client/ trust funds or alleged involvement in ML/TF schemes.
- e) A requirement that legal professionals complete periodic continuing legal education in CDD and AML/CFT topics.
- f) A requirement that legal professionals report suspicious transactions, comply with tipping-off and confidentiality requirements, internal controls requirements and higher-risk countries requirements.
- g) A requirement that legal professionals adequately document risk assessment, CDD and other AML related decisions and processes undertaken.

Risk-based approach to supervision

154. R.28 requires that legal professionals are subject to adequate AML/CFT regulation and supervision for monitoring compliance. A RBA to AML/CFT means that the measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resources to areas of higher ML/TF risk. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of legal professionals, any relevant supervisors and

SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.⁴³

Supervisors and SRBs' role in supervision and monitoring

155. Countries can ensure that legal professionals are subject to effective oversight through the supervision performed by a SRB, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF. A SRB is a body representing a profession (e.g. legal professionals, notaries, other independent legal professionals, accountants or TCSPs) that has a role (either exclusive or in conjunction with other entities) in regulating the persons who are qualified to enter and practise in the profession. A SRB also may perform supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

156. Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanction), and adequate financial, human and technical resources. Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on a RBA, taking into account inherent ML/TF risks in the legal sector, and mitigation by legal professionals and their firms.

157. Countries should ensure that supervisors and SRBs are equipped in identifying and sanctioning non-compliance by its members. Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

158. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant person should not continue to take part in the monitoring/ supervision of their practice/law firm to avoid conflicts of interest. This institutional conflict may be particularly relevant when it comes to enforcement, including sanctions, which should be sufficient to have a deterrent effect and also remove the benefits of non-compliance.

Background: national frameworks and understanding ML/TF risk- the role of countries

159. Countries should ensure that the extent to which a national framework allows legal professionals to apply a RBA should also reflect the nature, diversity and maturity of the sector, and its risk profile as well the ML/TF risks associated with individual legal professionals.

160. Access to information about ML/TF risks is essential for an effective RBA. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information

⁴³ See INR 28.1.

available for AML/CFT risk assessments conducted by legal professionals and the jurisdiction's national assessment of risk. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and legal professionals.⁴⁴ In situations where some legal professionals have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

161. Supervisors and SRBs should, as applicable draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supra-national risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

162. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which legal professionals operate in the country and the nature of services provided by them.

163. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the legal professional. Supervisors and SRBs should also consider the type of services the legal professional is providing as well as its size and business model (e.g. whether it is a sole practitioner), corporate governance arrangements, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation. Supervisors and SRBs should also consider the controls legal professionals have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements). Supervisors should note that under the RBA, particularly in the legal profession sector, given their diversity in scale, functions and number, there may be valid reasons for differences among risks and controls. There is therefore no one-size-fits-all approach. In evaluating the adequacy of their RBA, supervisors should take into consideration the circumstances of these differences.

164. Supervisors and SRBs should seek to ensure that their supervised populations are fully aware of, and compliant with measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues that affect several aspects of AML/CFT.

165. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers published by international bodies.⁴⁵ Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

166. Supervisors and SRBs should review their assessment of legal professionals' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the legal professional community.

⁴⁴ See INR 1.3.

⁴⁵ Such as the FATF, the OECD, the WB, the IMF and the UNODC.

Mitigating and managing ML/TF risk

167. Supervisors and SRBs should take proportionate measures to mitigate and manage ML/TF risk. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the inherent ML/TF risks. Supervisors and SRBs should consider the characteristics of the legal professionals, particularly their role as professional intermediaries. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of legal professionals and their clients, products and services.⁴⁶

168. Supervisors and SRBs should take into account the risk profile of legal professionals when assessing the adequacy of internal controls, policies and procedures.⁴⁷

169. Supervisors and SRBs should develop a means of identifying which legal professionals or classes of legal professionals are at the greatest risk of being used by criminals and communicate those findings to the legal professionals. This involves considering both the probability and impact of ML/TF risk.

170. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by legal professionals and the environment in which they operate. The risk can also vary depending on other factors:

- a) service and product risk (the likelihood that products or services can be used for ML/TF);
- b) client risk (the likelihood that clients' funds may have criminal origins);
- c) nature of transactions (e.g. frequency, volume and counterparties);
- d) geographical risk (whether the legal professional, its clients or other offices perform specified activities in riskier locations); and
- e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the legal professional as well as information on legal professional's compliance history, complaints about the legal professional or about the quality of the legal professional's internal controls. Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports in credible media, particularly those related to predicate offences for ML/TF or to financial crimes.

171. In adopting a RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of a legal professional within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the firm from the grouping.

⁴⁶ See INR 28.2.

⁴⁷ See INR 28.3

172. Supervisors and SRBs should also consider the impact, (i.e. the potential harm caused) if the legal professional or firm facilitates, unwittingly or otherwise, ML/TF. A small number of legal professionals may cause a high level of harm, including reputational harm to the profession. This can depend on:

- a) size (i.e. turnover), number and type of clients, number of office locations, value of transactions, and
- b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

173. Supervisors and SRBs should update the risk assessment on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of the legal professionals.

174. Supervisors or SRBs should consider whether legal professionals meet the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and character. This will include whether the legal professional meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

175. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate among categories of legal professionals based on various factors such as their client base, countries they deal with and applicable AML/CFT controls. Other determinative factors may include (a) whether the legal professional conducts litigation or transactional business; (b) whether the clients of the legal professional's firm are in the private or public sector; or (c) whether the legal professional's business is internationally or domestically focused.

176. Supervisors and SRBs should acknowledge that in a risk-based regime, not all legal professionals will adopt identical AML/CFT controls and that an isolated incident where the legal professional is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of a legal professional's AML/CFT controls. At the same time, legal professionals should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

Supervision of the RBA

Licensing or Registration

177. R.28 requires a country to ensure that regulated entities including legal professionals are subject to regulatory and supervisory measures to ensure compliance by the profession with AML/CFT requirements.

178. R.28 requires the supervisor or SRB to 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 in an accredited legal professional entity (where this is permitted under national law and regulations) or holding a management function in a legal professional entity. This may be achieved through the evaluation of these persons through a "fit and proper" test.

179. A licensing or registration mechanism is one of the means to identify legal professionals to whom the regulatory and supervisory measures, including the "fit and

proper” test should be applied. It also enables the identification of the population of legal professionals, for the purposes of assessing and understanding the ML/TF risks for the country, and the action that should be taken to mitigate them in accordance with R.1. Not all jurisdictions take this approach, and the application and precise objectives of licensing and registration differ among the jurisdictions that do use these mechanisms.

180. Licensing or registration provides a supervisor or SRB with the means to fulfil a “gatekeeper” role over who can enter a profession in which many individuals will be required to undertake the specified activities set forth in R.22. Not all accredited legal professionals who are appropriately licensed or registered may be performing the specified activities under R.22. There is no requirement for separate licensing or registration of legal professionals on the basis of their practice areas under the FATF Recommendations. Supervisors and SRBs should ensure that their supervisory efforts are directed at legal professionals whose practices involve the specified activities under R.22. Licensing or registration should also ensure that upon qualification, legal professionals are subject to AML/CFT compliance monitoring.

181. As appropriate, the supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry, or tax authority), information from financial institutions and DNFBPs, complaints by the public and open source information from advertisements and business and commercial registries, or any other sources that indicates that there are unsupervised individuals or businesses providing the specified activities under R.22.

182. Licensing or registration frameworks should define the activities that are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing “bad actors”.

183. The terms “licensing” or “registration” are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential, conduct as well as ML/TF risks on an ongoing basis. Some jurisdictions have adopted similar licensing regimes for legal professionals, generally where legal professionals carry out trust and corporate services, to encompass aspects of conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

184. A jurisdiction may have a registration framework over the entire DNFBP sector, including legal professionals or have a specific registration framework for each constituent of a DNFBP. Generally, a supervisor or SRB carries out the registration function.

185. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interest of its members. The SRB should ensure that registration decisions are taken separately and independently from its activities regarding member representation.

Fit and proper tests

186. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a

management function in a legal professional. Such tests are used in relation to legal professionals in some jurisdictions and may be used by supervisors or SRBs to ensure compliance with AML/CFT requirements.

187. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in a legal professional.

188. In some jurisdictions, a “fit and proper test” forms a fundamental part of determining whether to license or register the applicant and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual’s fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that role.

189. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. The questionnaire could gather personal identification information, residence and employment history, and require disclosure by the applicant of any convictions or adverse judgements, including pending prosecutions and convictions. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors, or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

190. The supervisor or SRB should also ensure that on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function. The supervisor or SRB should consider reviewing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against “brass-plate” operations

191. The supervisor or SRB should ensure that its licensing or registration requirements require the applicant to have a meaningful relationship with the country. Depending on the circumstances, a business with only staff who do not possess the professional requirements of a legal professional might not be licensed or registered.

192. A supervisor or SRB should consider the ownership and control structure of the applicant to make a licensing or registration decision, where applicable. Factors to take into account could include consideration of where the beneficial owners and controllers reside and the type and quality of its management, including directors, managers and compliance officers.

193. The supervisor or SRB should consider whether the ownership and control structure of law firms unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

194. Supervisors and SRBs should take measures to effectively monitor legal professionals providing specified legal services through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected risk-based approach. Supervisors and SRBs may choose to adjust:

- a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.
- b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of legal professionals. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer and other relevant staff, considering gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients, legal professionals and other matters, which may be observed in the course of an on-site visit and where appropriate, sample testing of reporting obligations.
- c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from legal professionals' inclusion in thematic review samples).
- d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of legal professionals' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the legal professionals' risk assessment, CDD, reporting and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of Directors and AML/CFT assessment in particular lines of business.

195. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever

appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to legal professionals to enable them to enhance their RBA.

196. Record keeping and quality assurance are important, so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

197. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by legal professionals. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFBPs, to include legal professionals when providing the services outlined in R.22(d). Sanctions should be available for the directors and senior management of the firm when a legal professional fails to comply with requirements.

198. Supervisors and SRBs should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, censure and reprimand to punitive measures (including disbarment and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in more severe supervisory response.

199. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

200. Supervisors and SRBs should communicate their regulatory expectations. This should be done through a consultative process after meaningful engagement with relevant stakeholders, including legal professionals. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. This could include guidance to clarify the interpretation and application of professional privilege and secrecy principle in the context of the nature of services provided by legal professionals.

201. Guidance issued to legal professionals should also discuss ML/TF risk within their sector and outline ML/TF indicators (i.e. red flags) and methods of risk assessment to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

202. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the legal profession, which may cover operational and practical issues, and be more detailed and explanatory in nature. Training

events may also provide an effective means to ensure legal professionals awareness and compliance with AML/CFT responsibilities. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to the legal profession and be consistent with all other legal requirements and obligations.

203. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions legal professionals will consider that separate guidance targeted at the legal profession will be the most appropriate and effective form.

204. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, findings of thematic reviews, training events, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

Training

205. Supervisors and SRBs should ensure that their staff, and other relevant employees are trained to assess the quality of ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of the AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension. Supervisory staff should recognise that in implementing the RBA, legal professionals should make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices.

206. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by legal professionals and the adequacy and proportionality of AML/CFT controls of legal professionals. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

207. Supervisors should avoid mandating the use of AML/CFT systems, tools or software of any third party commercial providers to avoid conflicts of interest in the effective supervision of firms.

Information exchange

208. Supervisors should encourage the information exchange between the public and private sector and within private sector (e.g. between financial institutions and legal professionals) is important for combating ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial

Intelligence Units and law enforcement), where applicable should be robust, secure and subject to compliance with national legal requirements.

209. The type of information that could be shared between the public and private sectors include:

- a) ML/TF risk assessments;
- b) Typologies (i.e. case studies) of how money launderers or terrorist financiers have misused legal professionals;
- c) feedback on STRs and other relevant reports;
- d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with legal professionals as a class or individually; and
- e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

210. Domestic co-operation and information exchange between FIU and supervisors of legal professionals and among competent authorities including law enforcement, intelligence, FIU, tax authorities, supervisors and SRBs is also important for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Such intelligence should also inform a supervisor's risk-based approach to supervisory assurance. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged where appropriate. When sharing information, protocols and safeguards should be implemented in order to protect personal data.

211. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the legal sector, taking into account the multi-jurisdictional reach of many legal professionals.

Supervision of beneficial ownership and source of funds/wealth requirements

212. The FATF Recommendations require competent authorities to have access to adequate, accurate and timely information on the beneficial ownership and control of legal persons (R.24). In addition, countries must take measures to prevent the misuse of legal arrangements for ML/TF, in particular ensuring that there is adequate, accurate and timely information on express trusts (R.25). Implementation of the FATF Recommendations on beneficial ownership has proven challenging. As a result, the FATF developed the *FATF Guidance on Transparency and Beneficial Ownership* to assist countries in their implementation of R.24 and R.25, as well as R.1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

213. R.24 and R.25 require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of

AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). Legal professionals must, however, be cautious in blindly relying on the information contained in registries. Ongoing monitoring is important during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership, as registries are unlikely to provide such information on a dynamic basis.

214. Those responsible for company formation and the creation of legal arrangements fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements or in their management and administration. The guidance in relation to beneficial ownership information in this section is intended for legal professionals who are involved in such arrangements by acting in the capacity of a formation agent, company director, company secretary, office for service, nominee or other similar capacity.

215. Legal professionals are also required to undertake and document adequate risk assessment of clients/transactions to fully understand the nature of the underlying clients' business activity. Evidence could include business plans/governance documents, financial statements and company registry filings.

216. As DNFBPs, legal professionals are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In some countries, a legal professional may be required for registering a legal person and will be responsible for providing basic and/or beneficial ownership information to the registry. A number of countries have notarial systems where a notary will attest to the accuracy of registry filings.

217. In their capacity as company directors, trustees or foundation officials of these legal persons and legal arrangements, legal professionals often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing banking or audit services to these types of client.

218. These financial institutions and other DNFBPs may request the CDD information collected and maintained by legal professionals, who because of their role as director or trustee, will act as the principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owners of the legal person or legal arrangement.

219. Under R.28, countries should ensure that legal professionals are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify them. R.24 and R.25, which deal with transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up-to-date information is available on a timely basis on these legal entities.

220. In accordance with R.28, legal professionals should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current basic and beneficial ownership information on legal persons and legal arrangements is maintained and will be available on a timely basis to competent authorities.

221. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which legal professionals have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client records on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

222. During on-site and offsite inspections, the supervisor or SRB should examine the policies, procedures and controls that are in place for on-boarding of new clients to establish what information and documentation is required where the client is a natural person or legal person or arrangement. The supervisor or SRB should verify the adequacy of these procedures and controls to identify beneficial owners to understand the ownership and control structure of these legal persons and arrangements and to ascertain the business activity. For example, self-declaration on beneficial ownership provided by the client without any other mechanism to verify the information may not be adequate in all cases.

223. Sample testing of records will assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the records selected should reflect the profile of the client base and include both new and existing clients.

224. The supervisor or SRB should consider the measures the legal professional has put in place for monitoring changes in the beneficial ownership of legal persons and legal arrangements to whom they provide services to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

225. During examinations, the supervisor or SRB should consider whether to verify the beneficial ownership information available on the records of the legal professional with that held by the relevant registry, if any. The supervisor or SRB may also consider information from other competent authorities such as FIUs, public reports and information from other financial institutions or DNFBPs, to verify the efficacy of the legal professional's controls.

Sources of funds and wealth

226. Legal professionals should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which legal professionals have established to identify and record sources of wealth in arrangements.

Nominee arrangements

227. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner.

228. A nominee shareholder is a natural or legal person who is officially recorded in the register of members and shareholders of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement.

229. In a number of countries, legal professionals act or arrange for another person (either an individual or corporate) to act as a director and act or arrange for another person (either an individual or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, one of the mechanisms to ensure that nominee shareholders and directors are not misused is by subjecting these legal professionals to licensing and recording their status in company registries. Countries may rely on a combination of measures in this respect.

230. There are legitimate reasons for a legal professional to act as or provide directors to a legal person or act or provide nominee shareholders. These may include the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. However, nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of the person from whom they will take instructions from or whom they represent. They are sometimes referred to as “strawmen”.

231. Nominee directors and nominee shareholders can create obstacles to identifying the true beneficial owner of a legal person, particularly where the status is not disclosed. This is because it will be the identity of the nominee that is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in various countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

232. The supervisor or SRB should be aware that undisclosed nominee arrangements may exist. They should consider whether undisclosed nominee arrangements would be identified and addressed during their on-site and offsite inspections and examination of the policies, procedures, controls and client records of the legal professional, including the CDD process and ongoing monitoring by the legal professional.

233. An undisclosed nominee arrangement may exist where there are the following (non-exhaustive) indicators:

- a) the profile of a director or shareholder is inconsistent with the activities of the company;
- b) the individual holds numerous appointments to unconnected companies;
- c) a director’s or shareholder’s source of wealth is inconsistent with the value and nature of the assets within the company;
- d) funds into and out of the company are sent to, or received from unidentified third party/ies;
- e) the directors or shareholders are accustomed to acting on instruction of another person; and

- f) requests or instructions are subject to minimal or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the director/s.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom a legal professional provides services

1. Taking a RBA, the amount of information that should be obtained by the legal professional will depend on whether the legal professional is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, a legal professional will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. A legal professional who is providing other services (e.g. acting as registered office) to a trust, company or other legal entity will be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. A legal professional that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by another legal professional or accountant or TCSP providing services to the trust or relevant extracts from the trust deed itself to enable the legal professional to identify the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. As described above, depending on the services being provided to the trust, a legal professional should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that the legal professional's policies should enable it to disregard source documents, data or information that are perceived to be unreliable) as described in more detail below:

- i. the settlor;
- ii. the protector;
- iii. the trustee(s), where the legal professional is not acting as trustee;
- iv. the named beneficiaries or class of beneficiaries, and
- v. any other natural person actually exercising effective control over the trust.

Settlor

- a) A settlor is generally any person (or persons) by whom the trust is made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).
- b) A settlor may or may not be named in the trust deed. Legal professionals should have policies and procedures in place to identify and verify the identity of the real economic settlor.

- c) A legal professional establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a trustee, company or other legal entity should have policies and procedures in place (using a RBA) to identify the source of funds in the trust, company or other legal entity.
- d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift or letter of wishes.
- e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

- a) Legal professionals should have policies and procedures in place, adopting a RBA to enable them to form a reasonable belief that they know the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that the legal professionals are satisfied that they know who the beneficiaries are. This does not require the legal professional to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the legal professionals should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).
- b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), legal professionals should obtain information to enable them to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).
- c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although legal professionals should satisfy themselves that these are the intended beneficiaries (e.g. by reference to the trust deed), they are not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary.
- d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, a legal professional is not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary.
- e) A legal professional who administers the trust or company or other legal entity owned by a trust or otherwise provides or acts as trustee or director to the trustee, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the

information has been provided, or there are other changes to the class of beneficiaries.

- f) A legal professional is not obliged to obtain other information about beneficiaries other than to enable the legal professional to satisfy itself that it knows who the beneficiaries truly are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

- a) A legal professional providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.
- b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:
 - i. dispose of or invest (other than as an investment manager) trust property;
 - ii. direct, make or approve trust distributions;
 - iii. vary or terminate the trust;
 - iv. add or remove a person as a beneficiary or to or from a class of beneficiaries; and/or
 - v. appoint or remove trustees.
- c) A legal professional who administers the trust or otherwise acts as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

- 4. These examples are subject to the more general guidance on what information should be obtained by the legal professional to enable it to identify settlors and beneficiaries. It is not intended to suggest that a legal professional must obtain more information about a beneficiary that is an entity where it would not need to obtain such information if the beneficiary is an individual.
 - a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, a legal professional should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.
 - b) In the case of a settlor which is a legal entity, a legal professional should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, the legal professional should take steps to satisfy itself as to the identity of the economic settlor of the trust (i.e. the person who has provided funds to the

legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor retains powers over the trust (e.g. a power of revocation), the legal professional should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

- c) In the case of a beneficiary which is an entity (e.g. a charitable trust or company), a legal professional should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the legal professional should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

- a) Where a legal professional is not itself acting as trustee, it is necessary for the legal professional to obtain information to enable it to identify and verify the identity of the trustee (s) and, where the trustee is a corporate trustee, identify the corporate entity, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.
- b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the legal professional should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. The legal professional can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the website of the body that regulates the trustee and of the regulated trustee itself).
- c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence that enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the legal professional should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the legal professional does not need to obtain detailed information to identify the directors or controlling persons of that entity that acts as shareholder of the private trust company.

Individual and Corporate protector

- a) Where a legal professional is not itself acting as a protector and a protector has been appointed, the legal professionals should obtain information to identify and verify the identity of the protector.
- b) Where the protector is a legal entity, the legal professional should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

- c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the legal professional should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. The legal professional can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the website of the body that regulates the protector and of the regulated protector itself).

Annex 2: Sources of further information

1. Various sources of information exist that may help governments and legal professionals in their development of a RBA. Although not an exhaustive list, this Annex highlights a number of useful web-links that governments and legal professionals may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such as AML/CFT assessments.

Legislation and Court Decisions

2. The rulings by the ECJ of June 26th, 2007 by the Belgium Constitution Court of January 23rd 2008 and the French Conseil d'État of April 10th, 2008 confirmed that AML/CFT regulation cannot require or permit the breach of the legal professional's duty of professional secrecy when performing the essential activities of the profession.
3. The Court of First Instance in the Joined Cases T-125/03 & T-253/03 Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission of the European Communities has restated the ruling in the AM&S case that professional secrecy "meets the need to ensure that every person must be able, without constraint, to consult a legal professional whose profession entails the giving of independent legal advice to all those in need of it (AM&S, paragraph 18). That principle is thus closely linked to the concept of the legal professional's role as collaborating in the administration of justice by the courts (AM&S, paragraph 24).
4. In Judgement of the Court (Grand Chamber) of 26 June 2007 in Case C-305/05 in a question referred for a preliminary ruling, the Court holds that "the obligations of information and of cooperation with the authorities responsible for combating money laundering [...] and imposed on legal professionals by Article 2a(5) of Directive 91/30848, account being taken of the second subparagraph of Article 6(3)⁴⁹ thereof, do not infringe the right to a fair trial as guaranteed by Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 6(2) EU". The Court reaches this conclusion by considering that: (i) obligations of information and cooperation apply to legal professionals only in so far as they advise their client in the preparation or execution of certain transactions; (ii) as soon as the legal professional acting in connection with a transaction is called upon for assistance in defending the client or in representing him before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings, that

⁴⁸ Article 2a(5) of Directive 91/308 listed the specified transactional activities in whose performance legal professionals were to be considered as obliged entities.

⁴⁹ According to which "Member States shall not be obliged to apply the obligations laid down in paragraph 1 to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings".

legal professional is exempt from the obligations of information and cooperation, regardless of whether the information has been received or obtained before, during or after the proceedings. An exemption of that kind safeguards the right of the client to a fair trial; (iii) the requirements relating to the right to a fair trial do not preclude the obligations of information and cooperation from being imposed on legal professionals acting specifically in connection with the specified activities, in cases where the second subparagraph of Article 6(3) of that directive does not apply, where those obligations are justified by the need to combat money laundering effectively, in view of its evident influence on the rise of organised crime”⁵⁰.

5. **Michaud v. France case of 6 December 2012.** This case concerned the obligation on French legal professionals to report their suspicions regarding possible ML activities by their clients. Among other things, the applicant, a member of the Paris Bar and the Bar Council, submitted that this obligation, which resulted from the transposition of European directives, was in conflict with Article 8 of the European Convention on Human Rights, which protects the confidentiality of lawyer-client relations.
6. The European Court of Human Rights in its judgement held that there had been no violation of Article 8 of the Convention. While stressing the importance of the confidentiality of lawyer-client relations and of legal professional privilege, it considered, however, that the obligation to report suspicions pursued the legitimate aim of prevention of disorder or crime, since it was intended to combat ML and related criminal offences, and that it was necessary in pursuit of that aim. The Court held that the obligation to report suspicions, as implemented in France, did not interfere disproportionately with legal professional privilege, since legal professionals were not subject to the above requirement when defending litigants and the legislation had put in place a filter to protect professional privilege, thus ensuring that legal professionals did not submit their reports directly to the authorities, but to the president of their Bar association.
7. Directive (EU) 2015/849 (AMLD) provides:
 - Art. 2 AMLD: 1. This Directive shall apply to the following obliged entities: [...] (3) the following natural or legal persons acting in the exercise of their professional activities: [...] (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures;
8. Art. 34(2): “Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors ***only to the strict extent that such exemption*** relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of

⁵⁰ <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-305/05>

defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings”⁵¹.

9. In the United States there is a “crime-fraud” exception to attorney-client privilege. See, e.g. Am. Law Institute, Restatement of the Law Third, Restatement of the Law Governing Lawyers §82 Client Crime or Fraud (2000). As the U.S. Supreme Court observed, “[i]t is the purpose of the crime-fraud exception to the attorney-client privilege to assure that the ‘seal of secrecy’ ... between legal professional and client does not extend to communications ‘made for the purpose of getting advice for the commission of a fraud.’” *United States v. Zolin*, 491 U.S. 554, 562 (1989) (internal citation omitted). Before determining whether this exception applies, there must be a showing of “a factual basis adequate to support a good faith belief by a reasonable person that *in camera* review of the materials may reveal evidence to establish a claim that the crime-fraud exception applies.” *Id.* at 572. Under case law in the U.S. further developing this principle, the crime-fraud exception can apply even where the attorney acts innocently—“the lawyers’ innocence does not preserve the attorney-client privilege against the crime-fraud exception. The privilege is the client’s, so it is the client’s knowledge and intentions that are of paramount concern to the application of the crime-fraud exception; the attorney need know nothing about the client’s ongoing or planned illicit activity for the exception to apply.” *United States v. Chen*, 99 F.3d 1495, 1504 (9th Cir. 1996) (internal quotations omitted). Under these principles, persons (both legal and natural) have been obliged to disclose pursuant to subpoenas or other legal process factual information that otherwise would have been subject to attorney-client privilege. See, e.g. *In re Grand Jury*, 705 F.3d 133, 155-61 (3d Cir. 2012).

Guidance on the Risk-based Approach

1. Law Society of Ireland: www.lawsociety.ie⁵².
2. Law Society of England and Wales: www.lawsociety.org.uk
3. Law Society of Hong Kong: www.hklawsoc.org.hk
4. Organisme d'autoréglementation de la Fédération Suisse des Avocats et de la Fédération Suisse des Notaires (SRO SAV/SNV): home page: snv.ch/www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf (art.41 to 46)
5. The Netherlands Bar Association: www.advocatenorde.nl
6. The Royal Dutch Notarial Society: www.notaris.nl
7. The American Bar Association Voluntary Good Practices Guidance for Legal professionals to Detect and Combat Money Laundering and Terrorist Financing, published 23 April 2010, available on the ABA website: www.americanbar.org.

⁵¹ Article 33(1) of the Directive refers to reporting STRs to the FIU

⁵² AML guidance and other AML resources available to solicitors in Ireland by logging into the members area www.lawsociety.ie/aml

8. The American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 463 on the Voluntary Good Practices Guidance, published 23 May, 2013, available on the ABA website: www.americanbar.org.
9. A Lawyer's Guide to Detecting and Preventing Money Laundering, collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, published October 2014, available on the IBA website: www.ibanet.org.
10. The FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, 2013, Chapters 4 and 5.
11. Comparative research published by the Solicitors Regulation Authority about ML/TF vulnerabilities observed by the SRA in England and Wales.
12. Comparative Guidance for the legal sector in England and Wales, published by the Legal Sector Affinity Group and approved by HM Treasury.

Other sources of information to help assist countries' and legal professionals' risk assessment of countries and cross-border activities

10. In determining the levels of risks associated with particular country or cross border activity, legal professionals and governments may draw on a range of publicly available information sources. These may include reports that detail observance of international standards and codes, specific risk ratings associated with illicit activity, corruption surveys and levels of international co-operation. A non-exhaustive list is as follows:
 - i. IMF and World Bank Reports on observance of international standards and codes (Financial Sector Assessment Programme)

WB reports:
<http://documents.worldbank.org/curated/en/docsearch/document-type/904559>

 - a. IMF: www.imf.org/external/NP/rosc/rosc.aspx
 - ii. OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting)

www.oecd.org/trade/topics/export-credits/arrangement-and-sector-understandings/financing-terms-and-conditions/country-risk-classification/
 - iii. Egmont Group of financial intelligence units that participate in regular information exchange and the sharing of good practice

www.egmontgroup.org/
 - iv. Signatory to the United Nations Convention against Transnational Organized Crime

www.unodc.org/unodc/crime_cicp_signatures_convention.html
 - v. The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury economic and trade, Sanctions Programmes

www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml

- vi. Consolidated list of persons, groups and entities subject to EU Financial Sanctions: <https://data.europa.eu/euodp/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions>
- vii. Joint Guidelines of the European Supervisory Authorities (ESA) on anti-money laundering risk and counter terrorist financing <https://esas-joint-committee.europa.eu/Publications/Guidelines>

Annex 3: Glossary of terminology

Beneficial Owner

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.

Competent Authorities

Competent authorities refers to all public authorities 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 and bearer negotiable instruments (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.

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.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

- a) Casinos (which also includes internet and ship based casinos).
- 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, 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 the FATF 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.

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 that come into being through the operation of the law and that do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).

FATF Recommendations

Refers to the FATF 40 Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with a legal professional or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term “*Legal professional*” refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign and *domestic PEPs* are individuals who are or have been entrusted by a foreign country or 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.

Red Flags

Any fact or set of facts or circumstances that, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A “*red flag*” may be used as a short hand for any indicator of risk that puts an investigating legal professional on notice that further checks or other appropriate safeguarding actions will be required. 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. Red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements. 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.

Self-regulatory body (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons who 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.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions (“financial supervisors”) 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.

Annex 4: Supervisory practices for implementation of the RBA

Ireland

AML/CFT Compliance Monitoring in Ireland

The Law Society of Ireland is the educational, representative and regulatory body of the solicitors' profession in Ireland. In addition to the statutory functions it exercises under the Solicitors Acts, the Society is also the competent authority for the monitoring of solicitors for the purposes of compliance with Ireland's anti-money laundering and counter-terrorist financing laws under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended.

The Society uses a risk-based system when choosing firms for inspection in addition to conducting a number of random inspections. For many years, firms have been chosen for inspection on the basis of pre-determined risk factors which trigger an accounts inspection. These risk factors include:

- complaints by the public
- previous investigation experience
- the contents of the firm's annual reporting accountant's report
- delays in complying with filing obligations in relation to accountants reports and practicing certificates
- professional indemnity insurance issues
- judgement debts
- media reports
- notifications of concern by government authorities including An Garda Síochána and the Revenue Commissioners

AML/CFT compliance checks are carried out in conjunction with the Society's financial regulation of solicitors' firms. When AML/CFT deficiencies are discovered, targeted standalone checks are implemented until any deficiencies are satisfactorily removed. The process available to compel compliance and used in the past is outlined below.

- If a solicitor fails to implement procedures to combat ML/TF, a report is submitted to the Regulation of Practice Committee who will require the solicitor to provide it with a copy of their new written AML/CFT procedures and evidence that those procedures have been communicated to all staff and will be implemented in full.
- Where it is suspected that a solicitor has committed a substantive offence of ML/TF or failed to fulfil reporting obligations, the matter is referred to the Money Laundering Reporting Committee of the Law Society for appropriate action.
- The experience of the Law Society to date has been that the failure to implement AML/CFT procedures tends to reflect a failure of the solicitor to implement satisfactory procedures to ensure compliance with the

Solicitors Act, in particular the provisions of the Solicitors Accounts Regulations. When a solicitor fails to implement satisfactory procedures to ensure compliance with the Solicitors Accounts Regulations and with the Solicitors (ML and TF) Regulations, the Society will re-investigate the firm until such time that satisfactory procedures have been put in place. If the solicitor does not implement satisfactory procedures, the matter may be referred to the Solicitors Disciplinary Tribunal.

- If it comes to the attention of the Law Society that a solicitor has been engaged in dishonesty particularly in relation to clients' monies (which may occur in parallel with activity suspected to be related to ML/TF), a number of sanctions can be applied, including:
 - An application to the President of the High Court for an Order immediately suspending that solicitor from practice.
 - An application for an Order that no bank shall make any payment from any bank account held by that solicitor or under that solicitor's control.
 - An application for an Order that any documents held by the solicitor be immediately delivered to the Law Society or its nominee.
- In addition to supervision, the Law Society also engages in a range of other AML/CFT outreach and engagement activities including:
 - Awareness raising via a dedicated AML web resource hub, eZine articles, Gazette and email alerts
 - The development of AML Guidance Notes - these are comprehensive notes covering all AML/CFT obligations and ML/TF risks, which follow a question and answer format for ease of reference. They also contain a dedicated chapter providing a non-exhaustive list of indicators of potential suspicious circumstances.
 - In November 2018, supplementary guidance was provided to solicitors to help with new obligations which transpose 4AMLD. Topics covered include how to conduct a Business Risk Assessment, update Policies, Controls and Procedures, and carry out Customer Risk Assessments and 4AMLD changes to CDD measures.
 - Tailored guidance via an Anti-Money Laundering Helpline. This helpline receives queries from solicitors about AML on a daily basis and provides real-time specific guidance. The helpline provides a vital confidential support service to solicitors when navigating potential red flags and deciding whether or not to proceed with a legal service. The Society's guidance is to document their thought process with a particular emphasis on the risk of committing the substantive offence of money laundering should they provide a legal service which may exhibit red flags. In this way, the service can help prevent unwitting facilitation of money laundering by solicitors.
 - AML Education is provided to trainee solicitors attending qualifying courses in the Law Society. In addition, for qualified solicitors, AML modules feature on the Law Society's Diploma and CPD courses. Throughout 2017, for example, the Society delivered extensive AML training across the country and online through a total of 9 seminars with 2 379 attendees.

- CPD Regulations 2015 (S.I. No. 480/2015) require firms to appoint an AML Compliance Partner (failure to do so will mean that each partner in the firm will be designated as an AML Compliance Partner). The AML Compliance Partner must annually undertake a minimum of 3 hours training in regulatory matters, of which at least 2 hours shall be accounting and AML compliance. Training during 2017 has had a measurable impact on the awareness of solicitors of their AML obligations and ML/TF risks evidenced by increased demand for AML guidance in the days following an AML seminar.

France

The CARPA is a verification and regulation system under the responsibility of the Bar Council in France. It applies to all handling of funds received by lawyers on behalf of their clients. It conducts verification under the authority of the Chairman of the Bar Council and has a role in the fight against ML/TF. TRACFIN, the French FIU has an interest in the CARPA, guaranteeing the traceability of all financial flows. The rules of the CARPA system are as follows:

Any handling of funds made by a lawyer must be related to a legal or judicial act.

Any handling of funds made by a lawyer on behalf of his clients must be routed through CARPA (with the sole exception that trusts do not enter into the scope of intervention of CARPA in the current state of the law).

The bank account is opened in the name of CARPA, in which the funds received by the lawyers are deposited on behalf of their clients.

A lawyer cannot receive funds or give instructions to pay them to the beneficiaries without the prior verification of CARPA exercised under the authority and the responsibility of the Bar Council and of the Chairman of the Bar Council. The verifications concern, in particular:

- i. the nature and the description of the case;
- ii. the origin of the funds;
- iii. the destination of the funds;
- iv. the actual beneficiary of the transaction; and
- v. the connection between the financial payment and the legal or judicial transaction carried out by the lawyer in the framework of his professional activity.

CARPA can reject a transaction if it cannot verify the above elements.

The CARPA is not a financial institution and is backed by a bank. As the CARPA is under the authority of the Bar Council and the Chairman of the Bar Council, lawyers have the obligation to provide the necessary explanations for the CARPA to operate without being able to rely upon professional secrecy (which would apply if they were dealing with a bank). The controls thus exercised by the CARPA on the one hand and by its bank

on the other intersect in a complementary way with regard to professional secrecy.

Malaysia

AML/CFT Supervisory Practices of Legal Professionals in Malaysia

A. Fit and Proper Requirements – Self-Regulatory Bodies (SRBs)

In Malaysia, the legal professionals are regulated under the Legal Profession Act 1976, Advocate Ordinance Sabah 1953 and Advocate Ordinance Sarawak 1953, respectively. Prior to admission to the Bar, they are subject to appropriate market entry controls in which they are required to fulfil the “fit and proper” requirements under their respective governing legislation. Practising certificates will be subsequently issued by the High Court of Malaya and High Court of Sabah and Sarawak in conjunction with the respective SRBs for legal professionals, i.e. Bar Council Malaysia (BC) and Sabah Law Society (SLS) as the SRBs, as well as Advocates Association of Sarawak (AAS).

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated supervisory authority for the AML/CFT supervision of the Designated Non-Financial Businesses and Professions (DNFBPs) & Other Financial Institutions in Malaysia, including legal professionals.

BNM adopts a risk-based approach supervision on legal professionals, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D’SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia’s third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness had stipulated the legal professionals’ net ML and TF risks as “**MEDIUM HIGH**” and “**MEDIUM**” level, respectively, as exacerbated by the sector’s marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

ii. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D’SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on legal professionals are guided accordingly to include a range of supervisory tools, as follows:

On-site Examination

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management.

In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions. The follow-up measures have been imposed on a number of legal firms selected for on-site examination, highlighting the higher risk of the sector and consistent with the most recent NRA results.

Off-site Monitoring and Supervisory Outreach Activities

Apart from on-site examinations, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by legal professionals. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for the legal professions is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of Data and Compliance Reports and internal audit reports. In addition, BNM and the relevant SRBs conduct periodic nationwide AML/CFT outreach and awareness programmes.

Spain

General Council of the Notariat of Spain – Money Laundering Centralised Prevention Body

On 28/12/2005 the Spanish General Council of the Notariat established, pursuant to Ministerial Order 2963/2005, of 20 September 2005, regulating the Centralised Prevention Body, a body specialising in the self-regulation of notarial organisation, as permitted by the INR.²³ *“Countries may allow lawyers, notaries, other legal professionals and independent accountants to send their STRs to their appropriate self-regulatory organisations, provided that there are adequate forms of cooperation between these organisations and the FIU.”*

This Body takes on certain obligations in the name of notaries:

- Transaction's analysis.

- Communication of suspicious transactions to the FIU.
- Preparation of sector risk analysis
- Preparation of risk-based AML/TF Internal Policies and Procedures.
- Definition of risk indicators for the notarial sector.
- Training of notaries and employees.
- Supervision of the fulfilment of AML/CTF obligations by notaries.

It intersects between the FIU and notaries, with the generic mission of intensifying collaboration between the notariat and authorities in fight against ML/TF. It has drawn up guides, manuals, FAQ documents, best practice documents; prepared in-house databases to improve the application of CDD at notary offices; resolved more than 7 000 consultations from notary offices; designed on-line training programmes; developed in-person training courses for notaries and employees; established a single matrix of common risk indicators; conducted a sectoral risk analysis; implemented remote supervision of all notary offices and in-person supervision at over 80 notarial practices, among other activities.

The AML system used by Spain's notaries represents a considerable advance for Public Authorities, which thanks to its implementation now have access to:

- A new source of valuable information: notarial indexes (a single database with information on all the public instruments and policies notarised and witnessed in the country). This information, processed in an integrated and automated manner to detect potential ML/TF operations
- A body with AML specialists operating the database, who manage the database, analyse and report to the FIU high-risk operations on behalf of notaries and who can analyse not only the transactions of each notary office (as would be the case if there were no centralised body) but all notary offices together.

The system also offers advantages for notaries, who can delegate the management of (and in practice are relieved from) some of their duties (analysing and, where applicable, reporting operations with evidence of ML/TF, training, internal procedures, etc.) to a team of experts working on their behalf.

General Council of the Notariat of Spain – Practices for Due Diligence: Beneficial Ownership Database

On 24 March 2012, the General Council of the Notariat resolved to set up the "Beneficial Ownership Database" ("Base de Datos de Titular Real", or "BDTR") personal data filing system, and in compliance with data protection regulations published this resolution in the Official State Gazette on 28 April 2012.

The resolution allowed for information to be accessed:

- By notaries, as they are subject to AML obligations.
- By the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (Spanish FIU) to fulfil the tasks entrusted to the Service.
- By the court, taxation, law enforcement and administrative authorities responsible for the prevention and investigation of money laundering.
- By other parties subject to Prevention of Money Laundering Act 10/2010, of 28 April 2010, on the terms set out therein.

Article 6 of Royal Decree 304/2014, of 5 May, approving the Regulation of Prevention of Money Laundering and Terrorist Financing Act 10/2010, of 28 April, established in Spanish law that *"for fulfilment of the obligation to identify and verify the identity of the beneficial owner established in this article, the parties subject to this Act may access the database of beneficial ownership of the General Council of the Notariat ..."*

As a result, not only notaries but also all parties subject to AML requirements may consult the BDTR to facilitate compliance with Due Diligence obligations. This thus allows the FIU and Law Enforcement Agencies to obtain information on owners with a percentage of less than 25% (full corporate regime) at Spanish private limited liability companies, on any given date. They may also request information on which companies a natural person owns (reverse beneficial ownership) on any given date.

Two levels of information quality is ensured:

- Information based on a statement to a public official (foreign companies, foundations, associations, Spanish corporations).
- Information verified in accordance with the sale and purchase transaction of the shares of Spanish Private Limited Liability Companies.

The General Council of the Notariat has established agreements with associations of parties subject to AML obligations (banks, savings banks, investment firms, auditors, lawyers, lottery agencies, credit institutions,

casinos, etc.) and has provided the information called for in more than 2 000 000 requests made to these applicants.

UK

Supervisory Approach of the Solicitors Regulation Authority

The Solicitors Regulation Authority (SRA) regulates solicitors and their firms, as well as other lawyers and non-lawyer managers working in law firms across England and Wales. The SRA also regulates those working as registered European lawyers or registered foreign lawyers. The SRA seeks to protect the public by ensuring that solicitors meet high standards and by acting when risks are identified. With regards to the Money Laundering Regulations, two thirds of firms that the SRA supervises (67%) offer services that fall within scope, the two main categories being acting as an independent legal professional or acting as a trust or company services provider

There are significant barriers to entry to the profession. Requirements include having a qualifying law degree, followed by the Legal Practice Course and then a two-year period of recognised training incorporating the Professional Skills Course. Character and suitability test is also conducted before admission to the roll of solicitors. The SRA requires firms to obtain approval of owners and managers. Firms are required to have Compliance Officers of Legal Practice (COLPs) and Compliance Officers of Financial Administration (COFAs) approved by the SRA. They should have sufficient seniority and independence. Firms are also required to declare whether they are doing work within scope of the Money Laundering Regulations. Those firms in scope of the Regulations must submit an additional application form to declare any individual who is applying to register as a beneficial owner, officer or manager (BOOM).

Risk-based approach

The SRA carries out both qualitative and quantitative risk assessment of how the regulated community is exposed to ML/TF. Each firm is given a risk rating, which informs the supervisory approach of the SRA. Supervisory activities fall into two broad categories: i) reactive work (responding to concerns and breaches); and ii) proactive work (e.g. engaging with firms to prevent breaches, identify potential breaches, explore risks, enhance risk understanding and provide evidence of poor and good behaviours). The SRA uses the information/intelligence that it receives to build a firm's profile. The assessment takes into account the specific breach alleged, the severity of the allegation, the quality of the information and their ability to investigate. Information is coded and then RAG rated (red, amber or green, with red being the most severe). Reports received are risk assessed and conduct matters are created for

matters assessed as high or medium. Those with an AML/CFT angle often leads to an onsite investigation where the main issues are considered, and a fact-based report produced.

Enforcement: The SRA has a number of enforcement tools. This includes letter of advice, finding and warning, reprimand, severe reprimand and rebuke, based on the gravity of violation. The SRA also has powers to impose fines on individuals and firms. In cases of serious misconduct, the SRA can refer a case to the Solicitors Disciplinary Tribunal, which can impose higher fines and also has powers to suspend or strike off. The SRA has the power to disqualify individuals from involvement in specific roles in certain types of firms. It can also prosecute for information offences or acting as a bogus firm and can revoke authorisations or withdraw approvals. The SRA can also prevent non-lawyers from working within legal businesses.

US

Fit and Proper requirements: Lawyers⁵³ in the United States

The discussion below describes the fit and proper requirements in the US, which is the country with the largest number of lawyers subject to an alternative supervisory system.

The highest court of the state in which a lawyer is licensed is responsible for adopting the version of the Model Rules of Professional Conduct applicable in that state and for enforcing the duties of lawyers under those rules. State bar associations or independent agencies created by court rules serve as licensing, regulatory, and disciplinary agencies of the court.

The US system regulates lawyers throughout their careers and includes rigorous controls on lawyers. These controls begin with the rules on the bar admission and are designed, among other things, to prevent criminals from becoming or controlling lawyers and to detect effectively any breaches that might occur.

Entry Requirements: Legal education in the US is a post graduate program, not an undergraduate program and most US jurisdictions require their bar examination applicants to have attended an ABA-approved law school. The US has a unified legal profession, which means that US lawyers who perform “transactional” legal work need to be licensed by state supreme courts and their disciplinary agencies, as do those lawyers who litigate cases in front of a court tribunal. As part of the mandatory licensing process, prospective lawyers are subject to a series

⁵³ The term “Lawyers” is intentionally used in this discussion of the situation in the US as opposed to legal professionals as the requirements described do not extend to all legal professionals within the US.

of requirements to ensure they possess the necessary character and fitness to sit for the bar examination and to practice law. Applicants to US law schools need to disclose any criminal convictions or other encounters with the legal system.

Ongoing Requirements: US lawyers must renew their licenses annually. The requirements for renewal include mandatory compliance with rules of professional conduct, mandatory rules about accounts involving client funds, and additional rules that vary from state to state and include matters such as mandatory continuing education requirements, random audits of client trust accounts, and programs designed to identify and assist lawyers with substance abuse and mental health issues. US lawyers have mandatory obligations to report wrongdoing by other lawyers and failure to comply subject a lawyer to discipline. Many states require lawyers to self-report criminal convictions to the lawyer disciplinary agency.

Annex 5: Examples of Red flags highlighting suspicious activities or transactions for legal professionals⁵⁴

- a) 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;
 - legal person or arrangement, including NPOs, that request services for purposes or transactions, which are not compatible with those declared or not typical for those organisations.
 - 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.
- b) The customer 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.
- c) 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.
- d) The client is using multiple bank accounts or foreign accounts without good reason.
- e) Private expenditure is funded by a company, business or government.
- f) 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.
- g) An unusually short repayment period has been set without logical explanation.
- h) Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

⁵⁴ See also the [Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership, July 2018](#), Annex E – Indicators of concealed beneficial ownership.

- i) The asset is purchased with cash and then rapidly used as collateral for a loan.
- j) There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested that are not appropriate for the common practice used for the ordered transaction.
- k) Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.
- l) The collateral being provided for the transaction is currently located in a high-risk country.
- m) 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.
- n) There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.
- o) The company receives an injection of capital or assets in kind that is excessively high in comparison with the business, size or market value of the company performing, with no logical explanation.
- p) 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.
- q) Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the customer or the possible group of companies to which it belongs or other justifiable reasons.

Annex 6: Members of the RBA Drafting Group

FATF Members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors (GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD
Accountants		
Member	Office	Institution
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants
Legal professionals and Notaries		
Member	Office	Institution
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
Alexander Winkler	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

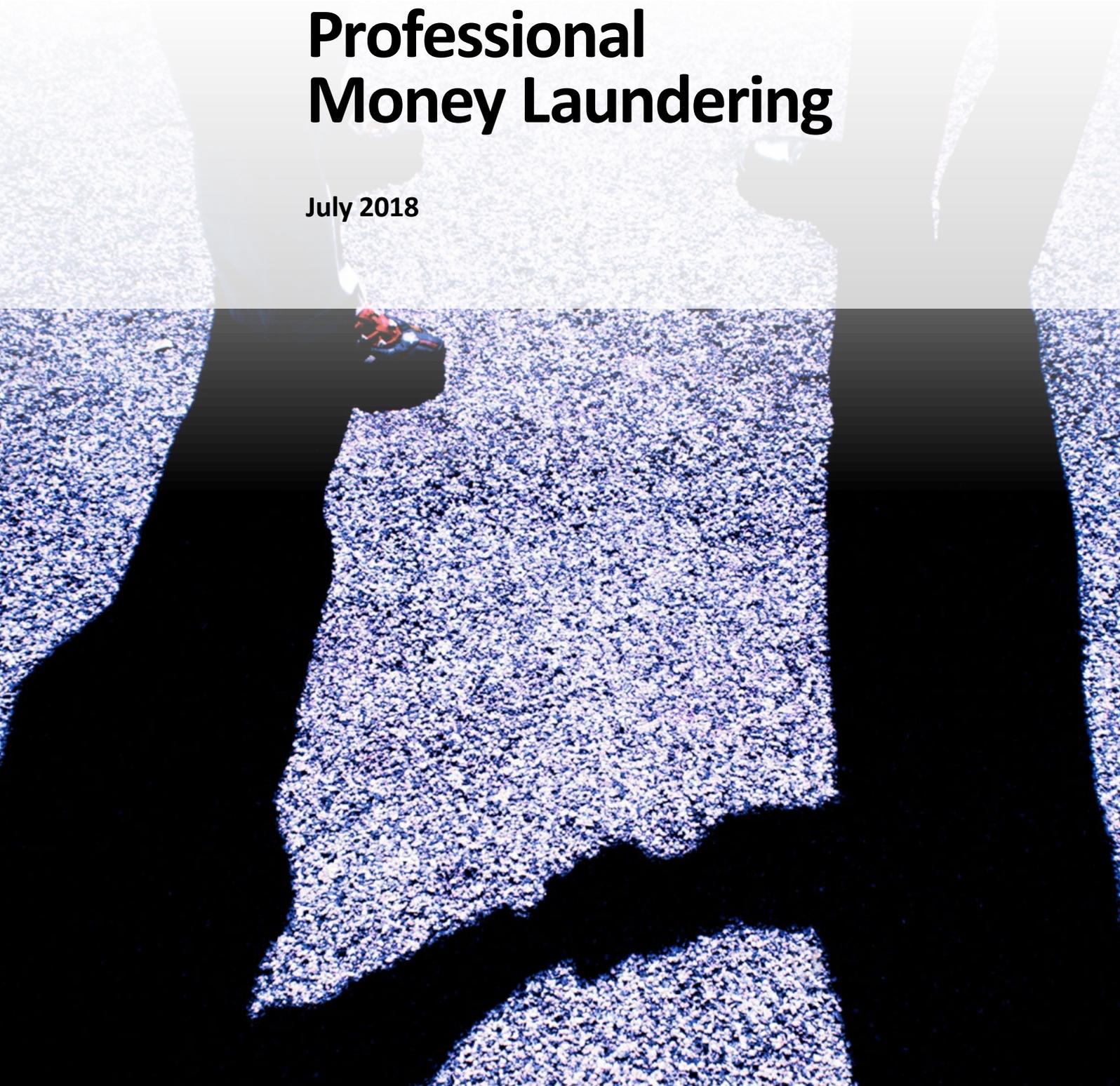
FATF Members and observers	Office	Country/Institution
TCSPs		
Member	Office	Institution
John Riches (Co-chair) and Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland



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

© 2018 FATF. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to

the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail:

contact@fatf-gafi.org)

Photocredits coverphoto ©Thinkstock

TABLE OF CONTENTS

Table of Acronyms	5
Executive Summary	6
Professional money laundering.....	9
Section I: Introduction	9
Purpose, Scope and Objectives.....	9
Structure of the Report.....	9
Methodology	10
Section II: Characteristics of Professional Money Laundering.....	10
Key Characteristics.....	10
Commissions / Fees.....	11
Advertising / Marketing.....	11
Record Keeping (Shadow Accountancy).....	12
Individuals, Organisations and Networks	12
Section III: Specialised Services and Business Models	15
Roles and Functions.....	16
General Business Model of Professional Money Laundering Networks	17
Stage I: Criminal proceeds are transferred to, or collected by, PMLs	18
Stage II: Layering stage executed by individuals and/or networks	18
Stage III: Laundered funds are handed back over to clients for investment or asset acquisition.....	19
Section IV: Types of Dedicated ML Organisations and Networks	19
Money Transport and Cash Controller Networks	19
Money Mule Networks.....	22
Digital Money and Virtual Currency Networks	25
Proxy Networks.....	26
Section V: Supporting Mechanisms Used by Professional Money Launderers.....	30
Trade-Based Money Laundering (TBML)	30
Account Settlement Mechanisms	33
Underground Banking and Alternative Banking Platforms	34
Section VI: Complicit/Criminal Financial Service Providers and Other Professionals	35
Money Value Transfer Services (MVTS) Providers.....	36
Financial Institutions	38
Legal and Professional Services.....	41
Payment Processing Companies.....	45
Virtual Currency Payment Products and Services (VCPSS).....	46
Section VII: Concluding Remarks.....	47
References	49

Boxes

Box 1. Khanani Money Laundering Organisation.....	13
Box 2. Cash Controller Network and Account Settlement Scheme.....	20
Box 3. Operation Kandil – Use of Cash Courier Network.....	22
Box 4. Use Of Money Mules to Launder Criminal Proceeds	23
Box 5. Avalanche Network.....	24
Box 6. Laundering Proceeds from Dark Web Drug Stores	25
Box 7. Facilitating the Laundering of Proceeds from Bank Fraud.....	27
Box 8. Creating Infrastructure to Launder Funds	28
Box 9. Large-Scale International Money Laundering Platform	29
Box 10. ML Network, Operating as a Trade-Based ML Scheme1	30
Box 11. Venezuelan Currency Smuggling Network.....	32
Box 12. Money Laundering as Part of an “Account Settlement Scheme” Between Various Criminal Organisations.....	33
Box 13. Investigation of Massive Underground Banking System	34
Box 14. Alternative Banking Platforms	35
Box 15. Corrupt Official Joining Criminal Enterprise to Launder Funds	35
Box 16. Use of Foreign Exchange Broker and “Quick Drop” Facilities	37
Box 17. Complicit MVTS Agents to Facilitate Third-Party ML	37
Box 18. General Manager and Chairman of a Foreign Bank	39
Box 19. Complicit Bank Employees, Securities Market Deals and the Sale of Shell Companies	40
Box 20. A Complicit Lawyer and Bank Employee	41
Box 21. Operation CICERO.....	42
Box 22. Use of Shell Companies and Accountant Providing Corporate Secretarial Services	43
Box 23. Money Laundering through Real Estate Investments, Gastronomic Services and Show Production Services Linked With Drug Trafficking.....	44
Box 24. International Payment Processor Providing ML Services.....	45
Box 25. Complicit Virtual Currency Exchanger	47

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 offence¹. 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," 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.

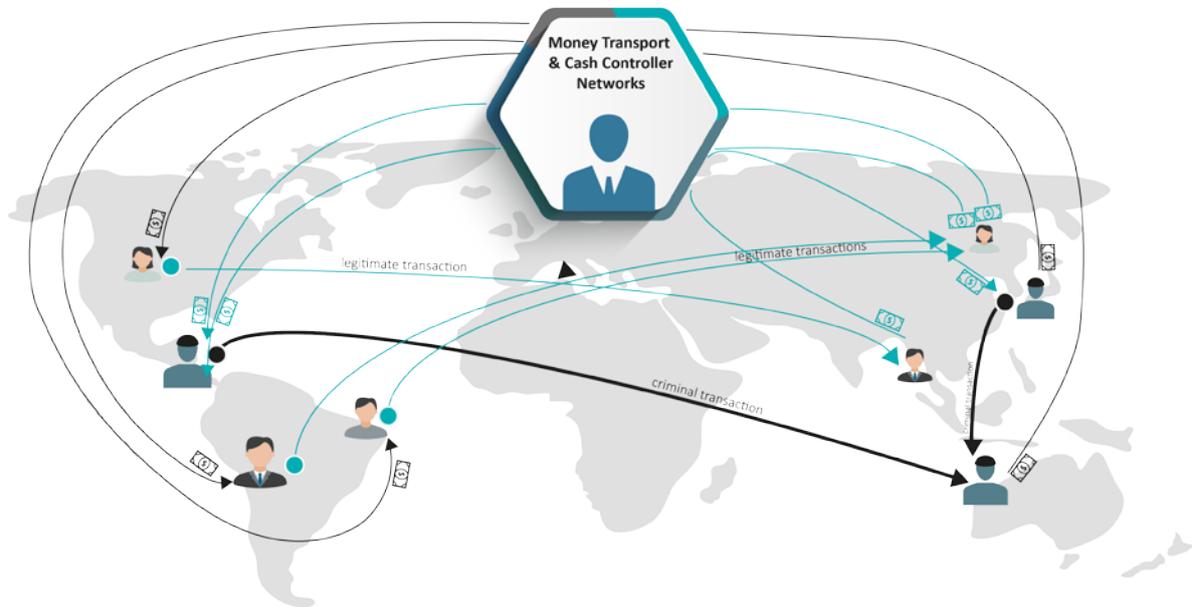
Money Transport and Cash Controller Networks

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

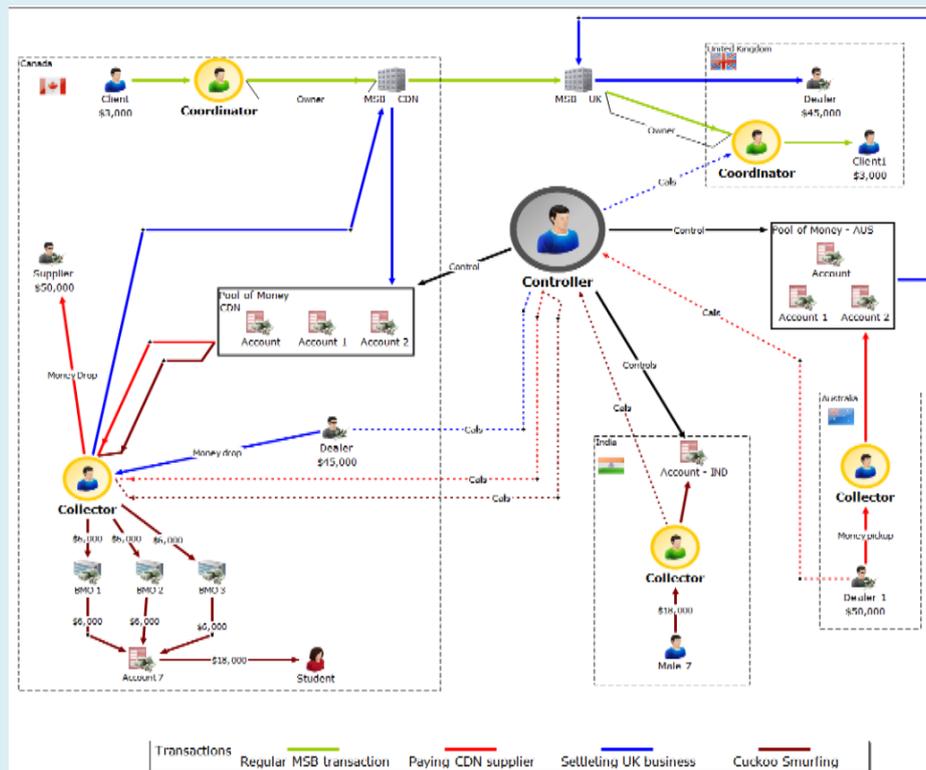
USD 3 000 GREEN: Basic transaction. The Canadian client wants to send money to another client in the UK. It is conducted through the MVTs provider's intermediary.

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. 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 cryptocurrency) 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 men¹). 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 group². 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 MVTTS 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, MVTs 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 deposited⁴. 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 ILOTA⁵, 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 inquiries. 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 institutions⁶.

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 commingled 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" services⁷, 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 (VCPSS)

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 VCPSS, 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 required⁸. 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 coordination 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

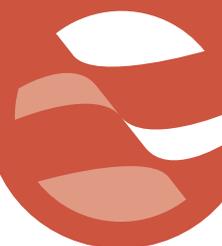
This threat report addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. A number of characteristics have been identified, 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-financialinvestigationguidance.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.

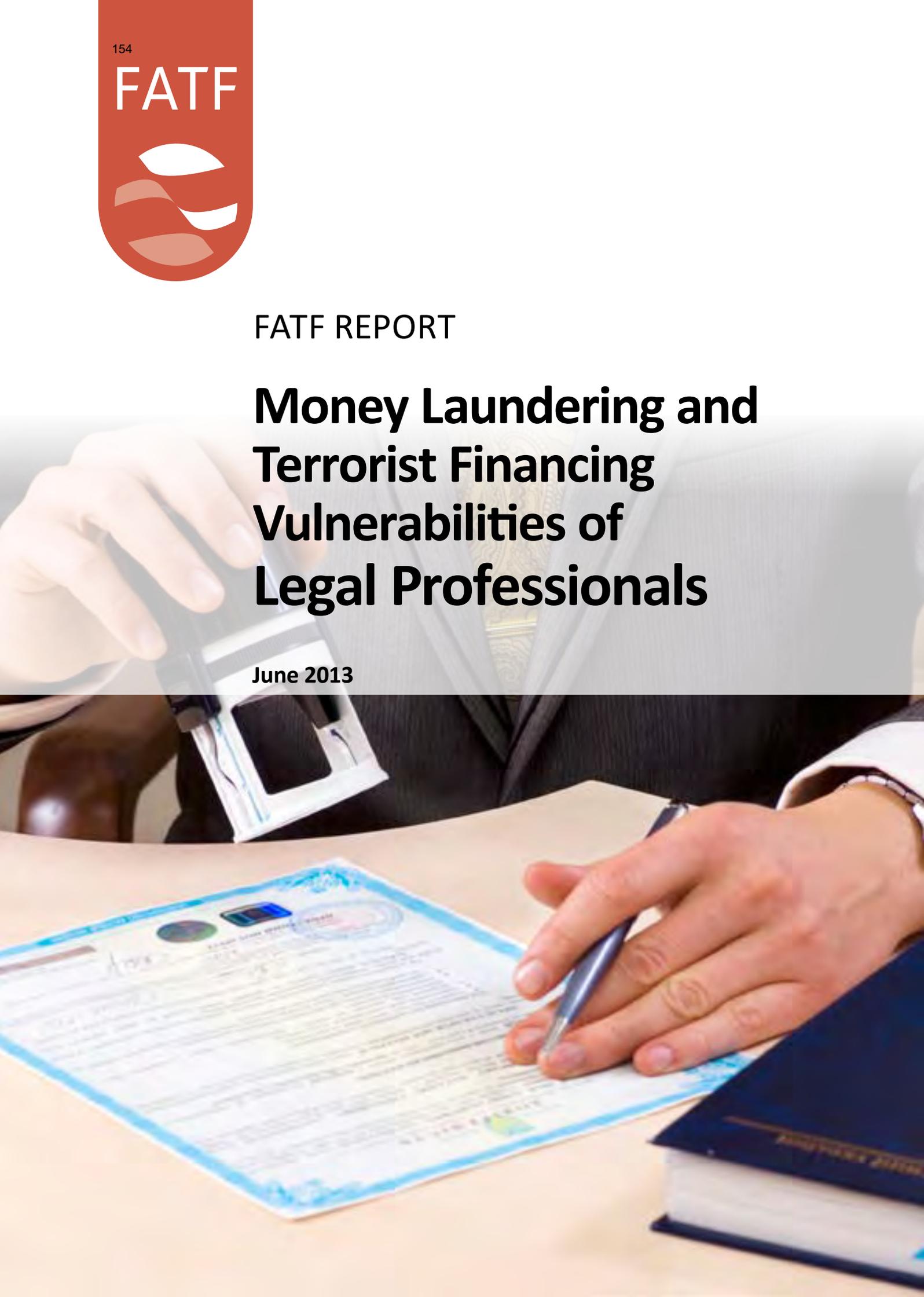
This report aims to assist authorities to target PMLs, as well as the structures that they utilise to launder funds, in order to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.



FATF REPORT

Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals

June 2013





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

© 2013 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

TABLE OF CONTENTS

ACRONYMS	3
EXECUTIVE SUMMARY	4
CHAPTER 1: INTRODUCTION	7
Background	7
Objectives	9
Methodology used in this study	10
CHAPTER 2: SCOPE OF THE LEGAL SECTOR	12
Types of legal professionals and their roles.....	12
Application of AML/CFT obligations	13
Unique features of the sector.....	15
CHAPTER 3: VULNERABILITIES	23
Vulnerabilities identified in literature.....	23
Vulnerabilities identified through STRs and asset recovery	24
Supervision of legal professionals.....	28
Disciplinary and criminal sanctions imposed on legal professionals.....	30
Taking enforcement action against legal professionals.....	30
CHAPTER 4: MONEY LAUNDERING TYPOLOGIES	34
Method 1: Misuse of client account	37
Method 2: Property purchases	44
Method 3: Creation of companies and trusts.....	54
Method 4: Management of companies and trusts.....	59
Method 5: Managing client affairs and making introductions	63
Method 6: Litigation.....	69
Method 7: Other methods.....	71
CHAPTER 5: RED FLAG INDICATORS	77
Red flags about the client	77
Red flags in the source of funds.....	79
Red flags in the choice of lawyer	80
Red Flags in the nature of the retainer.....	81
CHAPTER 6: CONCLUSIONS	83
Key findings	83
Opportunities for future action	84
ANNEX 1: BIBLIOGRAPHY	87
ANNEX 2: RESPONDENTS TO THE QUESTIONNAIRE	91
ANNEX 3: DEFINITIONS	92
ANNEX 4: TYPES OF LEGAL PROFESSIONALS	93
ANNEX 5: SCHEDULE OF CASES	96

ANNEX 6: ADDITIONAL CASE STUDIES	108
Method: Misuse of client account	108
Method: Purchase of real property	115
Method: Creation of companies and trusts.....	128
Method: Management of companies and trusts.....	137
Method: Managing client affairs and making introductions	139
Method: Use of specialised legal skills	145

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:

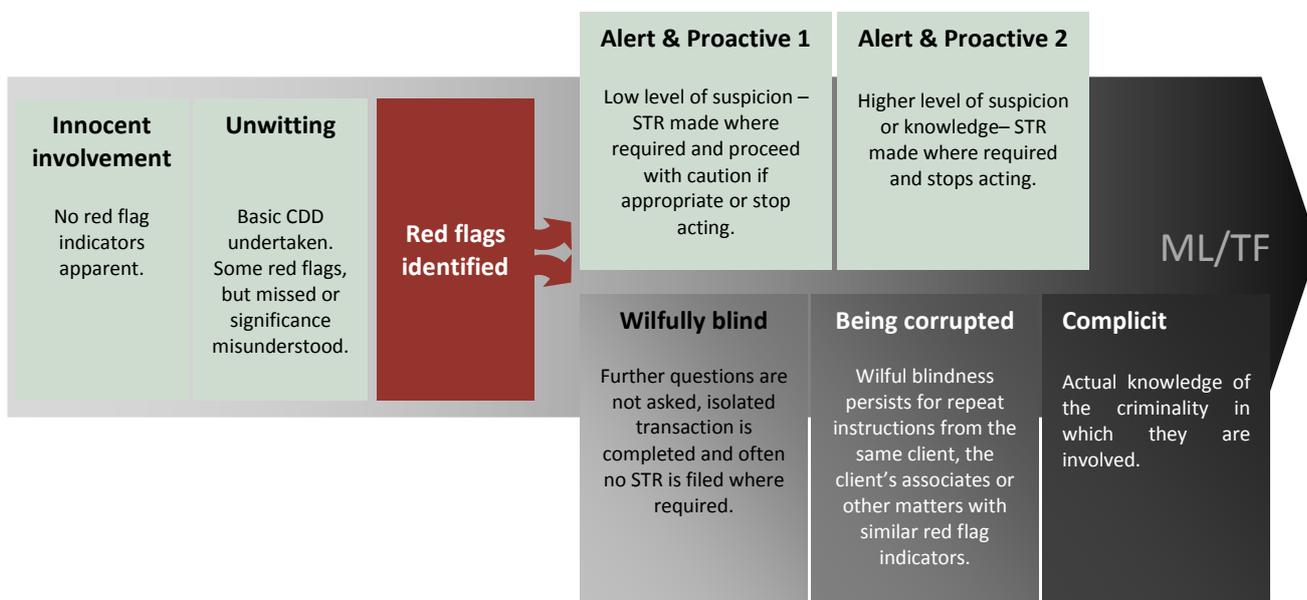
- misuse of client accounts;
- purchase of real property;
- creation of trusts and companies;
- management of trusts and companies;
- managing client affairs and making introductions;
- undertaking certain litigation; and
- setting up and managing charities.

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 indicators 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 Schneider² 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 laundering⁹.

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 were sufficiently recognised and that the responses provided to the questionnaire by SRBs and professional bodies were 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 countries¹⁴.

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 CDD¹⁵ 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 reports¹⁶, 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 Recommendations¹⁷, 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 seven¹⁸ 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 professionals¹⁹, 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 few²⁰ 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 conduct²². 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 ethics²³ 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 countries²⁴. 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 account²⁵ 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 few²⁶ 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 below¹:

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 previously²⁷ 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 challenges²⁹ 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 countries³⁰, 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 Columbia³¹ 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 independence 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 reported³³.

REPORTING BY LEGAL PROFESSIONALS

The table below shows the number of reports as identified via the FATF questionnaire³⁴.

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

Country	Legal professionals			DNFBPs	Total
	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 professionals³⁵, 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.

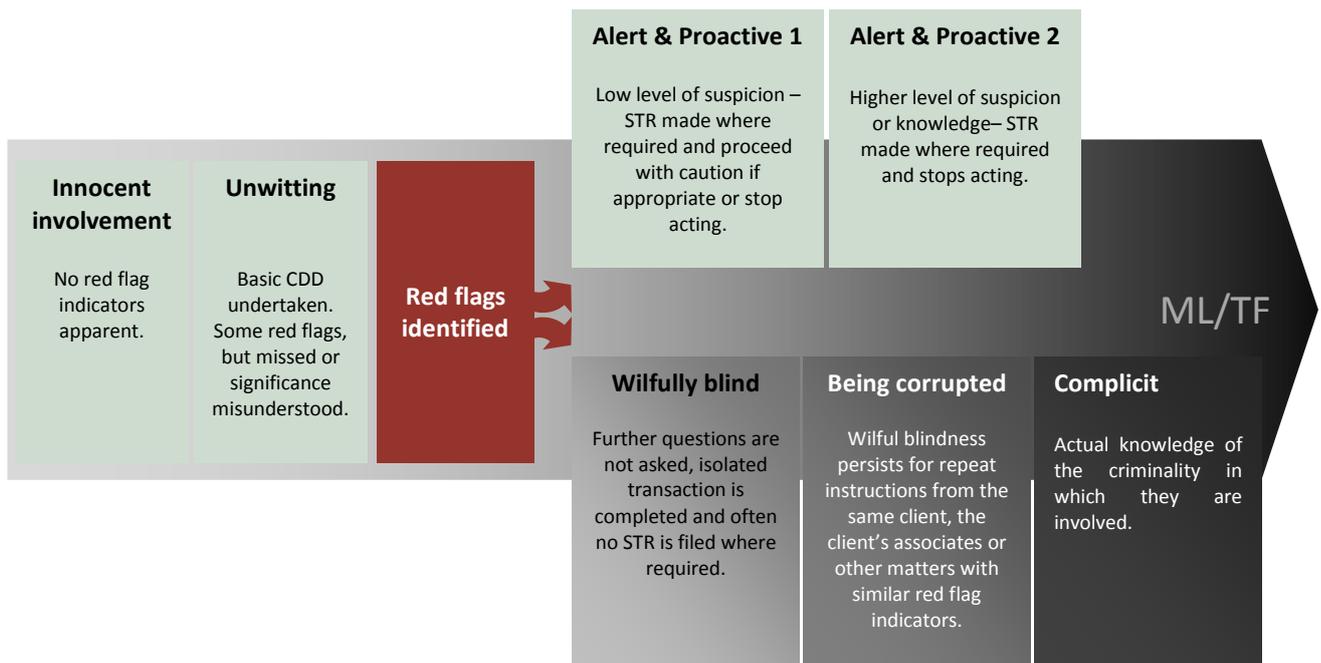
At the outset of this typology exercise, the objective was to identify examples of complicit involvement by legal professionals on the one hand and unknowing involvement on the other. A more detailed review of the case studies has indicated that such a stark distinction is not really appropriate.

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 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/secretcy 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:	<ul style="list-style-type: none"> • 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:	<ul style="list-style-type: none"> • 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 previously⁴⁰ 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 Permanent 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 rationale 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 clients⁴² – 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 or 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 Duynne, 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 directly⁴⁸ 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. Notaries⁴⁹

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	<ul style="list-style-type: none"> • Client known to have convictions for acquisitive crime
Red flag indicators:	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Disproportionate amounts of cash
Red flag indicators:	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Disproportionate level of private funding not consistent with the known legitimate income
Red flag indicators:	

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)

<p>Case 75</p> <p>Red flag indicators:</p>	<ul style="list-style-type: none"> • 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 was not 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)

<p>Case 76</p> <p>Red flag indicators:</p>	<ul style="list-style-type: none"> • 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 through 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 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 m² 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 were engaging in fraud by attempting to sell properties they did not own. Some purchases aborted and funds were 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	<ul style="list-style-type: none"> • Changes in instructions
Red flag indicators:	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • There are attempts to disguise the real owner or parties to the transaction
Red flag indicators:	<ul style="list-style-type: none"> • 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 offshore 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 Osborne – 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	<ul style="list-style-type: none"> • Client holds a public position in a high risk country
Red flag indicators:	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Client holds a public position in a high risk country
Red flag indicators:	<ul style="list-style-type: none"> • 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.)

<p>Case 113</p> <p>Red flag indicators:</p>	<ul style="list-style-type: none"> • 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

<p>Case 114</p> <p>Red flag indicators:</p>	<ul style="list-style-type: none"> • 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 struck 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



Financial Action Task Force
Groupe d'action financière

RBA GUIDANCE FOR LEGAL PROFESSIONALS

23 October 2008

© FATF/OECD 2008

All rights reserved. No reproduction, copy, transmission or translation of this publication may be made without written permission.

**Applications for permission to reproduce all or part of this publication should be made to:
FATF Secretariat, OECD, 2 rue André Pascal 75775 Paris Cedex 16, France**

TABLE OF CONTENTS

SECTION ONE: USING THE GUIDANCE PURPOSE OF THE RISK-BASED APPROACH	4
Chapter One: Background and Context	4
Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges	8
Chapter Three: FATF and the Risk-Based Approach.....	11
SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES	15
Chapter One: High-level principles for creating a risk-based approach.....	15
Chapter Two: Implementation of the Risk-Based Approach.....	19
SECTION THREE: GUIDANCE FOR LEGAL PROFESSIONALS ON IMPLEMENTING A RISK-BASED APPROACH.....	25
Chapter One: Risk Categories.....	25
Chapter Two: Application of a Risk-Based Approach	31
Chapter Three: Internal Controls	34
ANNEXES	36
ANNEX 1.....	36
A. Financial Action Task Force Documents	36
B. Legislation/and Court Decisions	36
C. Links to Information on the Supervisory Program in Certain Countries	36
D. Guidance on the Risk-based Approach	37
E. Other sources of information to help assist countries’ and legal professionals’ risk assessment of countries and cross-border activities.....	37
ANNEX 2.....	39
ANNEX 3.....	41

SECTION ONE: USING THE GUIDANCE

PURPOSE OF THE RISK-BASED APPROACH

Chapter One: Background and Context

1. In June 2007, the FATF adopted Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures, which includes guidance for public authorities and guidance for financial institutions. This was the culmination of extensive consultation between private and public sector members of an Electronic Advisory Group (EAG) established by the FATF.

2. In addition to financial institutions, the FATF Recommendations also cover a number of designated non-financial businesses and professions (DNFBPs). At its June 2007 meeting, the FATF's Working Group on Evaluation and Implementation (WGEI) endorsed a proposal to convene a meeting of the representatives from the DNFBPs to assess the possibility of developing Guidance on the risk-based approach for their sectors, using the same structure and style as the completed Guidance for financial institutions.

3. This meeting was held in September 2007 and was attended by members of organisations which represent lawyers, notaries, trust and company service providers (TCSPs), accountants, casinos, real estate agents and dealers in precious metals and dealers in precious stones. This private sector group expressed an interest in contributing to FATF Guidance on implementing a risk-based approach for their sectors. The Guidance for the DNFBPs would follow the principles of the risk-based approach already established by FATF, and would highlight risk factors specific to the DNFBPs, as well as suggest mitigation strategies that fit with the particular activities and businesses of the DNFBPs. The FATF established another EAG to facilitate the work.

4. The private sector group met again in December 2007 and was joined by a number of specialist public sector members. Separate working groups comprising public and private sectors members were established, and private sector chairs were appointed.

5. The EAG continued work until this Guidance for legal professionals was presented to the WGEI. After further international consultation with both public and private sectors, the FATF adopted this Guidance at its October 2008 Plenary. Guidance for each of the other DNFBP sectors is being published separately.

Purpose of the Guidance

6. The purpose of this Guidance is to:
- Support the development of a common understanding of what the risk-based approach involves.
 - Outline the high-level principles involved in applying the risk-based approach.
 - Indicate good practice in the design and implementation of an effective risk-based approach.

7. However, it should be noted that applying a risk-based approach is not mandatory. A properly applied risk-based approach does not necessarily mean a reduced burden, although it should result in a more cost effective use of resources. For some countries, applying a rules-based system might be more appropriate. Countries¹ will need to make their own determinations on whether to apply a risk-based approach, based on their specific money laundering/terrorist financing risks, size and nature of the DNFBP activities, and other relevant information. The issue of timing is also relevant for countries that may have applied anti-money laundering/counter-terrorist financing (AML/CFT) measures to DNFBPs, but where it is uncertain whether the DNFBPs have sufficient experience to implement and apply an effective risk-based approach.

Target Audience, Status and Content of the Guidance

8. This Guidance has been prepared for, and in relation to, legal professionals.² The legal professionals sector includes various professions, including lawyers and notaries, and in some countries there are also different categories of lawyers *e.g.* barristers and solicitors. Many legal professionals are required to comply with specific legislation and regulation and rules and regulations enacted or adopted by professional associations or other self regulatory organisations (SROs). The activities of legal professionals are very diverse, as are the legal and professional obligations with which they are required to comply. The specifics of an individual legal professional's and/or a firm or other collection of legal professionals' particular risk-based processes should accordingly be determined based on the activities undertaken by the legal professional, the ethical and existing supervisory structure for legal professionals and the susceptibility of a legal professional's activities (both generally and particularly) to money laundering and terrorist financing.

9. Legal professionals provide a range of services and activities that differ vastly, such as in their methods of delivery and in the depth and duration of the relationships formed with clients. This Guidance is written at a high level to take into account the differing practices of legal professionals in different countries, and the different levels and forms of supervision or monitoring that may apply. It is not intended as a template for national legislation imposing obligations on legal professionals or SROs. Each country and its national authorities should aim to establish an active dialogue with its legal professionals and other DNFBP sectors that will be mutually beneficial in establishing effective systems to combat money laundering and terrorist financing.

10. The following general observations about legal professionals should help inform the approach. Consideration should also be given to the particular activities performed by legal professionals on a national, provincial, or local basis. Because legal professionals typically refer to those benefiting from their services as "clients" rather than "customers", that term is thus generally used throughout this paper, except where specific terms of art such as "customer due diligence" and "know your customer" are used (in such cases a customer can be equated to a client).

11. For purposes of this Guidance, legal professionals include both lawyers and notaries.
- Lawyers are members of a regulated profession and are bound by their specific professional rules and regulations. Their work is fundamental to promoting adherence to the rule of law in the countries in which they practice. Lawyers hold a unique position in society by providing

¹ All references in the FATF Recommendations and in this document to country or countries apply equally to territories or jurisdictions.

² This refers to sole legal practitioners and partners or employed legal professionals within professional firms. It is not meant to refer to "internal" (*i.e.* in-house) professionals that are employees of other types of businesses, nor to legal professionals working for government agencies, who may already be subject to separate measures that would combat money laundering and terrorist financing. See FATF 40 Recommendations Glossary, definition of "Designated Non-Financial Businesses and Professions" (e).

access to law and justice for individuals and entities, assisting members of society to understand their increasingly complex legal rights and obligations, and assisting clients to comply with the law. Lawyers have their own professional and ethical codes of conduct by which they are regulated. Breaches of the obligations imposed upon them can result in a variety of sanctions, including disciplinary and criminal penalties. The provisions contained in this Guidance, when applied by each country, are subject to professional secrecy and legal professional privilege. As is recognised by the interpretative note to the FATF Recommendation 16, the matters that would fall under legal professional privilege or professional secrecy and that may affect any obligations with regard to money laundering and terrorist financing are determined by each country. Likewise, ethical rules that impose obligations, duties, and responsibilities on legal professionals vary by country. The legal professionals' counseling and advisory role, especially in an increasing regional and global marketplace, does not generally involve a cash handling function.

- Both civil and common law countries have notaries, but the roles of civil and common law notaries differ. Common law mainly differs from civil law in that precedents can be drawn from case law, while in civil systems codified rules are applied by judges to the cases before them. In some common law countries, the common law notary public is a qualified, experienced practitioner, trained in the drafting and execution of legal documents. In other common law countries, the notary public is a public servant appointed by a governmental body to witness the signing of important documents (such as deeds and mortgages) and administer oaths. Known only in civil law jurisdictions, civil law notaries are both members of an autonomous legal profession – although regulated by the law – and qualified public officials, as they are appointed by the State through a selective public contest among law graduates. Civil law notaries, who are bound by an obligation of impartiality with respect to both parties, must be regarded, in matters of real property (conveyancing), family law, inheritance and corporate legal services as practising non-contentious activities. They act as gatekeepers by drafting, ensuring the legality and certainty of the instruments and the authenticity of signatures presented to them; providing as well a public fiduciary function by performing the role of a trusted third party . Civil law notaries are obliged by law not to detach themselves from the core of the relationship, therefore making them responsible for all aspects of the deed. For this reason, civil law notaries are assigned functions of a public nature as part of their legal assignments. In civil law jurisdictions, notarial written documents are particular means of evidence, unlike in the common law systems, which are based on the free evidence of witnesses in court: special supreme State powers are devolved to civil law notaries and they can therefore assign “public authority” to each deed they perform. Thereby the civil law notary’s deed has a special effectiveness in a trial, whereby it is a means of peremptory binding evidence; furthermore, it is as judicially enforceable as a judgement; if it complies with the law, it can be registered on a public registry. Owing to these characteristics, civil law notaries play a different role in comparison to the services provided by other legal professionals. This Guidance does not cover those common law notaries who perform merely administrative acts such as witnessing or authenticating documents, as these acts are not specified activities.

12. Recommendation 12 mandates that the requirements for customer due diligence requirements (CDD), record-keeping, and paying attention to all complex, unusual large transactions set out in Recommendations 5, 6, and 8 to 11 apply to DNFBPs in certain circumstances. Recommendation 12 applies to legal professionals when they prepare for and carry out certain specified 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.

This Guidance has been prepared to assist legal professionals in those situations. Unless legal advice and representation consists of preparing for or carrying out transactions relating to these specified activities, it is not subject to the FATF Recommendations. The Recommendations would thus not cover, for example, an initial meeting before any preparatory work is carried out, or the usual level of advice given at legal aid or other “walk up” clinics.

13. It is possible that more than one legal professional will be preparing for or carrying out a transaction, in which case they will all need to observe the applicable CDD and record-keeping obligations. However, several legal professionals may be involved in a transaction for a specified activity but not all are preparing for or carrying out the overall transaction. In that situation, those legal professionals providing advice or services (*e.g.* a local law validity opinion) peripheral to the overall transaction who are not preparing for or carrying out the transaction may not be required to observe the applicable CDD and record-keeping obligations.

14. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions and AMLCFT controls, and Recommendation 21 regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, apply to DNFBSs subject to the certain qualifications. Specifically, Recommendation 16 applies to legal professionals when they engage in a financial transaction on behalf of a client, in relation to the activities referred to in Recommendation 12. Recommendation 16, however, provides that legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. The lawyer-client relationship is protected by law, regulations, and rules, and codes of conduct (such as legal professional privilege) in many countries, including in some countries by constitutional provisions. This is recognised by the Interpretative Note to Recommendation 16.

15. The wider audience for this Guidance includes countries, regulators, and self-regulatory organisations (SROs), which are considering how to apply AML/CFT measures to legal professionals. Countries need to identify the most appropriate regime, tailored to address individual country risks, which takes into consideration the activities and professional and ethical codes of conduct of legal professionals in their countries. This regime should recognise the differences between the DNFBS sectors, as well as the differences between the DNFBSs (particularly legal professionals) and financial institutions. However, this Guidance does not override the purview of national authorities. The manner in which legal professionals, SROs, or other supervisory bodies approach their responsibilities under a risk-based CDD system must necessarily be informed by and conform with the existing legal and oversight framework within each country’s jurisdiction.

- To the extent a country has adopted a risk-based approach regime, the legal professionals practising in that country should refer to that country’s guidance for that regime.
- This Guidance does not supplant specific professional guidance issued by designated competent authorities or SROs in a particular country, and does not constitute a legal interpretation of AML or CFT obligations of legal professionals, and should not be relied on by legal professionals or the judiciary in determining whether a legal professional has complied with his or her AML or CFT obligations.

16. The provisions in this Guidance are subject to applicable professional secrecy, legal professional privilege or rules of professional conduct, which are determined by each country.

Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges

The purpose of the Risk-Based Approach

17. The FATF Recommendations contain language that permits countries to some degree to adopt a risk-based approach to combating money laundering and terrorist financing. That language also authorises countries to permit DNFBPs to use a risk-based approach in applying certain of their AML and CFT obligations.

18. By adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk. This can inadvertently lead to a ‘tick box’ approach with the focus on meeting regulatory requirements rather than on combating money laundering or terrorist financing efficiently and effectively.

19. A number of the DNFBP sectors, including legal professionals, are already subject to regulatory or professional requirements (including as promulgated by SROs) that complement AML/CFT measures. For example, by virtue of their professional codes of conduct, many lawyers are already subject to an obligation to identify their clients (*e.g.* to check for conflict of interest) and the substance of the matter submitted to them by such clients, in order to appreciate the consequences that their advice may have. If a lawyer provides legal advice to a client that helps the client commit an offence, that lawyer may, depending on the lawyer’s state of knowledge, become an accomplice to the offence. This Guidance must be considered in the context of these professional and ethical codes of conduct. Where possible, it will be beneficial for legal professionals (and relevant authorities and SROs) to devise their AML/CFT policies and procedures in a way that harmonises with other regulatory or professional requirements. A risk-based AML/CFT regime should not impede free access to the services provided by legal professionals for legitimate purposes, but should create barriers to those who seek to misuse these services.

20. A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. Countries will need to identify the main vulnerabilities and address them accordingly. Legal professionals will need this assistance and information to help them to identify higher risk clients and services, including delivery channels, and geographical locations. These are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve.

21. The strategies to manage and mitigate money laundering and terrorist financing are typically aimed at preventing the activity from occurring through a mixture of deterrence (*e.g.* appropriate CDD measures), detection (*e.g.* monitoring and suspicious transaction reporting), and record-keeping so as to facilitate investigations.

22. Proportionate procedures should be designed based on assessed risk. Higher risk areas should be subject to enhanced procedures; this would include measures such as enhanced CDD checks and enhanced transaction monitoring. It also follows that in instances where risks are low, simplified, modified or reduced controls may be applied.

23. There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, an effective risk-based approach does involve identifying and categorising money laundering and terrorist financing risks and establishing reasonable controls based on risks identified.

24. An effective risk-based approach will allow legal professionals to exercise reasonable business and professional judgement with respect to clients. Application of a reasoned and well-articulated risk-based approach will justify the judgements made with regard to managing potential money laundering and terrorist financing risks. A risk-based approach should not be designed to prohibit or impede legal professionals from continuing with legitimate practice – especially given their role in society and the proper functioning of the justice system - or from finding innovative ways to diversify or expand their practices.

25. Regardless of the strength and effectiveness of AML/CFT controls, criminals will continue to attempt to move illicit funds undetected and will, from time to time, succeed. Criminals are more likely to target the DNFBP sectors, including legal professionals, if other routes become more difficult. For this reason, DNFBPs may be more or less vulnerable depending on the effectiveness of the AML/CFT procedures applied in other sectors. A risk-based approach allows DNFBPs, including legal professionals, to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

26. A reasonably designed and effectively implemented risk-based approach can provide an appropriate and effective control structure to manage identifiable money laundering and terrorist financing risks. However, it must be recognised that any reasonably applied controls, including controls implemented as a result of a reasonably designed and effectively implemented risk-based approach, will not identify and detect all instances of money laundering or terrorist financing. Therefore, designated competent authorities, SROs, law enforcement, and judicial authorities must take into account and give due consideration to a well reasoned risk-based approach. When there is a failure to implement an adequately designed risk-based approach or failure of a risk-based programme that was not adequate in its design, designated competent authorities, SROs, law enforcement or judicial authorities should take action as necessary and appropriate.

Potential Benefits and Challenges of the Risk-Based Approach

Benefits

27. The adoption of a risk-based approach to combating money laundering and terrorist financing can yield benefits for all parties, including the public. Applied effectively, the approach should allow a more efficient and effective use of resources and minimise burdens on clients. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively.

28. For legal professionals, the risk-based approach allows the flexibility to approach AML/CFT obligations using specialist skills and responsibilities. This requires legal professionals to take a wide and objective view of their activities and clients.

29. Efforts to combat money laundering and terrorist financing should also be flexible in order to adapt as risks evolve. As such, legal professionals should use their judgement, knowledge and expertise to develop an appropriate risk-based approach for their particular organisation, structure and practice activities.

Challenges

30. The risk-based approach is not necessarily an easy option and is challenging to both public and private sector entities. Some challenges may be inherent to the use of the risk-based approach. Others may stem from the difficulties in making the transition to a risk-based system. A risk-based approach requires resources and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems, and to train personnel. It further requires that sound and well-trained judgement be exercised in the design and implementation of procedures, and systems. It will certainly lead to a greater diversity in practice that should lead to innovations and improved compliance. However, it may also cause uncertainty regarding

expectations, difficulty in applying uniform regulatory treatment, and lack of understanding by clients regarding information required.

31. Implementing a risk-based approach requires that legal professionals have a sound understanding of the risks and are able to exercise sound judgement. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. The process will always benefit from information sharing by designated competent authorities and SROs. The provision of good practice guidance is also valuable. Attempting to pursue a risk-based approach without sufficient expertise may lead to flawed judgements. Legal professionals may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, thereby creating vulnerabilities. They, and (if applicable) their staff members, may be uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. This may also be true at various levels of management. However, in situations where management fails to recognise or underestimate the risks, a culture may develop that allows for inadequate resources to be devoted to compliance, leading to potentially significant compliance failures.

32. Designated competent authorities and SROs should place greater emphasis on whether legal professionals have an effective decision-making process with respect to risk management. Sample testing may be used or individual decisions reviewed as a means to test the effectiveness of a legal professional's overall risk management. Designated competent authorities and SROs should recognise that even though appropriate risk management structures and procedures are regularly updated, and the relevant policies, procedures, and processes are followed, decisions may still be made that are incorrect in light of additional information that was not reasonably available at the time.

33. In implementing the risk-based approach, legal professionals should be given the opportunity to make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices. Such potential diversity of practice will require that designated competent authorities and SROs make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges for staff working to monitor compliance. The existence of good practice guidance, continuing legal education, and supervisory training, industry studies and other materials will assist the designated competent authority or an SRO in determining whether a legal professional has made sound risk-based judgements.

34. Recommendation 25 requires adequate feedback to be provided to the financial sector and DNFBPs. Such feedback helps institutions, firms and businesses to more accurately assess the money laundering and terrorist financing risks and to adjust their risk programmes accordingly. This in turn makes the detection of suspicious activity more likely and improves the quality of any required suspicious transaction reports. As well as being an essential input to any assessment of country or sector wide risks, the promptness and content of such feedback is relevant to implementing an effective risk-based approach.

The potential benefits and potential challenges can be summarised as follows:

Potential Benefits:

- Better management of risks and cost-benefits
- Focus on real and identified threats
- Flexibility to adapt to risks that change over time

Potential Challenges:

- Identifying appropriate information to conduct a sound risk analysis
- Addressing short term transitional costs
- Greater need for more expert staff capable of making sound judgements. Regulatory response to potential diversity of practice.

Chapter Three: FATF and the Risk-Based Approach

35. The varying degrees of risk of money laundering or terrorist financing for particular types of DNFBPs, including legal professionals, or for particular types of clients, or transactions is an important consideration underlying the FATF Recommendations. According to the Recommendations, with regard to DNFBPs there are specific Recommendations where the degree of risk is an issue that a country either must take into account (if there is higher risk), or may take into account (if there is lower risk).

36. The risk-based approach is either incorporated into the Recommendations (and the Methodology) in specific and limited ways in a number of Recommendations, or it is inherently part of or linked to those Recommendations. For instance, for DNFBPs, including legal professionals risk is addressed in three principal areas (a) Customer/client Due Diligence (R.5, 6, 8 and 9); (b) legal professionals and/or firms' internal control systems (R.15); and (c) the approach of oversight/monitoring of DNFBPs, including legal professionals (R.24).

Client Due Diligence (R. 5, 6, 8 and 9)

37. Risk is referred to in several forms:

a) Higher risk – Under Recommendation 5, a country must require its DNFBPs, including legal professionals, to perform enhanced due diligence for higher-risk clients, business relationships or transactions. Recommendation 6 (politically exposed persons) is an example of this principle and is considered to be a higher risk scenario requiring enhanced due diligence.

b) Lower risk – A country may also permit legal professionals to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). Legal professionals may thus reduce or simplify (but not avoid completely) the required measures.

c) Risk arising from innovation – Under Recommendation 8, a country must require legal professionals to give special attention to the risks arising from new or developing technologies that might favour anonymity.

d) Risk assessment mechanism – The FATF standards require that there be an adequate mechanism by which designated competent authorities or SROs assess or review the procedures adopted by legal professionals to determine the degree of risk and how they manage that risk, as well as to review the actual determinations themselves. This expectation applies to all areas where the risk-based approach applies. In addition, where the designated competent authorities or SROs have issued guidelines on a suitable approach to risk-based procedures, it will be important to establish that these have been followed. The Recommendations also recognise that country risk is a necessary component of any risk assessment mechanism (R.5 & R.9).

Internal control systems (R.15)

38. Under Recommendation 15, the development of “appropriate” internal policies, training and audit systems will need to include a specific, and ongoing, consideration of the potential money laundering and terrorist financing risks associated with clients, products and services, geographic areas of operation and so forth. The Interpretative Note to Recommendation 15 makes it clear that a country may allow legal professionals to have regards to the money laundering and terrorist financing risks, and to the size of the business, when determining the type and extent of measures required.

Regulation and oversight by designated competent authorities or SROs (R.24)

39. Countries should ensure that legal professionals are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in a given business, *i.e.* if there is a low risk then reduced monitoring measures may be taken.

Applicability of the risk-based approach to terrorist financing

40. There are both similarities and differences in the application of a risk-based approach to terrorist financing and money laundering. They both require a process for identifying and assessing risk. However, the characteristics of terrorist financing make its detection difficult and the implementation of mitigation strategies may be challenging due to considerations such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

41. Funds that are used to finance terrorist activities may be derived either from criminal activity or may be from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing, though the activity, which may be indicative of suspicion, may not be identified as or connected to terrorist financing. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering. Where funds are from legal sources then it is even more difficult to determine if they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services to further their goals, with the only covert fact being the intended use of such materials and services purchased. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering. In all cases, however, legal professionals are not responsible for determining the type of underlying criminal activity or intended terrorist purpose.

42. The ability of legal professionals to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities is significantly more challenging than is the case for potential money laundering and other suspicious activity. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering).

43. Specific individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which such sanctions apply and the obligations on legal professionals to comply with those sanctions are decided by individual countries and are not a function of risk. Legal professionals may commit a criminal offence if they undertake business with a listed individual, organisation or country, or its agent, in contravention of applicable sanctions.

44. For these reasons, this Guidance has not comprehensively addressed the application of a risk-based process to terrorist financing. It is clearly preferable that a risk-based approach be applied where reasonably practicable, but further consultation with key stakeholders is required to identify a more comprehensive set of indicators of the methods and techniques used for terrorist financing, which can then be factored into strategies to assess terrorist financing risks and devise measures to mitigate them. DNFBPs, including legal professionals, would then have an additional basis upon

40-44 and such subsequent consultations when they occur.

Limitations to the risk-based approach

45. There are circumstances in which the application of a risk-based approach will not apply, or may be limited. There are also circumstances in which the application of a risk-based approach may not apply to the initial stages of a requirement or process, but then will apply to subsequent stages. The limitations to the risk-based approach are usually the result of legal or regulatory requirements that mandate certain actions to be taken.

46. Requirements to freeze assets of identified individuals or entities, in countries where such requirements exist, are independent of any risk assessment. The requirement to freeze is absolute and cannot be impacted by a risk-based process. Similarly, while the identification of potential suspicious transactions can be advanced by a risk-based approach, in countries where such obligations exist, the reporting of such suspicious transactions, once identified, is not risk-based. (See paragraph 119.)

47. CDD comprises several components – Identification and verification of the identity of clients and of beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing due diligence. Of these components, the identification and verification of identity of clients are requirements that must be completed regardless of the risk-based approach. However, in relation to all other CDD components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep records and documents that have been obtained for due diligence purposes, as well as transaction records, is not dependent on risk levels.

48. Countries may allow legal professionals to apply reduced or simplified measures where the risk of money laundering or terrorist financing is lower. However, these reduced or simplified measures do not necessarily apply to all aspects of CDD. Where these exemptions are subject to certain conditions being met, it is necessary to verify that these conditions apply, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. Information beyond client identity, such as client location, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a client should be sufficient to determine whether to go further, and in many cases client monitoring will provide additional information.

49. Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk clients, monitoring is needed to verify that transactions match the initial low risk profile and if not, trigger a process for appropriately revising the client's risk rating. Equally, risks for some clients may only become evident once a relationship with a client has begun. This makes appropriate and reasonable monitoring of client transactions an essential component of a properly designed risk-based approach; however, within this context it should be understood that not all transactions or clients will be monitored in exactly the same way. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this could be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption. Given the relationship between a legal professional and his/her client, the most effective form of ongoing monitoring will often be continued observance and awareness of a client's activities by the legal professional. This requires legal professionals to be alert to this basis of monitoring and for training of legal professionals to take this feature into account.

Distinguishing Risk-Based Monitoring and Risk-Based Policies and Processes

50. Risk-based policies and processes should be distinguished from risk-based monitoring by designated competent authorities or SROs. There is a general recognition within monitoring practice that resources should be allocated taking into account the risks posed by individual practices. The methodology adopted by the designated competent authorities or SROs to determine allocation of monitoring resources should cover the practice focus, the risk profile and the internal control environment, and should permit relevant comparisons between practices. Most fundamentally, such methodology needs to recognize that the relationship between the legal professional and the client is often an on-going one. The methodology used for determining the allocation of resources will need updating on an ongoing basis so as to reflect the nature, importance and scope of the risks to which individual practices are exposed. Consequently, this prioritisation should lead designated competent authorities or SROs to focus increased regulatory attention to legal professionals who engage in activities assessed to be of higher risk of money laundering or terrorist financing.

51. However, it should also be noted that the risk factors taken into account to prioritise the designated competent authorities or SROs' work will depend not only on the intrinsic risk associated with the activity undertaken, but also on the quality and effectiveness of the risk management systems put in place to address such risks.

52. Since designated competent authorities or SROs should have already assessed the quality of risk management controls applied by legal professionals, it is reasonable that their assessments of these controls be used, at least in part, to inform money laundering and terrorist financing risk assessments conducted by individual firms or businesses.

Summary box: A risk-based approach to countering money laundering and terrorist financing at the national level: key elements for success

- Legal professionals, designated competent authorities and/or SROs should have access to reliable and actionable information about the threats.
- There must be emphasis on cooperative arrangements among the policy makers, law enforcement, regulators, and the private sector.
- Authorities should publicly recognise that the risk-based approach will not eradicate all elements of risk.
- Authorities have a responsibility to establish an atmosphere in which legal professionals need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Designated competent authorities' and/or SROs' supervisory staff must be well-trained in the risk-based approach, both as applied by designated competent authorities/SROs and by legal professionals.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

Chapter One: High-level principles for creating a risk-based approach

53. The application of a risk-based approach to countering money laundering and the financing of terrorism will allow designated competent authorities or SROs and legal professionals to use their resources most effectively. This chapter sets out five high-level principles that should be considered by countries when designing a risk-based approach applicable to legal professionals. They could be considered as setting out a broad framework of good practice.

54. The five principles set out in this Guidance are intended to assist countries in their efforts to improve their AML/CFT regimes. They are not intended to be prescriptive, and should be applied in a manner that is well-considered, is appropriate to the particular circumstances of the country in question and takes into account the way in which legal professionals are regulated in that country and the obligations they are required to observe.

Principle One: Understanding and responding to the threats and vulnerabilities: a national risk assessment

55. Successful implementation of a risk-based approach to combating money-laundering and terrorist financing depends on a sound understanding of the threats and vulnerabilities. Where a country is seeking to introduce a risk-based approach at a national level, this will be greatly aided if there is a national understanding of the risks facing the country. This understanding can flow from a national risk assessment that can assist in identifying the risks.

56. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of designated competent authorities or SROs and the nature of DNFBPs, including legal professionals, each country's judgements about the risks will be unique, as will their decisions about how to implement a national assessment in practice. A national assessment need not be a single formal process or document. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and current understanding of the risks. Designated competent authorities and SROs, in consultation with the private sector, should consider how best to achieve this while also taking into account any jurisdictional limitations of applying the risk-based approach to legal professionals, as well as any risk associated with providing information on money laundering and terrorist vulnerabilities.

Principle Two: A legal/regulatory framework that supports the application of a risk-based approach

57. Countries should consider whether their legislative and regulatory frameworks are conducive to the application of the risk-based approach. Where appropriate the obligations imposed should be informed by the outcomes of the national risk assessment.

58. The risk-based approach does not mean the absence of a clear statement of what is required from the DNFBPs, including from legal professionals. However, under a risk-based approach, legal professionals should have a degree of flexibility to implement policies and procedures which respond appropriately to their own risk assessment. In effect, the standards implemented may be tailored

and/or amended by additional measures as appropriate to the risks of an individual legal professional and/or practice. The fact that policies and procedures, in accordance to the risk levels, may be applied to different services, clients and locations does not mean that policies and procedures need not be clearly defined.

59. Basic minimum AML/CFT requirements can co-exist with a risk-based approach. Indeed, sensible minimum standards, coupled with scope for these to be enhanced when the risk justifies it, should be at the core of risk-based AML/CFT requirements. These standards should, however, be focused on the outcome (combating through deterrence, detection, and, when there is a requirement in a particular country, reporting of money laundering and terrorist financing), rather than applying legal and regulatory requirements in a purely mechanistic manner to every client. SROs may assist in the development of such standards for legal professionals.

Principle Three: Design of a monitoring framework to support the application of the risk-based approach

60. In certain countries, SROs play a critical role in the regulation of legal professionals, which may be based on fundamental constitutional principles. Some SROs have the ability to audit or investigate their own members, although in some countries these powers may be limited to reviewing policies and procedures as opposed to specific clients and matters. Depending on the powers of and responsibilities accepted by SROs, SROs may be able to facilitate or ensure compliance by legal professionals with the relevant legislation and/or develop guidance relating to money laundering. In some countries, the SROs may provide a greater level of scrutiny than that which can be afforded by a government or regulatory AML program. SROs should be encouraged to work closely with domestic AML/CFT regulators. Countries should ensure that SROs have appropriate resources to discharge their AML/CFT responsibilities. In some cases, legal professionals may conduct activities falling within the scope of Recommendation 12 that under national law may also require supervision from appropriate authorities.

61. Where appropriate, designated competent authorities and SROs should seek to adopt a risk-based approach to the monitoring of controls to combat money laundering and terrorist financing. This should be based on a thorough and comprehensive understanding of the types of activity carried out by legal professionals, and the money laundering and terrorist financing risks to which these are exposed. Designated competent authorities and SROs will probably need to prioritise resources based on their overall assessment of where the risks are in the legal professionals' practices.

62. Designated competent authorities and SROs with responsibilities other than those related to AML/CFT will need to consider these risks alongside other risk assessments arising from the designated competent authority's or SRO's wider duties.

63. Such risk assessments should help the designated competent authority or SRO choose where to apply resources in its monitoring programme, with a view to using limited resources to achieve the greatest effect. A risk assessment may also indicate that the designated competent authority or SRO does not have adequate resources to deal with the risks. In such circumstances, the designated competent authority or SRO may need to obtain, where possible, additional resources or adopt other strategies to manage or mitigate any unacceptable residual risks.

64. The application of a risk-based approach to monitoring requires that designated competent authorities' and SROs' staff be able to make principle-based decisions in a fashion similar to what would be expected from the staff of a legal professional's practice. These decisions will cover the adequacy of the arrangements to combat money laundering and terrorist financing. As such, a designated competent authority or SRO may wish to consider how best to train its staff in the practical application of a risk-based approach to monitoring. This staff will need to be well-briefed as to the general principles of a risk-based approach, the possible methods of application, and what a risk-based approach looks like when successfully applied within the context of a national risk assessment.

Principle Four: Identifying the main actors and ensuring consistency

65. Countries should consider who the main stakeholders are when adopting a risk-based approach to combating money laundering and terrorist financing. These will differ from country to country. Thought should be given as to the most effective way to share responsibility between these parties, and how information may be shared to best effect. For example, consideration may be given to which body or bodies are best placed to provide guidance to legal professionals about how to implement a risk-based approach to AML/CFT.

66. A list of potential stakeholders may include the following:

- Government – This may include legislature, executive, and judiciary.
- Law enforcement agencies – This might include the police, customs and similar agencies.
- The financial intelligence unit (FIU), security services, and other similar agencies.
- Designated competent authorities/SROs (particularly bar associations and law societies).
- The private sector – This might include legal professionals and law firms and legal professional organisations and associations such as national, state, local, and specialty professional societies and bar associations.
- The public – Arrangements designed to counter money laundering and terrorist financing are ultimately designed to protect the law-abiding public. However, these arrangements may also act to place burdens on clients of legal professionals.
- Others – Those who are in a position to contribute to the conceptual basis underpinning the risk-based approach, such stakeholders may include academia and the media.

67. Clearly a government will be able to exert influence more effectively over some of these stakeholders than others. However, regardless of its capacity to influence, a government will be in a position to assess how all stakeholders can be encouraged to support efforts to combat money laundering and terrorist financing.

68. A further element is the role that governments have in seeking to gain recognition of the relevance of a risk-based approach from designated competent authorities. This may be assisted by relevant authorities making clear and consistent statements on the following issues:

- Legal professionals can be expected to have the flexibility to adjust their internal systems and controls taking into consideration lower and high risks, so long as such systems and controls are reasonable. However, there are also minimum legal and regulatory requirements and elements that apply irrespective of the risk level, such as minimum standards of CDD.
- Acknowledging that a legal professional's ability to detect and deter money laundering and terrorist financing may sometimes be necessarily limited and that information on risk factors is not always robust or freely available. There can therefore be reasonable policy and monitoring expectations about what a legal professional with good controls aimed at preventing money laundering and the financing of terrorism is able to achieve. A legal professional may have acted in good faith to take reasonable and considered steps to prevent money laundering, and documented the rationale for his/her decisions, and yet still be abused by a criminal.

- Acknowledging that not all high-risk situations are identical and as a result will not always require the application of precisely the same type of enhanced due diligence.

Principle Five: Information exchange between the public and private sector

69. Effective information exchange between the public and private sector will form an integral part of a country's strategy for combating money laundering and terrorist financing. In some cases, it will allow the private sector to provide designated competent authorities and SROs with information they identify as a result of previously provided government intelligence. In countries where SROs regulate and monitor legal professionals for AML compliance, such SROs may well acquire information that would be relevant to a country's strategy for combating money laundering and terrorist financing. To the extent that such information may be released in accordance with applicable laws, regulations, and rules, the results may be made available to the designated competent authorities.

70. Public authorities, whether law enforcement agencies, designated competent authorities or other bodies, have privileged access to information that may assist legal professionals to reach informed judgements when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, legal professionals are able to understand their clients' legal needs reasonably well. It is desirable that public and private bodies work collaboratively to identify what information is valuable to help combat money laundering and terrorist financing, and to develop means by which this information might be shared in a timely and effective manner.

71. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, designated competent authorities and law enforcement agencies should be able to share information and feedback on results and identified vulnerabilities, so that consistent and meaningful inputs can be provided to the private sector. All parties should of course, consider what safeguards are needed to adequately protect sensitive information held by public bodies from being disseminated in contravention of applicable laws and regulations.

72. Relevant stakeholders should seek to maintain a dialogue so that it is well understood what information has proved useful in combating money laundering and terrorist financing. For example, the types of information that might be usefully shared between the public and private sector would include, if available:

- Assessments of country risk.
- Typologies or assessments of how money launderers and terrorists have abused DNFBPs, especially legal professionals.
- Feedback on suspicious transaction reports and other relevant reports.
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards and a country's legal and regulatory framework, it may also be appropriate for authorities to share targeted confidential information with legal professionals.
- Countries, persons or organisations whose assets or transactions should be frozen.

73. When choosing what information can be properly and profitably shared, public authorities may wish to emphasise to legal professionals that information from public bodies should inform, but not be a substitute for legal professionals' own judgements. For example, countries may decide not to create what are perceived to be definitive country-approved lists of low risk client types. Instead,

public authorities may prefer to share information on the basis that this will be one input into legal professionals' decision making processes, along with any other relevant information that is available to legal professionals.

Chapter Two: Implementation of the Risk-Based Approach

Assessment of Risk to Inform National Priorities:

74. A risk-based approach should be built on sound foundations: effort must first be made to ensure that the risks are well understood. As such, a risk-based approach should be based on an assessment of the threats. This is true whenever a risk-based approach is applied, at any level, whether by countries or individual legal professionals and/or firms. A country's approach should be informed by its efforts to develop an understanding of the risks in that country. This can be considered as a "national risk assessment".

75. A national risk assessment should be regarded as a description of fundamental background information to assist designated competent authorities, law enforcement authorities, the FIU, financial institutions and DNFBPs to ensure that decisions about allocating responsibilities and resources at the national level are based on a practical, comprehensive and up-to-date understanding of the risks.

76. A national risk assessment should be tailored to the circumstances of the individual country, both in how it is executed, and its conclusions, though countries should be mindful that money laundering and terrorist financing can often have an international dimension, and that such information may also add value to the national risk assessment. Factors that may influence the risk of money laundering and terrorist financing in a country could include the following:

- Political environment.
- Legal environment.
- A country's economic structure.
- Cultural factors, and the nature of civil society.
- Sources, location and concentration of criminal activity.
- Size and composition of the financial services industry.
- Ownership structure of financial institutions and DNFBPs businesses.
- Size and nature of the activity carried out by DNFBPs, including legal professionals.
- Corporate governance arrangements in relation to financial institutions and DNFBPs and the wider economy.
- The nature of payment systems and the prevalence of cash-based transactions.
- Geographical spread of the financial industry's and DNFBPs' operations and clients.
- Types of products and services offered by the financial services industry and DNFBPs.
- Types of customers/clients serviced by financial institutions and DNFBPs.
- Types of predicate offences.

- Amounts of illicit money generated domestically.
- Amounts of illicit money generated abroad and laundered domestically.
- Main channels or instruments used for laundering or financing terrorism.
- Sectors of the legal economy affected.
- Underground/informal areas in the economy.

77. Countries should also consider how an understanding of the risks of money laundering and terrorist financing can be best achieved at the national level. Relevant questions could include: Which body or bodies will be responsible for contributing to this assessment? How formal should an assessment be? Should the designated competent authority's or SRO's view be made public? These are all questions for the designated competent authority or SRO to consider.

78. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and up-to-date understanding of the risks. To achieve the desired outcome, designated competent authorities and SROs should ensure that they identify and provide DNFBPs (including legal professionals) with the information needed to develop this understanding and to design and implement measures to mitigate the identified risks.

79. Developing and operating a risk-based approach involves forming judgements. It is important that these judgements are well informed. It follows that, to be effective, the risk-based approach should be information-based and include intelligence where appropriate. Effort should be made to ensure that risk assessments are based on fresh and accurate information. Governments utilising partnerships with law enforcement bodies, FIUs, designated competent authorities/SROs and legal professionals themselves, are well placed to bring their knowledge and expertise to bear in developing a risk-based approach that is appropriate for their particular country. Their assessments will not be static and will change over time, depending on how circumstances develop and how the threats evolve. As such, countries should facilitate the flow of information between different bodies, so that there are no institutional impediments to information dissemination.

80. Whatever form they take, a national assessment of the risks, along with measures to mitigate those risks, can inform how resources are applied to combat money laundering and terrorist financing, taking into account other relevant country policy goals. It can also inform how these resources are most effectively assigned to different public bodies and SROs, and how those bodies make use of those resources in an effective manner.

81. As well as assisting designated competent authorities and SROs to decide how to allocate funds to combat money laundering and terrorist financing, a national risk assessment can also inform decision-makers on the best strategies for implementing a regulatory regime to address the risks identified. An over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on legal professionals. Alternatively, less aggressive efforts may not be sufficient to protect society from the threats posed by criminals and terrorists. A sound understanding of the risks at the national level could help obviate these dangers.

Effective systems for monitoring and ensuring compliance with AML/CFT requirements – General Principles

82. FATF Recommendation 24 requires that legal professionals should be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether there is an effective system, regard may be had to the risk of money laundering or terrorist financing in the sector. There should be a designated competent authority or SRO responsible for

monitoring and ensuring compliance by legal professionals; and the authority or SRO should have adequate powers and resources to perform its functions, including powers to monitor and sanction.

Defining the acceptable level of risk

83. The level of AML/CFT risk will generally be affected by both internal and external risk factors. For example, risk levels may be increased by internal risk factors such as weak compliance resources, inadequate risk controls and insufficient senior management involvement. External level risks may rise due to factors such as the action of third parties and/or political and public developments.

84. As described in Section One, all activity involves an element of risk. Designated competent authorities and SROs should not prohibit legal professionals from conducting business with high risk clients. However, legal professionals would be prudent to identify, with assistance from this or other Guidance, the risks associated with acting for high risk clients. When applicable law prohibits legal professionals from acting for a client, the risk-based approach does not apply.

85. However, this does not exclude the need to implement basic minimum requirements. For instance, FATF Recommendation 5 (that applies to legal professionals through the incorporation of R.5 into R.12) states that “where [the legal professional] is unable to comply with [CDD requirements], it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transaction report in relation to the customer.” So the level of risk should strike an appropriate balance between the extremes of not accepting clients, and conducting business with unacceptable or unmitigated risk. As is recognised by the interpretative note to FATF Recommendation 16, however, in those countries where a reporting requirement has been adopted the matters that would fall under legal professional privilege or professional secrecy are determined by each country.³

86. Where legal professionals implement a risk-based approach, designated competent authorities and SROs must expect legal professionals to put in place effective policies, programmes, procedures and systems to mitigate the risk and acknowledge that even with effective systems not every suspect transaction will necessarily be detected. They should also ensure that those policies, programmes, procedures and systems are applied effectively to prevent legal professionals from becoming conduits for illegal proceeds and ensure that they keep records and make reports (where obligated) that are of use to national authorities in combating money laundering and terrorist financing. Efficient policies and procedures will reduce the level of risks, but are unlikely to eliminate them completely. Assessing money laundering and terrorist financing risks requires judgement and is not an exact science. Monitoring aims at detecting unusual or suspicious transactions among an extremely large number of legitimate transactions; furthermore, the demarcation of what is unusual may not always be straightforward since what is “customary” may vary depending on the clients’ business. This is why developing an accurate client profile is important in managing a risk-based system. Moreover, although procedures and controls are frequently based on previous typologies, criminals will adapt their techniques, which may quickly limit the utility of such typologies.

87. Additionally, not all high risk situations are identical, and therefore will not always require precisely the same level of enhanced due diligence. As a result, designated competent authorities/SROs will expect legal professionals to identify individual high risk categories and apply specific and appropriate mitigation measures. Further information on the identification of specific risk categories is provided in Section Three, “Guidance for Legal Professionals on Implementing a Risk-Based Approach.”

³ See Annex 1 for a summary of decisions by judicial authorities on these issues.

Proportionate Supervisory/Monitoring Actions to support the Risk-Based Approach

88. Designated competent authorities and SROs should seek to identify weaknesses through an effective programme of both on-site and off-site supervision, and through analysis of internal and other available information.

89. In the course of their examinations, designated competent authorities and SROs should review a legal professional's AML/CFT risk assessments, as well as its policies, procedures and control systems to arrive at an overall assessment of the risk profile of legal professionals' practices and the adequacy of their mitigation measures. Where available, assessments carried out by or for legal professionals may be a useful source of information. The designated competent authority/SRO assessment of management's ability and willingness to take necessary corrective action is also a critical determining factor. Designated competent authorities and SROs should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe response.

90. Nevertheless, it may happen that the lack of detection of an isolated high risk transaction, or of transactions of an isolated high risk client, will in itself be significant, for instance where the amounts are significant, or where the money laundering and terrorist financing typology is well known, or where a scheme has remained undetected for a long time. Such a case might indicate an accumulation of weak risk management practices or regulatory breaches regarding the identification of high risks, monitoring, staff training and internal controls, and therefore, might alone justify action to ensure compliance with the AML/CFT requirements.

91. Designated competent authorities and SROs can and should use their knowledge of the risks associated with services, clients and geographic locations to help them evaluate legal professionals' money laundering and terrorist financing risk assessments, with the understanding, however, that they may possess information that has not been made available to legal professionals and, therefore, legal professionals would not have been able to take such information into account when developing and implementing a risk-based approach. Designated competent authorities and SROs (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist legal professionals in managing their risks. Where legal professionals are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by their designated competent authorities and SROs⁴. Guidance specifically designed for legal professionals is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where legal professionals use excessively narrow risk categories that do not capture all existing risks, or adopt criteria that lead to the identification of a large number of higher risk relationships, but without providing for adequate additional CDD measures.

92. In the context of the risk-based approach, the primary focus for designated competent authorities and SROs should be to determine whether or not the legal professional's AML/CFT compliance and risk management programme is adequate to: (a) meet the minimum regulatory requirements, and (b) appropriately and effectively mitigate the risks. The monitoring goal is not to prohibit high risk activity, but rather to be confident that legal professionals have adequately and effectively implemented appropriate risk mitigation strategies. Appropriate authorities should, when considering taking action (including applying penalties and sanctions), take into account and give due consideration to the reasoned judgements of legal professionals who are implementing and/or operating an appropriate risk-based approach, which judgements, in hindsight, may ultimately be determined to have been incorrect. In some countries and situations, judicial authorities alone will determine whether the legal professional has complied with the obligation to exercise reasonable judgement.

⁴ FATF Recommendations 5 and 25, Methodology Essential Criteria 25.1 and 5.12.

93. Under FATF Recommendation 24, designated competent authorities and SROs should have adequate powers to perform their monitoring functions, including the power to impose adequate sanctions for failure to comply with statutory and regulatory requirements to combat money laundering and terrorist financing. Fines and/or penalties are not appropriate in all regulatory actions, nor will they be permissible in all jurisdictions, to correct or remedy AML/CFT deficiencies. However, subject to the requirements of this paragraph, competent authorities, judicial authorities and SROs must have the authority and willingness to apply appropriate sanctions in cases where substantial deficiencies exist. Often, action will take the form of a remedial programme through the normal monitoring processes.

94. In considering the above factors it is clear that proportionate monitoring will be supported by two central features:

a) Regulatory Transparency

95. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Designated competent authorities and SROs are aware that legal professionals, while looking for professional freedom to make their own risk judgements, will also seek guidance on regulatory obligations. As such, the designated competent authority/SRO with AML/CFT supervisory/monitoring responsibilities should seek to be transparent in setting out what it expects, and will need to consider appropriate mechanisms of communicating these messages. For instance, this may be in the form of high-level requirements, based on desired outcomes, rather than detailed processes. If SROs responsible for the regulation of the relevant legal professionals (including regulation of AML risks) carry out regular AML compliance reviews of their members or otherwise take measures to supervise compliance, the form of an SRO monitoring programme should be determined by each SRO's rules and regulations.

96. No matter what individual procedure is adopted, the guiding principle will be that there is an awareness of legal responsibilities and regulatory expectations. In the absence of this transparency there is the danger that monitoring actions may be perceived as either disproportionate or unpredictable, which may undermine even the most effective application of the risk-based approach by legal professionals.

b) General Education, Staff Training of Designated Competent Authorities, SROs, and Enforcement Staff

97. SROs or other bodies that have a supervisory or educational role for legal professionals and legal professional organisations all have a stake in an effective risk-based system. This includes making available to legal professionals educational materials, further guidance and increasing awareness of money laundering concerns and risks. Central to the ability of legal professionals to seek to train and guard against money laundering effectively in a risk-based approach, is the provision of realistic typologies, particularly those where there is unwitting involvement.

98. In the context of the risk-based approach, it is not possible to specify precisely what a legal professional has to do, in all cases, to meet its regulatory obligations. Thus, a prevailing consideration will be how best to ensure the consistent implementation of predictable and proportionate monitoring actions. The effectiveness of monitoring training will therefore be important to the successful delivery of proportionate supervisory/monitoring actions.

99. Training should aim to allow designated competent authorities/SRO staff to form sound comparative judgements about AML/CFT systems and controls. It is important in conducting assessments that designated competent authorities and SROs have the ability to make judgements regarding management controls in light of the risks assumed by firms and considering available industry practices. Designated competent authorities and SROs might also find it useful to undertake

comparative assessments so as to form judgements as to the relative strengths and weaknesses of different legal professional organisations' arrangements.

100. The training should include instructing designated competent authorities and SROs about how to evaluate whether senior management has implemented adequate risk management measures, and determine if the necessary procedures and controls are in place. The training should also include reference to specific guidance, where available. Designated competent authorities and SROs also should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

101. To fulfil these responsibilities, training should enable designated competent authorities and SROs monitoring staff to adequately assess:

- i. The quality of internal procedures, including ongoing employee training programmes and internal audit, compliance and risk management functions.
- ii. Whether or not the risk management policies and processes are appropriate in light of legal professionals' risk profile, and are periodically adjusted in light of changing risk profiles.
- iii. The participation of senior management to confirm that they have undertaken adequate risk management, and that the necessary procedures and controls are in place.

102. Educating legal professionals on AML/CFT issues and the risk-based approach is a key element of an effective risk-based approach. Designated competent authorities should thus consider, in discussion with SROs and legal professionals and other appropriate organisations, ways of encouraging educational bodies (such as universities and law schools) to include within the education and training of legal professionals at all levels appropriate references to AML/CFT laws and the appropriate role that legal professionals can play in combating money laundering and terrorist financing.

SECTION THREE: GUIDANCE FOR LEGAL PROFESSIONALS ON IMPLEMENTING A RISK-BASED APPROACH

Chapter One: Risk Categories

103. Potential money laundering and terrorist financing risks faced by legal professionals will vary according to many factors including the activities undertaken by the legal professional, the type and identity of client, and the nature of the client relationship and its origin. Legal professionals should identify the criteria that enable them to best assess the potential money laundering and where feasible terrorist financing risks their practices give rise to and should then implement a reasonable risk based approach based on those criteria. These criteria are not exhaustive and are not intended to be prescriptive, and should be applied in a manner that is well-considered, is appropriate to the particular circumstances of the country and takes into account the way in which legal professionals are regulated in that country and the obligations they are required to observe.

104. Identification of the money laundering risks and terrorist financing risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate these risks. Although a risk assessment should normally be performed at the inception of a client relationship, for a legal professional, the ongoing nature of the advice and services the legal professional often provides means that automated transaction monitoring systems of the type used by financial institutions will be inappropriate for many legal professionals. The individual legal professionals working with the client are better positioned to identify and detect changes in the type of work or the nature of the client's activities, this is because the lawyer's knowledge of the client and its business will develop throughout the duration of what is expected to be a longer term relationship. Legal professionals will need to pay attention to the nature of the risks presented by isolated, small and short-term client relationships that, depending upon the circumstances, may be low risk (*e.g.* advice provided to walk-ups in a legal aid clinic).

105. The amount and degree of monitoring will depend on the nature and frequency of the relationship. A legal professional may also have to adjust his or her risk assessment of a particular client based upon information received from a designated competent authority, SRO, or other credible sources.

106. Money laundering and terrorist financing risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling legal professionals, where required, to subject each client to reasonable and proportionate risk assessment. The most commonly used risk criteria are: country or geographic risk; client risk; and risk associated with the particular service offered. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering or terrorist financing may vary from one legal professional and/or firm to another, particularly given the size, sophistication, nature and scope of services offered by the legal professional and/or firm. These criteria, however, should not be considered in isolation. Legal professionals, in light of their individual practices and based on their reasonable judgements, will need to assess independently the weight to be given to each risk factor.

107. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is merely intended to provide a suggested framework for approaching the management of potential risks.

Country/Geographic Risk

108. There is no universally agreed definition by either designated competent authorities, SROs, or legal professionals that prescribes whether a particular country or geographic area (including the country within which the legal professional practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Money laundering and terrorist financing risks have the potential to arise from almost any source, such as the domicile of the client, the location of the transaction and the source of the funding. Countries that pose a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but that may not be universally recognised, may be taken into account by a legal professional because of the standing of the issuer of the sanctions and the nature of the measures.
- Countries identified by credible sources⁵ as generally lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as being a location from which funds or support are provided to terrorist organizations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.

Client Risk

109. Determining the potential money laundering or terrorist financing risks posed by a client, or category of clients, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a legal professional should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of clients whose activities may indicate a higher risk include:

- PEPs are considered as higher risk clients – If a legal professional is advising a client that is a PEP, or where a PEP is the beneficial owner of the client, with respect to the activities specified in Recommendation 12, then a legal professional will need to carry out appropriate enhanced CDD, as required by Recommendation 6. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's home country, the type of work the PEP is instructing the legal professional to perform or carry out, and the scrutiny to which the PEP is under in the PEP's home country.

⁵ “Credible sources” refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

- If a PEP is otherwise involved in a client (other than in the circumstances of Recommendation 6), then the nature of the risk should be considered in light of all relevant circumstances, such as:
 - The nature of the relationship between the client and the PEP. Even if the PEP does not have a controlling interest or a dominant position on the board or in management and therefore does not qualify as a beneficial owner, the PEP may nonetheless affect the risk assessment.
 - The nature of the client (*e.g.* is it a public listed company).
 - The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company and the client is purchasing real property for adequate consideration.
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated in all the circumstances of the representation).
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely fashion the true beneficial owner or controlling interests, such as the unexplained use of legal persons or legal arrangements, nominee shares or bearer shares.
- Clients that are cash (and cash equivalent) intensive businesses including:
 - Money services businesses (*e.g.* remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities).
 - Casinos, betting and other gambling related activities.
 - Businesses that while not normally cash intensive, generate substantial amounts of cash.
- Where clients that are cash intensive businesses are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations this may mitigate the risks.
- Charities and other “not for profit” organisations (NPOs) that are not subject to monitoring or supervision (especially those operating on a “cross-border” basis) by designated competent authorities⁶ or SROs.
- Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SROs.
- Clients having convictions for proceeds generating crimes who instruct the legal professional (who has actual knowledge of such convictions) to undertake specified activities on their behalf.
- Clients who have no address, or multiple addresses without legitimate reasons.
- Clients who change their settlement or execution instructions without appropriate explanation.

⁶ See Special Recommendation VIII.

- The use of legal persons and arrangements without any apparent legal or legitimate tax, business, economic or other reason.

Service Risk

110. An overall risk assessment should also include determining the potential risks presented by the services offered by a legal professional, noting that the various legal professionals provide a broad and diverse range of services. The context of the services being offered or delivered is always fundamental to a risk-based approach. Any one of the factors discussed in this Guidance alone may not itself constitute a high risk circumstance. High risk circumstances can be determined only by the careful evaluation of a range of factors that cumulatively and after taking into account any mitigating circumstances would warrant increased risk assessment. When determining the risks associated with provision of services related to specified activities, consideration should be given to such factors as:

- Services where legal professionals, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they actually control in the act of closing a business transaction.
- Services to conceal improperly beneficial ownership from competent authorities.
- Services requested by the client for which the legal professional does not have expertise excepting where the legal professional is referring the request to an appropriately trained professional for advice.
- Transfer of real estate between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.⁷
- 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.
- Transactions where it is readily apparent to the legal professional that there is inadequate consideration, such as when the client does not identify legitimate reasons for the amount of the consideration.
- Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes.
- Clients who offer to pay extraordinary fees for services which would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where a legal professional may receive a significant premium for a successful representation, should not be considered a risk factor.
- The source of funds and the source of wealth – The source of funds is the activity that generates the funds for a client, while the source of wealth describes the activities that have generated the total net worth of a client.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a client that would otherwise appear to be higher risk might allow for a legal professional to treat the client as lower risk.

⁷ See the FATF Typologies report *Money Laundering and Terrorist Financing through the Real Estate Sector* at <http://www.fatf-gafi.org/dataoecd/45/31/40705101.pdf>.

- Shell companies, companies with ownership through nominee shareholding and control through nominee and corporate directors⁸.
- Situations where it is difficult to identify the beneficiaries of trusts; this might include a discretionary trust that gives the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust, and when a trust is set up for the purpose of managing shares in a company that can make it more difficult to determine the beneficiaries of assets managed by the trust⁹;
- Services that deliberately have provided or purposely depend upon more anonymity in the client identity or participants than is normal under the circumstances and experience of the legal professional.
- Legal persons that, as a separate business, offer TCSP services should have regard to the TCSP Guidance, even if such legal persons are owned or operated by legal professionals. Legal professionals, however, who offer TCSP services should have regard to this Guidance, and should consider customer or service risks related to TCSPs such as the following:
 - Unexplained use of express trusts.
 - Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices.
 - In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
 - In the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and classes within an expression of wishes.

Variables that May Impact Risk

111. Due regard must be accorded to the vast and profound differences in practices, size, scale and expertise, amongst legal professionals. As a result, consideration must be given to these factors when creating a reasonable risk-based approach and the resources that can be reasonably allocated to implement and manage it. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a risk-based approach proportionate to the scope and nature of the practitioner's practice.

112. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular legal professional. This factor must always be considered in the context of the legal professional's practice. A legal professional's risk-based approach methodology may thus take into account risk variables specific to a particular client or type of work. Consistent with the risk-based approach and the concept of proportionality, the presence of one or more of these variables may cause a legal professional to conclude that either enhanced due diligence and monitoring is warranted, or conversely that normal CDD and monitoring can be reduced, modified or simplified. These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

⁸ See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" published 13 October 2006.

⁹ See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" Annex 2 on trusts, for a more detailed description of "potential for misuse" of trusts.

- The nature of the client relationship and the client's need for the legal professional to provide specified activities.
- The level of regulation or other oversight or governance regime to which a client is subject. For example, a client that is a financial institution or legal professional regulated in a country with a satisfactory AML/CFT regime poses less risk of money laundering than a client in an industry that has money laundering risks and yet is unregulated for money laundering purposes.
- The reputation and publicly available information about a client. Legal persons that are transparent and well known in the public domain and have operated for a number of years without being convicted of proceeds generating crimes may have low susceptibility to money laundering.
- The regularity or duration of the relationship.
- The familiarity of the legal professional with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a legal professional's own activities within the country.
- The proportionality between the magnitude or volume and longevity of the client's business and its legal requirements, including the nature of professional services sought.
- Subject to other factors (including the nature of the services and the source and nature of the client relationship), providing limited legal services in the capacity of a local or special counsel may be considered a low risk factor. This may also, in any event, mean that the legal professional is not "preparing for" or "carrying out" a transaction for a regulated activity specified in Recommendation 12.
- Significant and unexplained geographic distance between the legal professional organisation and the location of the client where there is no nexus to the type of work being undertaken.
- Where a prospective client has instructed the legal professional to undertake a single transaction-based service (as opposed to an ongoing advisory relationship) and one or more other risk factors are present.
- Risks that may arise from the use of new or developing technologies that permit non-face to face relationships and could favour anonymity. However, due to the prevalence of electronic communication between legal professionals and clients in the delivery of legal services, non-face to face interaction between legal professionals and clients should not, standing alone, be considered a high risk factor. For example, non-face to face, cross-border work for an existing client is not necessarily high risk work for certain organisations (such as regional, national or international law firms or other firms regardless of size that practice in that type of work) nor would customary services rendered by a sole practitioner on a local basis to a client in the local community who does not otherwise present increased risks.
- The nature of the referral or origination of the client. A prospective client may contact a legal professional in an unsolicited manner or without common or customary methods of introduction or referrals, which may increase risk. By contrast, where a prospective client has been referred from another trusted source subject to an AML/CFT regime that is in line with the FATF standards, the referral may be considered a mitigating risk factor.
- The structure of a client or transaction. Structures with no apparent legal, tax, business, economic or other legitimate reason may increase risk. Legal professionals often design

structures (even if complex) for legitimate legal, tax, business, economic or other legitimate reasons, in which case the risk of money laundering could be reduced.

- Trusts that are pensions may be considered lower risk.

Controls for Higher Risk Situations

113. Legal professionals should implement appropriate measures and controls to mitigate the potential money laundering and terrorist financing risks with respect to those clients that, as the result of the legal professional or firm risk-based approach, are determined to be higher risk. Paramount among these measures is the requirement to train legal professionals and appropriate staff to identify and detect changes in activity by reference to risk-based criteria. These measures and controls may include:

- General training on money laundering methods and risks relevant to legal professionals.
- Targeted training for increased awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work.
- Increased levels of CDD or enhanced due diligence for higher risk situations.
- Escalation or additional review and/or consultation by the legal professional or within a firm at the establishment of a relationship.
- Periodic review of the services offered by the legal professional and/or firm to determine whether the risk of money laundering and terrorist financing occurring has increased.
- Reviewing client relationships from time to time to determine whether the risk of money laundering and terrorist financing occurring has increased.
- The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that a legal professional establish specific controls targeting each risk criterion.

Chapter Two: Application of a Risk-Based Approach

Customer Due Diligence/Know Your Customer

114. Client Due Diligence/Know Your Client is intended to enable a legal professional to form a reasonable belief that it has appropriate awareness of the true identity of each client. The legal professional's procedures should apply in circumstances where a legal and professional is preparing for or carrying out¹⁰ the activities listed in Recommendation 12 and include procedures to:

- a) Identify and appropriately verify the identity of each client on a timely basis.
- b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner such that the legal professional is reasonably satisfied that it knows who the beneficial owner is. The general rule is that clients should be subject to the full range of CDD measures, including the requirement to identify the beneficial owner in accordance with this paragraph. The purpose of identifying beneficial ownership is to ascertain those natural persons who exercise effective control over a client, whether by means of ownership, voting

¹⁰ See paragraphs 12-13 regarding when a legal professional would or would not be engaged in "preparing for" or "carrying out" transactions for clients, and hence the requirements of Recommendation 12 would apply.

rights or otherwise. Legal professionals should have regard to this purpose when identifying the beneficial owner. They may use a risk-based approach when determining the extent to which they are required to identify the beneficial owner, depending on the type of client, business relationship and transaction and other appropriate factors in accordance with Recommendation 5 and its Interpretative Note, § 9-12¹¹.

c) Obtain appropriate information to understand the client's circumstances and business depending on the nature, scope and timing of the services to be provided. This information may be obtained from clients during the normal course of their instructions to legal professionals.

115. The starting point is for a legal professional to assess the risks that the client may pose taking into consideration any appropriate risk variables (and any mitigating factors) before making a final determination. The legal professional's assessment of risk will then inform the overall approach to CDD requirements and appropriate verification. Legal professionals will reasonably determine the CDD requirements appropriate to each client given the legal professional's familiarity with the client, which may include:

- A standard level of CDD, generally to be applied to all clients.
- The standard level being reduced after consideration of appropriate risk variables, and in recognised lower risk scenarios, such as:
 - Publicly listed companies (and their majority owned subsidiaries).
 - Financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.
 - Government authorities and state run enterprises (other than those from sanctioned countries).
- An increased level of CDD in respect of those clients that are reasonably determined by the legal professional to be of higher risk. This may be the result of the client's business activity, ownership structure, particular service offered including work involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as the risks outlined in paragraphs 108-109.

Monitoring of Clients and Specified Activities

116. The degree and nature of monitoring by a legal professional will depend on the type of legal professional, and if it is a firm, the size and geographic 'footprint' of the firm, the AML/CFT risks that the firm has identified and the nature of the regulated activity provided. Given the nature of the advisory relationship legal professionals have with their clients and that an element of that advisory relationship will usually involve frequent client contact, monitoring is typically best achieved by trained individuals having contact with the client (either face to face or by other means of communication). For purposes of paragraphs 116 to 118 (and related paragraphs), "monitoring" does not oblige the legal professional to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis his or her client. It rather refers to maintaining awareness throughout

¹¹ Legal professionals should have regard to the Interpretative Notes to Recommendation 5 and the AML/CFT 2004 Methodology Essential Criteria 5.5 and 5.8-5.12, which, among other things, provide more details on the measures that need to be taken to identify beneficial owners, and the impact of higher or lower risk on the required measures.

the course of work for a client to money laundering or terrorist financing activity and/or changing risk factors.

117. Monitoring of these advisory relationships cannot be achieved solely by reliance on automated systems and whether any such systems would be appropriate will depend in part on the nature of a legal professional's practice and resources reasonably available to the legal professional. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate monitoring systems and a risk-based approach proportionate to the scope and nature of the practitioner's practice. A legal professional's advisory relationships are best monitored by the individuals having direct client contact being appropriately trained to identify and detect changes in the risk profile of a client. Where appropriate this should be supported by systems, controls and records within a framework of support by the firm (*e.g.* tailored training programs appropriate to the level of staff responsibility).

118. Legal professionals should also assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs can fall within the system and control framework developed to manage the risk of the firm. The results of the monitoring may also be documented.

119. The civil law notary does not represent parties to a contract and therefore must maintain a fair position with regard to any duty to both parties.

Suspicious Transaction Reporting

120. This Guidance does not address FATF Recommendations relating to suspicious transaction reporting (STR) and the proscription against "tipping off" those who are the subject of such reports. Different countries have undertaken different approaches to these Recommendations of the FATF. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of the suspicious activity under these circumstances is not applicable. STRs are not part of risk assessment, but rather reflect a response mechanism – typically to an SRO or government enforcement authority – once a suspicion of money laundering has been identified. For those reasons, this Guidance does not address those elements of the FATF Recommendations.

Education, Training and Awareness

121. Recommendation 15 requires that legal professionals provide their staff with AML/CFT training, and it is important that legal professional staff receive appropriate and proportional training with regard to money laundering. For legal professionals, and those in smaller firms in particular, such training may assist with monitoring obligations. A legal professional's commitment to having appropriate controls relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant legal professionals with at least general information on AML/CFT laws, regulations and internal policies. To satisfy a risk-based approach, particular attention should be given to risk factors or circumstances occurring in the legal professional's own practice. In addition, governments, SROs and other representative bodies for both common and civil law notaries and bar associations should work with educational institutions to see that both legal professionals, and students taking courses to train for or become legal professionals, are educated on money laundering and terrorist financing risks. For example, bar societies and associations should be encouraged to produce continuing legal education programs on AML/CFT and the risk-based approach.

122. Applying a risk-based approach to the various methods available for training, however, gives each legal professional flexibility regarding the frequency, delivery mechanisms and focus of such training. Legal professionals should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

- Tailored to the relevant staff responsibility (*e.g.* client contact or administration).

- At the appropriate level of detail (*e.g.* considering the nature of services provided by the legal professional).
- At a frequency suitable to the risk level of the type of work undertaken by the legal professional.
- Used to test to assess staff knowledge of the information provided.

Chapter Three: Internal Controls

123. Many DNFBPs differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of DNFBPs have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against money laundering and terrorist financing. For a number of DNFBPs, a single person may be responsible for the functions of front office, back office, money laundering reporting, and senior management. This particularity of DNFBPs, including legal professionals, should be taken into account in designing a risk-based framework for internal controls systems. The Interpretative Note to Recommendation 15, dealing with internal controls, specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size of the business.

124. To enable legal professionals to have effective risk-based approaches, the risk-based process must be a part of the internal controls of the legal professional or firm. Legal professionals operate within a wide range of differing business structures, from sole practitioners to large partnerships. These structures often mean that legal professionals' businesses have a flat management structure and that most or all of the principals (or partners) of the firm hold ultimate management responsibility. In other organisations, legal professionals employ corporate style organisational structures with tiered management responsibility. In both cases the principals or the managers are ultimately responsible for ensuring that the organisation maintains an effective internal control structure. Engagement by the principals and managers in AML/CFT is an important aspect of the application of the risk-based approach since such engagement reinforces a culture of compliance, ensuring that staff adheres to the legal professional's policies, procedures and processes designed to limit and control money laundering risks.

125. The nature and extent of the AML/CFT controls, as well as meeting national requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will depend upon a number of factors, such as:

- The nature, scale and complexity of a legal professional's business.
- The diversity of a legal professional's operations, including geographical diversity.
- The legal professional's client, service and activity profile.
- The degree of risk associated with each area of the legal professional's operations.
- The services being offered and the frequency of client contact (either in person or by other means of communication).

126. Subject to the size and scope of the legal professional's organisation, the framework of risk-based internal controls should:

- Have appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP.
- Provide increased focus on a legal professional's operations (*e.g.* services, clients and geographic locations) that are more vulnerable to abuse by money launderers.
- Provide for periodic review of the risk assessment and management processes, taking into account the environment within which the legal professional operates and the activity in its marketplace.
- Designate personnel at an appropriate level who are responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme if appropriate given the scale of the organisation and the nature of the legal professional's practice.
- Inform the principals of compliance initiatives, identified compliance deficiencies and corrective action taken.
- Provide for programme continuity despite changes in management or employee composition or structure.
- Focus on meeting all regulatory record keeping or other requirements, as well as promulgated measures for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based CDD policies, procedures and processes.
- Provide for adequate controls for higher risk clients and services as necessary, such as review with or approvals from others.
- Provide for adequate supervision and support for staff activity that forms part of the organisation's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of relevant personnel.
- Provide for appropriate training to be given to all relevant staff.
- For groups, to the extent possible, provide a common control framework.

ANNEXES

ANNEX 1

SOURCES OF FURTHER INFORMATION

Various sources of information exist that may help governments and legal professionals in their development of a risk-based approach. Although not an exhaustive list, this Annex 1 highlights a number of useful web-links that governments and legal professionals may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such as AML/CFT assessments.

A. Financial Action Task Force Documents

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. Key resources include the 40 Recommendations on Money Laundering and 9 Special Recommendations on Terrorist Financing, the Methodology for Assessing Compliance with the FATF Recommendations, the Handbook for Countries and Assessors, methods and trends (typologies) reports and mutual evaluation reports.

www.fatf-gafi.org

B. Legislation/and Court Decisions

The rulings by the ECJ of June 26th 2007 by the Belgium Constitution Court of January 23rd 2008 and the French Conseil d'État of April 10th, 2008 have confirmed that anti-money laundering regulation cannot require or permit the breach the lawyer's duty of professional secrecy when performing the essential activities of the profession. In addition, the Court of First Instance in the Joined Cases T-125/03 & T-253/03 Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission of the European Communities has recently restated the ruling in the *AM&S* case that professional secrecy "meets the need to ensure that every person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it (*AM&S*, paragraph 18). That principle is thus closely linked to the concept of the lawyer's role as collaborating in the administration of justice by the courts (*AM&S*, paragraph 24).

C. Links to Information on the Supervisory Program in Certain Countries

Switzerland

1. See articles 18 to 21 of the lawyers and notaries' SRO regulations (SRO SAV/SNV): www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf

2. See articles 38 and 45 to 47 of the lawyers and notaries' SRO statutes (SRO SAV/SNV): www.oad-fsa-fsn.ch/fr/02_beitritt/01_regelwerke.htm/01_Statuten.pdf

D. Guidance on the Risk-based Approach

1. Law Society of Ireland: www.lawsociety.ie.
2. Law Society of England and Wales: www.lawsociety.org.uk
3. Law Society of Hong Kong: www.hklawsoc.org.hk
4. Organisme d'autoréglementation de la fédération suisse des avocats et de la fédération suisse des notaires (SRO SAV/SNV): home page: www.sro-sav-snv.ch/
www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf (art. 41 to 46)
5. The Netherlands Bar Association: www.advocatenorde.nl
6. The Royal Dutch Notarial Society: www.notaris.nl

E. Other sources of information to help assist countries' and legal professionals' risk assessment of countries and cross-border activities

In determining the levels of risks associated with particular country or cross border activity, legal professionals and governments may draw on a range of publicly available information sources, these may include reports that detail observance of international standards and codes, specific risk ratings associated with illicit activity, corruption surveys and levels of international cooperation. Although not an exhaustive list the following are commonly utilised:

- IMF and World Bank Reports on observance of international standards and codes (Financial Sector Assessment Programme)
 - World Bank reports: www1.worldbank.org/finance/html/cntrynew2.html
 - International Monetary Fund: www.imf.org/external/np/rosc/rosc.asp?sort=topic#RR
 - Offshore Financial Centres (OFCs) IMF staff assessments www.imf.org/external/np/ofca/ofca.asp
- Mutual evaluation reports issued by FATF Style Regional Bodies:
 1. Asia/Pacific Group on Money Laundering (APG) www.apgml.org/documents/default.aspx?DocumentCategoryID=8
 2. Caribbean Financial Action Task Force (CFATF) www.cfatf.org/profiles/profiles.asp
 3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/5_money_laundering/Evaluations/Reports_summaries_3.asp#TopOfPage
 4. Eurasian Group (EAG)

www.eurasiangroup.org/index-7.htm

5. GAFISUD

www.gafisud.org/miembros.htm

6. Middle East and North Africa FATF (MENAFATF)

www.menafatf.org/TopicList.asp?cType=train

7. The Eastern and South African Anti Money Laundering Group (ESAAMLG)

www.esaamlg.org/

8. Groupe Inter-gouvernemental d'Action contre le Blanchiment d'Argent (GIABA)

www.giabasn.org/?lang=en&sid

- OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting)
www.oecd.org/document/49/0,2340,en_2649_34171_1901105_1_1_1_1,00.html
- International Narcotics Control Strategy Report (published annually by the US State Department)
www.state.gov/p/inl/rls/nrcrpt/
- Egmont Group membership - Coalition of financial intelligence units that participate in regular information exchange and the sharing of good practice, acceptance as a member of the Egmont Group is based a formal procedure that countries must go through in order to be acknowledged as meeting the Egmont definition of an FIU.
www.egmontgroup.org/
- Signatory to the United Nations Convention against Transnational Organized Crime
www.unodc.org/unodc/crime_cicp_signatures_convention.html
- The Office of Foreign Assets Control (“OFAC”) of the US Department of the Treasury economic and trade, Sanctions Programmes
www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml
- Consolidated list of persons, groups and entities subject to EU Financial Sanctions
http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm
- UN Security Council Sanctions Committee - Country Status:
www.un.org/sc/committees/

ANNEX 2

GLOSSARY OF TERMINOLOGY

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a client 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.

Competent authorities

Competent authorities refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

Designated Non-Financial Businesses and Professions (DNFBPs)

- a. Casinos (which also includes internet casinos).
- 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, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the 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.
 - Acting as (or arranging for another person to act as) a nominee shareholder for another person.

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 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).

FATF Recommendations

Refers to the FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing.

Legal Person

Legal person refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent client relationship with a legal professional or otherwise own property.

Legal Professional

In this Guidance, the term “*Legal professional*” refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Individuals who are or have been entrusted with prominent public functions in 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Self-regulatory organisation (SRO)

A body that represents a profession (*e.g.* lawyers, notaries, other independent legal professionals or accountants), and which is made up of member professionals or a majority thereof, has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

ANNEX 3

MEMBERS OF THE ELECTRONIC ADVISORY GROUP

FATF and FSRB members and observers

Argentina; Asia Pacific Group (APG); Australia; Belgium; Azerbaijan; Canada; Chinese Taipei, China; European Commission (EC); Nigeria; France; Hong Kong, China; Italy; Japan; Luxembourg; MONEYVAL; Netherlands; New Zealand; Offshore Group of Banking Supervisors (OGBS); Portugal; Romania; Spain; South Africa; Switzerland; United Kingdom; United States.

Dealers in precious metals and dealers in precious stones industries

Antwerp World Diamond Centre, International Precious Metals Institute, World Jewellery Confederation, Royal Canadian Mint, Jewellers Vigilance Committee, World Federation of Diamond Bourses, Canadian Jewellers Association.

Real estate industry

International Consortium of Real Estate Agents, National Association of Estate Agents (UK), the Association of Swedish Real Estate Agents.

Trust and company service providers industry

The Society of Trust and Estate Practitioners (STEP), the Law Debenture Trust Corporation.

Accountants

American Institute of Certified Public Accountants, Canadian Institute of Chartered Accountants, European Federation of Accountants, German Institute of Auditors, Hong Kong Institute of Public Accountants, Institute of Chartered Accountants of England & Wales.

Casino industry

European Casino Association (ECA), Gibraltar Regulatory Authority, Kyte Consultants (Malta), MGM Grand Hotel & Casino, Unibet, William Hill plc.

Lawyers and notaries

Allens Arther Robinson, American Bar Association (ABA), American College of Trust and Estate Council, Consejo General del Notariado (Spain), Council of the Notariats of the European Union, Council of Bars and Law Societies of Europe (CCBE), International Bar Association (IBA), Law Society of England & Wales, Law Society of Upper Canada.

A Lawyer's Guide to Detecting and Preventing Money Laundering

A collaborative publication of the
International Bar Association, the
American Bar Association and the Council
of Bars and Law Societies of Europe

October 2014

³⁴⁵
This Guide has been prepared by working groups of the International Bar Association (“IBA”) (led by Stephen Revell), the American Bar Association (“ABA”) (led by Kevin Shepherd) and the Council of Bars and Law Societies of Europe (“CCBE”) with the help of Dr S. Chandra Mohan (Associate Professor of Law) and Lynn Kan (Juris Doctor), Singapore Management University, School of Law.

Contents of the Guide

Executive Summary	2
I. Introduction and Background	3
II. Sources of the Legal Profession’s AML Responsibilities	11
III. Vulnerabilities of the Legal Profession to Money Laundering	23
IV. The Risk-Based Approach and Money Laundering Red Flags	27
V. Case Studies	39
VI. Glossary and Further Resources	48
Endnotes	52

Disclaimer:

This Guide has been prepared and published for informational and educational purposes only and should not be construed as legal advice. The laws and regulations discussed in this Guide are complex and subject to frequent change and the reader should review and understand the laws and regulations that are applicable to the reader (which may involve the laws and regulations of more than one country) and not rely solely on this Guide. The IBA, ABA and CCBE assume no responsibility for the accuracy or timeliness of any information provided herein, or for updating the information in this Guide. For further information on applicable laws and regulations a reader may visit the following website of the IBA which aims to give country by country information provided by correspondents in each country – <http://www.anti-moneylaundering.org/globalchart.aspx>. In addition, readers should carefully consider the legal and regulatory issues in their own countries by referring to their bar association or law society for country specific guidance on anti-money laundering issues.

Money laundering and terrorist financing represent serious threats to life and society and result in violence, fuel further criminal activity, and threaten the foundations of the rule of law (in its broadest sense). Given a lawyer's role in society and inherent professional and other obligations and standards, lawyers must at all times act with integrity, uphold the rule of law and be careful not to facilitate any criminal activity. This requires lawyers to be constantly aware of the threat of criminals seeking to misuse the legal profession in pursuit of money laundering and terrorist financing activities.

While bar associations around the world play a key role in educating the legal profession, the onus remains on individual lawyers and on law firms to ensure that they are aware of and comply with their anti-money laundering ("AML") obligations. These obligations stem primarily from two sources:

- (i) the essential ethics of the legal profession including an obligation not to support or facilitate criminal activity; and
- (ii) in many countries, specific laws and regulations that have been extended to lawyers and require, in a formal sense, lawyers to take specific actions. These typically include an obligation to conduct appropriate due diligence about clients with a view to identifying those that may be involved in money laundering and, in some jurisdictions, an obligation to inform the authorities if they suspect clients and/or the persons the client is dealing with may be involved in money laundering. This obligation to report is highly controversial and is seen by many to endanger the independence of the legal profession and to be incompatible with the lawyer-client relationship. However, in some countries lawyers can themselves be prosecuted for a failure to carry out appropriate due diligence and report suspicious transactions to the authorities. Although we may not agree with or support such an approach, it is important that lawyers in such countries are fully aware of these obligations and the actions they need to take.

All lawyers must be aware of and continuously educate themselves about the relevant legal and ethical obligations that apply to their home jurisdiction and other jurisdictions in which they practice, and the risks that are relevant to their practice area and their clients in those jurisdictions. This is particularly so as the money laundering and terrorist financing activities of criminals are rapidly and constantly evolving to become more sophisticated. Awareness, vigilance, recognising red flag indicators and caution are a lawyer's best tools in assessing situations that might give rise to concerns of money laundering and terrorist financing. Such situations may, in some countries, result in (i) the lawyer being found guilty of an offence of supporting money laundering, due to the failure to properly "check" clients or report suspicious transactions where it is required and (ii) the lawyer being subject to professional discipline.

This Guide is intended as a resource to be used by lawyers and law firms to highlight the ethical and professional concerns relating to AML and to help lawyers and law firms comply with their legal obligations in countries where they apply. Clearly, this Guide does not impose any obligations on a lawyer. In it you will find:

- (i) a summary of certain international and national sources of AML obligations (Part II);
- (ii) a discussion of the vulnerabilities of the legal profession to misuse by criminals in the context of money laundering (Part III);
- (iii) a discussion of the risk-based approach to detecting red flags, red flag indicators of money laundering activities and how to respond to them (Part IV); and
- (iv) case studies to illustrate how red flags may arise in the context of providing legal advice (Part V).

This Guide is not a 'manual' which will ensure that lawyers satisfy their AML obligations. Rather, it aims to provide professionals with practical guidance to develop their own risk-based approaches to AML compliance which are suited to their practices.

I. Introduction and Background

I. Introduction and Background

348

Money laundering (the conversion of proceeds from crime into legitimate currency or other assets) and terrorist financing (whether from the proceeds of crime or otherwise) are not new phenomena. Criminals have been concealing the illicit origins of money through money laundering for decades. However, the scale of such activity has grown significantly – a 2009 estimate of the extent of money laundering put it at a staggering 2.7% of the world’s gross domestic product (or US\$1.6 trillion).¹

Measures combatting money laundering and terrorist financing overlap to a large extent, as criminals engaging in either of these activities are looking to transfer money while concealing the origin and destination of the funds. Further special considerations, however, apply in the fight against terrorist financing. Although this Guide focuses on anti-money laundering (“AML”) compliance and does not purport to tackle comprehensively the issue of the legal profession’s role in the fight against terrorist financing, many of the practices this Guide discusses would also help a lawyer from being misused to facilitate terrorist financing.

Money laundering involves three distinct stages: the placement stage, the layering stage, and the integration stage. The placement stage is the stage at which funds from illegal activity, or funds intended to support illegal activity, are first introduced into the financial system. The layering stage involves further disguising and distancing the illicit funds from their illegal source through the use of a series of parties and/or transactions designed to conceal the source of the illicit funds. The integration phase of money laundering results in the illicit funds being considered “laundered” and integrated into the financial system so that the criminal may expend “clean” funds. These stages are illustrated in the following diagram:²

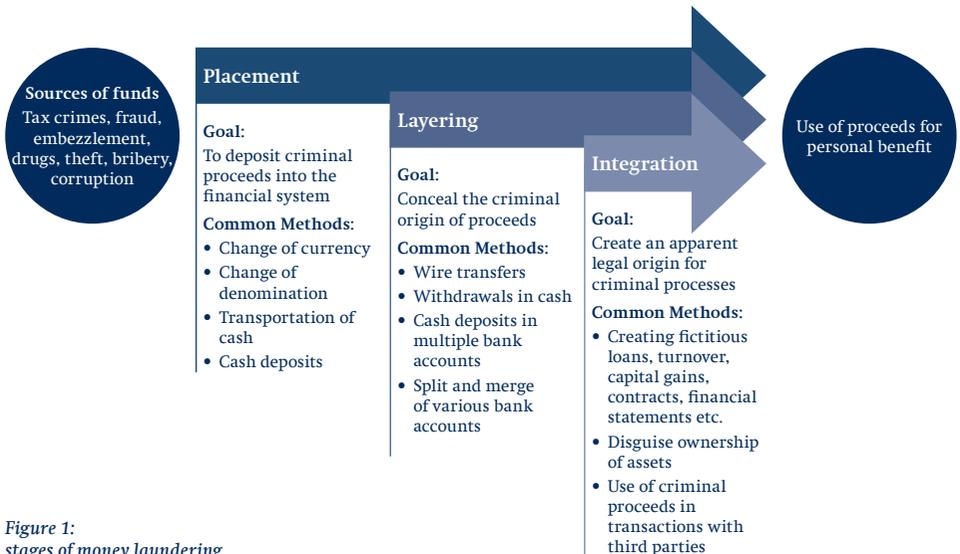


Figure 1: stages of money laundering

A. The 40 Recommendations

A diverse mix of domestic and international laws (both criminal and civil), regulations and standards has been developed to counter money laundering and terrorist financing. Most significant among these are the Recommendations of the Financial Action Task Force (“FATF”), an inter-governmental body established in 1989 at the G7 summit in Paris as a result of the growing concern over money laundering.³ The Recommendations are not international laws, but are a set of internationally endorsed global standards, which are based in part upon policies and recommendations stemming from United Nations (“UN”) conventions and Security Council resolutions. Further, the FATF Recommendations require that individual countries formulate and implement offences of money laundering and terrorist financing in accordance with the provisions set out in the Recommendations; FATF members and certain other countries have formally agreed to implement the Recommendations.⁴

The original Recommendations were drawn up in 1990 and were directed at the financial sector, as it was clear that banks were most at risk of being misused in connection with money laundering and terrorist financing. The Recommendations were first reviewed in 1996 and were supplemented with the Eight Special Recommendations on Terrorist Financing in 2001.⁵ A further revision in 2003 expanded the reach of the Recommendations to bodies that provide “access points” to financial systems, also referred to as “gatekeepers”. Broadly, these are persons, including lawyers⁶, FATF believes are in a position to identify and prevent illicit money flows through the financial system by monitoring the conduct of their clients and prospective clients and who could, if these persons are not vigilant, inadvertently facilitate money laundering and terrorist financing. The term used for “gatekeepers” in the 40 Recommendations is “Designated Non-Financial Businesses and Professions” (“DNFBP”).⁷ Extending the reach of the Recommendations to capture DNFBPs was motivated by FATF’s perception that “gatekeepers” were unwittingly assisting organised crime groups and other criminals to launder their funds by providing them with advice, or acting as their financial intermediaries.⁸ Unfortunately, when the Recommendations were extended to gatekeepers scant accommodation was made for the fact that many of the gatekeepers (including lawyers) have a fundamental role and provide different services as compared to the banks for which the Recommendations were originally drafted. As a result, FATF’s approach treats all gatekeepers in the same way as banks. Similarly, the extension was made without full recognition of the resources available to many gatekeepers, again particularly lawyers, as compared to the resources that are available to many banks.

The current version of the Recommendations, published in February 2012 and referred to in this Guide as the 40 Recommendations, embodies a focus on preventative measures, such as “customer due diligence” (“CDD”). This is done through the adoption of a risk-based approach, and the 40 Recommendations generally assume a somewhat different AML approach to the “hard law” approach embodied in both past international conventions and criminalisation of money laundering activities. Controversially, they include an obligation on gatekeepers, including lawyers, to report suspicious activity to the authorities.

The Recommendations set out a framework of measures, rather than direct obligations, that countries should implement to combat money laundering and terrorist financing. The 2003 revisions to the Recommendations are absolutely key from a lawyer's perspective. The 2003 revisions directed countries to bring into force laws or amendments to laws that put specific obligations on lawyers to take action in connection with money laundering and terrorist financing. Some in the legal profession view the Recommendations (and related national and regional legislation) as a source of another compliance burden on a profession that is already heavily regulated and, with regard to the obligation to report suspicious transactions, as a fundamental challenge to the lawyer-client relationship. Although lawyers and bar associations around the world (including the IBA, ABA and CCBE) deplore money laundering and terrorist financing and are keen to see lawyers play an appropriate role in the fight against these practices, many are concerned with the way in which AML obligations have been placed on the profession and the impact this has on lawyer-client relationships, a lawyer's independence and role in society and the rule of law. Notwithstanding these concerns, many jurisdictions have passed laws that formally impose obligations on lawyers and some have provided that breach of these obligations can expose lawyers to criminal prosecution. Lawyers must be aware of these laws and, where applicable, need to comply with them.

The basic intent behind the 40 Recommendations is consistent with what lawyers, as guardians of justice and the rule of law, and professionals subject to ethical obligations, have always done – namely to avoid assisting criminals or facilitating criminal activity. Some of the underlying ethical principles that the legal profession upholds, namely to avoid supporting criminal activity and being unwittingly involved in the pursuit of criminal activity, support the role that lawyers need to play in the fight against money laundering and terrorist financing. Notwithstanding these common ethical underpinnings, serious concerns remain about the obligation in the 40 Recommendations to report suspicious activity, particularly in jurisdictions where lawyers do not benefit from any relevant exceptions concerning the confidentiality created in a lawyer-client relationship. Importantly for lawyers, the Recommendations include a key interpretive note to Recommendation 23 that states that DFNBPs 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*”. However, even putting the 40 Recommendations to one side, it is at present an unanswered question in some jurisdictions as to what lawyers should ethically do if they become aware that their clients are misusing them for criminal purposes. For example, is it sufficient for the lawyers to stop acting or does this merely push the criminals to use the services of the lawyer next door (or in the next jurisdiction)?

FATF has published a typologies report⁹ to describe the vulnerabilities of the legal profession to money laundering and terrorist financing risks. FATF hoped this would assist lawyers in their interpretation of obligations imposed on them as a result of national or regional measures implementing the 40 Recommendations. Unfortunately, we do not believe this Report is as helpful as FATF intended, principally because it focuses heavily on situations in which lawyers are knowingly involved in money laundering and/or terrorist financing activities. As a result, the FATF report is in danger of creating a misleading impression of the legal profession. The profession generally believes that, contrary to what

the FATF typologies report may suggest, circumstances in which lawyers are knowingly involved in criminal activities are quite rare. As a matter of general principle, the legal profession does not want any exceptional or special treatment for lawyers who are knowingly involved in criminal activities – if so involved, such lawyers are also criminals and should be treated accordingly. We believe it is more productive to focus on situations where: (i) lawyers may become unknowingly and unintentionally involved in criminal activities and (ii) educating lawyers to be alert to misuse by criminals so that lawyers can play an active and informed role in the fight against money laundering and terrorist financing. Accordingly, this Guide focuses on situations where a criminal may seek to use the services of a lawyer who is not attuned to the risks and “red flag” indicators associated with such risks and aims to educate lawyers so that they can avoid their services from being used to facilitate money laundering or terrorist financing. Our intention is for the legal profession to continue to demonstrate leadership in this area and provide an important resource for lawyers across the globe seeking to guard against becoming unknowingly and unintentionally involved in money laundering and terrorist financing activities, regardless of the source of their AML obligations.

Before moving on to the substantive parts of this Guide, Section B below gives short descriptions of the efforts of bar associations across the globe to create other sources of guidance relating to AML obligations.¹⁰

B. Bar associations’ AML and counter terrorist financing efforts

Bar associations and law societies around the world, including the IBA, ABA and CCBE, have been actively supporting AML efforts by lawyers with policies and programmes to raise their members’ awareness of money laundering and terrorist financing issues and their members’ related obligations.

ABA	CCBE	IBA
<p>ABA comprises almost 400,000 members</p> <p>Operates the Task Force on Gatekeeper Regulation and the Profession that examines government and multilateral efforts to combat international money laundering and the implications of these efforts for the legal profession</p> <p>Formulates an effective AML and counter-terrorist financing policy consistent with the U.S. Constitution and other fundamental underpinnings of the lawyer-client relationship. Educates lawyers about AML initiatives, including ABA Formal Ethics Opinion 463.</p>	<p>The CCBE represents the bars and law societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers</p> <p>Includes the Anti-Money Laundering Committee</p> <p>Clarifies how the Recommendations and EU Directives have been implemented in the various EU member states.</p>	<p>Membership consists of 30,000 individual lawyers and over 195 bar associations/law societies globally</p> <p>Operates the Anti-Money Laundering Legislation Implementation Working Group</p> <p>Focuses on challenges for the legal profession presented by compliance with AML legislation throughout the world</p> <p>Provides country by country information on the following website: http://www.anti-moneylaundering.org/globalchart.aspx</p>

Table 1:
Anti-money laundering efforts of bar associations¹¹

The IBA has a specialised working group within its Public and Professional Interest Division, the Anti-Money Laundering Legislation Implementation Working Group, which focuses on the challenges for the legal profession presented by compliance with AML legislation throughout the world.

The ABA's Task Force on Gatekeeper Regulation and the Profession was created in 2002 to analyse and coordinate the ABA's response to AML enforcement initiatives by the U.S. federal government and other organisations that could adversely affect the lawyer-client relationship. It reviews and evaluates ABA policies and rules regarding the ability of lawyers to disclose client activity and information, helps develop policy positions on gatekeeper-related issues, runs educational programs for lawyers and law students and produces related guidance materials for lawyers.¹²

The CCBE has had many discussions with FATF and the European Commission in connection with AML regulations and directives. The CCBE's website sets out its canon of policy work, including numerous position papers and consultations on AML directives. Further, it has worked alongside other European organisations and the Commission of the European Communities to produce a useful document setting out the implementation of the Recommendations within the European Union ("EU") and answering questions on related issues such as tipping-off, the jurisdiction of relevant bar associations over reporting obligations, and the circumstances under which a lawyer is obliged to report to authorities.¹³

A number of European countries have bodies, such as national bar associations, law societies and regulators of the legal profession, that publish guidance and examples of good practices to help lawyers comply with their AML obligations. Lawyers are advised to contact their bar or law society to enquire about the existence of guidelines and to familiarise themselves with such country specific guidance where applicable. An example of such guidance is that produced by the Law Society of England and Wales and the body that steers its AML policy work, the Money Laundering Task Force ("MLTF"). In 2002, following discussions with government, law enforcement, other regulatory bodies and the profession, the MLTF issued official guidance for solicitors. In 2009, in response to the Third EU Money Laundering Directive and the subsequent update of the United Kingdom ("U.K.") AML Regulations, the Law Society of England and Wales released its first AML Practice Note. Her Majesty's Treasury approved the Practice Note, meaning that regulators and the courts must have regard to it when considering allegations that a solicitor has not complied with AML obligations. It is updated regularly – the next wholesale revision will update the Practice Note for the Fourth EU Money Laundering Directive and resultant changes to U.K. AML legislation. The Law Society of England and Wales has also put together a comprehensive package of resources to assist solicitors in complying with U.K. AML legislation¹⁴ and operates a Practice Advice Service that receives approximately 6,000 calls annually from solicitors seeking AML advice.¹⁵

We would encourage bar associations all over the world to consider how they can best help their lawyer members: (i) access and understand relevant AML obligations; (ii) reflect on the ways lawyers and law firms may be misused by criminals in the context of money laundering and terrorist financing; and (iii) reflect on practices lawyers and law firms

can adopt in their particular jurisdiction and in accordance with the relevant bar rules, to ensure the highest ethical standards of the profession are maintained.

Ultimately, however, it is the responsibility of members of the profession to ensure that they each:

- (i) understand the formal AML obligations they are subject to in their country and by reference to their practice;
- (ii) understand their ethical obligations in this area;
- (iii) train their staff to be alert to the misuse of the lawyer and the law firm practice to misuse by criminals;
- (iv) train their staff to identify complex transactions that could inadvertently engage predicate offences¹⁶ and how to advise clients about any reporting obligations triggered; and
- (v) take appropriate action dependent upon the regulations they are subject to if they know or suspect a client or a potential client (or someone dealing with their client) is laundering money or financing terrorists. These actions may include seeking to dissuade the client from the proscribed course of conduct, taking the matter up the chain of authority within the client management structure, reporting the matter to the authorities (at least, where this is required) or refusing to act.

As indicated above, not all lawyers and jurisdictions support the approach recommended in the 40 Recommendations. In particular, many lawyers, bar associations, and others in the international legal community reject or challenge the validity of the requirement placed upon lawyers to report suspicions of money laundering to the authorities due to concerns that this breaches basic lawyer-client confidentiality and privilege rules. In some countries this has led to intensive discussions to persuade member countries not to apply the 40 Recommendations to lawyers and/or to modify their application, in other countries to change, challenge or suspend laws that have been introduced and in certain countries to develop alternative procedures that lawyers are encouraged to follow with a view to preventing money laundering but in ways different from those recommended by FATF.

For example, the Federation of Law Societies of Canada (“FLSC”) launched a constitutional challenge against attempts by the Canadian government to oblige lawyers to report suspicious transactions. This court challenge resulted in an interlocutory injunction suspending application of the AML legislation to Canadian lawyers and Quebec notaries and ultimately led to amendments to the legislation exempting legal counsel from the suspicious transactions reporting requirements. Independent of the litigation, the FLSC developed a model rule to prevent lawyers and Quebec notaries from accepting large sums of cash from their clients. The rule, which has been adopted by all Canadian law societies (the regulators of the legal profession in Canada), restricts members of the legal profession from receiving cash in excess of \$7,500, an amount below the reporting threshold in the legislation. The FLSC subsequently created a model “Know Your Customer” rule (the “KYC Rule”) that requires lawyers to apply identity verification rules

and use reasonable efforts to ascertain a party's identity whenever they assist or advise on a financial transaction. All Canadian law societies have since adopted this rule.

In spite of the AML initiatives of the regulators of Canada's legal profession in 2008, the federal government sought to compel lawyers and Quebec notaries to comply with new client identification and record-keeping regulations. This led to renewal of the FLSC's constitutional challenge. Both the British Columbia Supreme Court and the British Columbia Court of Appeal have ruled that the legislation and regulations: (i) unduly infringe upon the lawyer-client relationship and (ii) are unnecessary in light of the effect and constitutional regulations imposed on legal counsel by the provincial and territorial regulators. An appeal to the Supreme Court of Canada by the federal government was heard in May 2014 and the parties are awaiting the Court's judgment.

The Japan Federation of Bar Associations has played a vital role in ensuring lawyers in Japan are excluded from reporting obligations in legislation imposing AML obligations.¹⁷ Its own regulations allow the legal profession to maintain a "Never to Whistleblow" approach to countering money laundering. The Japan Federation of Bar Associations has drafted its own comprehensive list of events specific to lawyers that trigger client identification duties, which are similar to the situations specified in the 40 Recommendations. In short, the Japan Federation of Bar Associations accepts CDD, but not suspicious transaction reporting.

II. Sources of the Legal Profession's AML Responsibilities

II. Sources of the Legal Profession's AML Responsibilities

356

Lawyers must understand the matrix of AML obligations to: (i) uphold the ethical standards that apply to them, (ii) comply with their AML obligations and (iii) avoid exposing themselves to the risk of unintentionally assisting criminals in the execution of criminal activity (and potential criminal prosecution arising therefrom). The AML obligations not only define the lawyers' role in the fight against money laundering and terrorist financing, but also require lawyers to act and deal with all clients in a variety of ways. If lawyers fail to act in accordance with these obligations in certain jurisdictions (e.g., failing to implement an adequate CDD program or failing to report suspicions of money laundering), they will be at risk of prosecution even if "innocent" of any crime of actual money laundering. It is important to emphasise that these responsibilities apply even in the absence of any intent knowingly to engage in money laundering. In virtually all jurisdictions, it is a criminal offence for a lawyer knowingly and intentionally to engage in, aid or facilitate any other person to engage in, money laundering. In those circumstances, the "crime/fraud" exception to the lawyer-client privilege is likely to apply, thus stripping away any ethical or legal duties of confidentiality.

A. International obligations

From the perspective of the authorities, the 40 Recommendations provide the main international AML standards¹⁸ and have been endorsed by more than 180 countries. As noted above, though, the 40 Recommendations were initially developed for the financial sector and, at times, do not lend themselves well for application to the legal profession with its broad spectrum of legal practices and firms – sole proprietors and multi-jurisdictional international firms – varied internal structures and above all, its professional and ethical duties. The two crucial Recommendations applicable to lawyers provide as follows:

Recommendation 22(d): *"The CDD 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: 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."*

Recommendation 23(a): *"The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications: 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."*

Recommendations 22(d) and 23(a) extend the ambit of only nine of the substantive 40 Recommendations to “lawyers, notaries and independent legal professionals”¹⁹ and are clear that FATF’s AML requirements are only intended to apply when the lawyer is carrying out certain specified transactions and activities – that are believed by FATF to carry a higher risk of money laundering – rather than to all of the legal services provided by the profession. The following conclusions necessarily stem from its ambit:

- certain activities undertaken by lawyers are not within the scope of the 40 Recommendations – e.g., acting for a client on a *bona fide* litigation, including in some jurisdictions the completion of transactions settling or disposing of such litigation – provided that none of the services specified in Recommendation 22(d) are also being carried out;
- notwithstanding the above, Recommendation 22(d) is widely drafted and the relevant “activities” ought to be interpreted cautiously. It would be advisable that lawyers err on the side of caution and comply with relevant national laws when they have any doubt as to whether they are applicable. Of course, a more careful analysis should be undertaken before making a suspicious transaction report (“STR”) (on which see more below); and
- in any event, the ethical considerations that a lawyer should apply in an AML context are not limited by reference to Recommendation 22(d) and these ethical principles should apply to all work carried out by a lawyer. However, the fact that the Recommendations formally apply only to a narrow range of transactions is extremely important in the context of suspicious transaction reporting that many lawyers believe should be construed as narrowly as possible – particularly given the view among many lawyers that STRs run contrary to the confidentiality and loyalty requirements of the lawyer-client relationship.

The Interpretative Note to Recommendation 23 states that DFNBP’s should not be required to report suspicious transactions where they have obtained information raising their suspicions “*in circumstances where they are subject to professional secrecy or legal professional privilege*”. In many jurisdictions (or where cross-border issues arise), this qualification requires a very careful consideration of the ambit of professional secrecy or privilege. Such analyses have highlighted the lack of clarity around the meaning and ambit of such terms that in turn has led, in certain jurisdictions, to a protracted debate as to the scope of this caveat.

Before considering in more detail how the relevant Recommendations apply to lawyers, it is important to emphasise that these Recommendations do not have direct applicability to lawyers (or others). The Recommendations only apply as a result of individual countries adopting laws and regulations that are based upon them. There is a requirement upon countries that are members of FATF to implement the Recommendations and many other countries have chosen to do so. Many countries have implemented the Recommendations in whole or in part and members of FATF are “evaluated” based on their implementation of the Recommendations. Although lawyers need to understand the 40 Recommendations as they form the basis of the laws in many countries, and indeed have been strictly followed in many countries including for example through EU directives, it is the laws

and regulations in an individual country to which the lawyer (and others) are subjected to – accordingly, it is those laws and regulations that the lawyer needs to be both familiar with and comply with, not the 40 Recommendations themselves.

In this Guide we have discussed the Recommendations that apply to lawyers at length because it is beyond the scope of this Guide to provide an analysis of the legal regime in each country that has implemented the Recommendations and, to generalise broadly, many countries have adopted the Recommendations without significant change subject to two critical—and fundamental—points:

- (i) some countries, such as the U.K., have “gold plated” the 40 Recommendations, meaning that they have extended the 40 Recommendations to an expansive range of “predicate offences” (i.e., the offences that generate the money laundering that in turn generate the obligations to prevent money laundering), even if the conduct constituting the offence occurred outside the U.K., and not just serious criminal offences; and
- (ii) in some countries, for example the U.S., concerns about the impact of STR on the administration of justice, the lawyer-client relationship, the rule of law, and the independence of the legal profession, have led to an approach that focuses on educating lawyers regarding unwitting involvement so that criminals will not be able to find lawyers who will assist them in their unlawful schemes. In a recent empirical study regarding terrorist financing, U.S. law firms performed among the best among surveyed entities in refusing requests for help in suspicious circumstances. This is a good illustration of approaches that are “different” to those in the 40 Recommendations and are working effectively in practice.

The following discussion of the Recommendations (and suggested actions) is general and not country-specific. Nevertheless, a discussion of the 40 Recommendations is relevant to all lawyers, regardless of whether they are subject to corresponding national laws implementing the 40 Recommendations as they are the core international AML standards. In addition, lawyers have ethical obligations (including with regard to AML – see further Section C below) and a knowledge of the 40 Recommendations can help lawyers enhance their general AML compliance and better understand the issues that concern regulators.

Customer due diligence – Recommendation 10

This Recommendation requires lawyers to know who their client is when:

- (i) business relations are being established and certain occasional transactions are entered into;
- (ii) there is a suspicion of money laundering or terrorist financing; or
- (iii) there are doubts as to the veracity or adequacy of previously obtained customer identification data.

When dealing with a client that is not an individual or a group of individuals, effective CDD requires identifying not only the client but also its beneficial owner(s), i.e., the

person(s) who ultimately own or control the client. For more information on this, see paragraph (iii) of Section A of Part IV.

Suggested Actions For Lawyers

Identify the client and their beneficial owner

Use reliable, independent source documents, data or information. If dealing with a corporate, request structure chart and details of beneficial ownership

Understand the business relationship

Understand, and if appropriate, obtain information about the purpose and intended outcome of the transaction for which your services are being engaged

Maintain CDD activities

Conduct due diligence about the business relationship and services on an ongoing basis to ensure they accord with your knowledge of the client, its source of funds and risk profile

If you cannot carry out satisfactory CDD

Do not establish a business relationship or continue acting for the client. In relevant countries consider whether you are required to make an STR

Record keeping requirements – Recommendation 11

FATF recommends that, for a period of 5 years after the end of a business relationship or the date of an “occasional transaction”, lawyers maintain necessary records on all transactions (international and domestic) that could be required to comply with requests for information from competent authorities.

Suggested Actions For Lawyers

Relevant records

Keep documents obtained for your CDD measures (copies or originals), files and business correspondence for a period of time after the end of the business relationship or after the date of the “occasional transaction” (usually corresponding to the time period recommended by FATF (i.e., 5 years) or, if longer, a national limitation period (e.g., 10 years in Italy)). In the U.S., a number of states require lawyers to maintain certain client records for several years (e.g., 5-7 years in some states).

Records include

Electronic communications (e.g., emails) and documentation, as well as physical, hard copy communications (e.g., letters) and documentation

Records must be

“Sufficient to permit the reconstruction of individual transactions” (including the amounts and types of currency involved) so that they can serve as evidence in a prosecution

Enhanced CDD for politically-exposed persons – Recommendation 12

Lawyers must have appropriate risk-management systems in place to determine whether a client or its beneficial owner is a politically exposed person (“PEP”), that is, a person who is or has been entrusted with prominent public functions or his or her close associates.²⁰ Enhanced CDD measures must be applied to all *foreign* PEPs, their family members and close associates. In certain circumstances, enhanced CDD measures also may need to be applied to domestic PEPs or international organisation PEPs. If a lawyer determines a client or its beneficial owner to be a domestic or international organisation PEP, the lawyer must carry out a risk assessment of the business relationship with the

PEP (bearing in mind the same red flag indicators that apply to assessing money laundering risks generally, discussed in Part IV). If the outcome of such a risk assessment is that the business relationship would be one of higher risk, the lawyer ought to apply enhanced CDD measures consistent with those that would apply to a foreign PEP.

Underlying the rationale for applying enhanced CDD to PEPs and their associates is the influence that PEPs have, which puts them in positions that can be misused to launder money and finance terrorism, as well as to facilitate predicate offences, such as corruption and bribery.

Suggested Actions For Lawyers

When dealing with PEPs, or their families or close associates:

- obtain senior partner (or another partner's) approval for establishing/continuing the business relationship
- take reasonable steps to establish the source of wealth and funds
- conduct enhanced ongoing monitoring of the business relationship

Note: The broad definition of PEP may make it difficult to determine whether your clients (or their beneficial owners) are PEPs. Check whether you have access to any resources (such as a database containing the names and identities of PEPs) that may help you with this

New technologies – Recommendation 15

Lawyers must keep pace with new ways in which money laundering and terrorist financing are carried out because they could be advising on transactions involving such technologies.

Suggested Actions For Lawyers

New technologies – identify, assess and manage the risks that may arise when:

- new products and business practices are developed by/for lawyers
- new technologies are used by lawyers for new and existing products

Reliance on third parties and group-wide compliance – Recommendation 17

Lawyers can rely on a third-party to carry out CDD measures on their behalf. This is most likely to be relevant when the client is based in a different country to that in which the lawyer is based, e.g., a law firm in country A instructs a law firm in country B on behalf of a client. Note that when CDD is carried out through a third-party, AML responsibility still rests with the lawyer who is doing the relying, i.e., the relying lawyer may be found guilty if that lawyer undertook legal work that assisted money laundering activities having relied on someone who failed to perform proper CDD.

Suggested Actions For Lawyers

Choice of third party

Be satisfied that the third party (i) has a good reputation, (ii) is regulated, supervised and monitored, (iii) has measures in place for compliance with CDD and record-keeping requirements under Recommendations 10 and 11 and (iv) has necessary information concerning country specific risks in its country of operation

CDD information

Obtain necessary information under Recommendation 10 for your own records from the third party and satisfy yourself that copies of identification data and other documentation collected under CDD measures will be available from the third party upon request

Internal controls – Recommendation 18

Law firms and other organisations to which the 40 Recommendations apply must implement compliance programmes against money laundering and terrorist financing.

Suggested Actions For Lawyers

If you manage a law firm or practice

Ensure that an adequate AML compliance programme is in place and provide appropriate training for your employees on an ongoing basis

International law firms

Internal controls ensuring AML compliance must be implemented in foreign branches and majority-owned law firms abroad. Consider whether compliance with additional local requirements is required

Enhanced CDD for higher risk countries – Recommendation 19

The 40 Recommendations call for enhanced CDD measures to be applied to clients from higher risk countries (being countries designated by FATF as such²¹).

Suggested Actions For Lawyers

Identifying high risk countries

See Part IV of this Guide for a list of country and geographic risk factors that you can use to identify whether you are dealing with a client from a higher risk country

Client from higher risk country

When dealing with such natural or legal persons and financial institutions apply enhanced measures that are effective and proportionate to the risks, e.g., carry out more thorough background checks and insist on provision of original documents where practicable

Suspicious transaction reporting – Recommendation 20

This Recommendation suggests that national laws should require that suspicions that funds are the proceeds of crime be reported to a financial intelligence unit (“FIU”). Many lawyers view this as the most difficult Recommendation to comply with as it is contrary to their views of the traditional confidentialities between client and lawyer. Accordingly, great care should be taken before any such report is made. However, in those countries where lawyers are required to make reports they need to be aware of the obligation to do

so and the consequences of any failure to report. There are examples in some jurisdictions (e.g., the U.K.) of lawyers being successfully prosecuted for a failure to report. In countries where the obligation to report exists, the relevant bar association (or specialist group) often provides advice and guidance on the topic and lawyers, in particular sole practitioners and small law firms, are encouraged to take advantage of this support.

Suggested Actions For Lawyers

Suspicious Transaction Reports

Familiarise yourself with the requirements relating to STRs in the relevant jurisdiction. If there is an obligation to make STRs and you suspect, or have reasonable grounds to suspect, that funds are proceeds of a criminal or terrorist activity report your suspicions to the relevant FIU (or as required in the relevant jurisdiction(s))

Tippling off and confidentiality – Recommendation 21

There is a tension between client confidentiality and compliance with AML obligations by lawyers, who owe an ethical obligation to their clients to maintain confidence and to act in their clients' best interests (see Section C below). Except in limited circumstances, in many countries lawyers may not divulge confidential client information without seeking their clients' prior consent. Some countries do not even allow clients to "waive" their right to confidentiality. These obligations are juxtaposed against the fact that compliance with AML obligations in some countries necessitates the reporting of confidential information by lawyers to the authorities. Recommendation 21 aims to ensure that, when sharing their suspicions about money laundering and terrorist financing activity with the relevant authorities in good faith, lawyers:

- (i) are protected from the repercussions of breaching the duty of confidentiality; and
- (ii) do not tip-off their clients as to the STRs they make, so as to not thwart any investigative efforts into the reported person's activities. Avoiding tipping off is an extremely problematic issue for lawyers not least as it may involve the lawyers ignoring the client and/or stalling and/or taking other action that is not consistent with good service and putting the client first. Even in situations where the FIU permits a lawyer to continue acting the lawyer is still under an obligation to avoid tipping off and, for example, avoiding an honest explanation for any delay that may have occurred as a result of the reporting.

Suggested Actions For Lawyers

STRs

Consider adding provisions to your terms of engagement that track the protections in Recommendation 21 so as to protect yourself contractually from civil liability for compliance with STR obligations if you report suspicions in good faith to the FIU

Tippling-off

Do not disclose to, or tip off, the client that an STR is being filed with the FIU

B. National obligations

As mentioned in Part I, the 40 Recommendations do not themselves impose obligations on lawyers – instead, they are a set of recommendations that national legislatures should follow when imposing AML obligations through domestic law. Accordingly, where AML obligations have been imposed via national laws, what really matters to lawyers are the laws of the country (or countries) in which they practice.

In some jurisdictions national laws reflect collaborative efforts by a group of countries. A prime example of this is the EU, which, since 2003, has been imposing AML obligations on lawyers via the Second Anti-Money Laundering Directive.²² Among other things, the directive requires lawyers to conduct CDD whenever they carry out activities that are largely identical with those listed in Recommendation 22(d) – the influence of the Recommendations is readily apparent in the directive. Indeed, the EU is currently updating the directive to reflect the changes to the 40 Recommendations and published a proposal in 2013 for a fourth AML Directive.²³ Of course, directives do not have direct effect in the EU member states and are implemented via national laws and regulations. These may therefore be implemented differently. Nonetheless, there is a common approach to imposing AML obligations on lawyers throughout all the EU member states.

There are jurisdictions where no formal AML obligations are imposed on lawyers, but in which lawyers are still expected to play a role in the fight against money laundering. For example, unlike their European counterparts, U.S. lawyers are not subject to the general AML responsibilities.²⁴ They are not mandated by separate law to comply with those gatekeeper requirements concerning suspicious activity reporting, CDD or record-keeping.²⁵ This does not mean they should reduce their awareness of suspicious transactions involving their clients. Furthermore, although not part of a set of wider AML obligations, U.S. lawyers must not:

- retain a fee received from illicit funds;
- receive currency of \$10,000 or more unless they file currency transaction reports;²⁶ and
- transact, facilitate or advise with respect to a transaction with “blocked persons”, namely drug traffickers, terrorists and former foreign leaders of certain nations like North Korea, or with any other person subject to U.S. economic sanctions, without a license from the U.S. Treasury Department.²⁷

In jurisdictions where AML obligations are not imposed by law on lawyers, but where civil or criminal liability will still arise if a lawyer participates (even unwittingly) in a client’s scheme to launder money, it would be advisable for lawyers to be aware of the 40 Recommendations to minimise the risk of facing criminal prosecution or civil liability.

Throughout the world, self-regulating organisations (“SROs”) (or, in certain jurisdictions, co-regulating organisations) such as bar associations play a part in shaping lawyers’ AML obligations.²⁸ Depending on the powers and responsibilities of the SROs (e.g., in the U.S. these include independent lawyer disciplinary agencies), they may be able to facilitate or

ensure compliance by lawyers with the relevant legislation and/or develop guidance relating to money laundering and terrorist financing (refer to Section B of Part I).

In jurisdictions where there are no laws imposing AML or related obligations, lawyers still have ethical obligations that require them to avoid supporting criminal activity and being unwittingly involved in its pursuit (see Section C below). Those lawyers who are not subject to any relevant national laws should have regard to international standards (predominantly the 40 Recommendations) to ensure that they are meeting their ethical obligations. Such lawyers will still be faced with the difficult issue of reporting money laundering suspicions to authorities, which, if there are no national laws on AML compliance, is unlikely to be a regulated issue. In such circumstances, we suggest that lawyers consult applicable ethics rules and standards as well as guidance issued by their bar association(s) or law societies.

C. Ethical obligations and STRs – challenges to lawyers

Among other obligations relating to criminal conduct, professional ethics require lawyers not to assist clients in the conduct of criminal activity. Clearly, an important part of the lawyer’s role is to represent persons who have been charged with criminal activity and indeed to represent guilty criminals (e.g., in sentencing and litigation situations). Similarly, lawyers frequently advise clients as to whether certain actions may be criminal and/or illegal (e.g., advising on whether a tax scheme is a legal avoidance of tax, as opposed to an illegal evasion of tax). Neither FATF nor any other regulatory body has apparently suggested that the role a lawyer plays in providing such types of advice conflicts with underlying ethical requirements, or is inconsistent with the principles behind the 40 Recommendations and national legislation.

As a profession, lawyers accept the premise that they should not assist clients in the conduct of criminal activity and the profession should be on its guard against misuse by criminals. Ethical obligations arguably already require lawyers to analyse carefully the reputation and motivation of their clients through “client due diligence” – there is very little disagreement about this among lawyers. The more difficult ethical issue is whether lawyers should be required to report clients to the authorities if they suspect them of money laundering. The applicable legal standard for forming a “suspicion,” which might be quite low, is a factor that adds to the difficulty facing lawyers in this regard.

A public interest underlies both AML measures and the duties of confidentiality that lawyers owe to clients. However, as mentioned above in the context of Recommendation 21, there is a tension between compliance with AML obligations and the duties of confidentiality and loyalty that the legal profession owes to its clients. In requiring lawyers to file STRs on their clients, the 40 Recommendations risk compromising the independence of the profession, because by reporting on their clients’ suspect transactions and activities to the authorities, lawyers are effectively becoming agents of the state.²⁹ The “no-tipping off rule”, which forbids lawyers who file STRs from informing their client that they have done so, may further damage the clients’ confidence in their lawyers’ services and impact the administration of justice.³⁰

Traditionally, communications between lawyers and clients in the provision of legal advice and representation in current and future litigation have been protected by legal professional privilege (a common law concept) and professional secrecy (a continental law concept), which are only abrogated in certain countries under certain circumstances by statute, ethical rule, or because the arrangement between lawyer and client is criminal in nature. As mentioned in Section A above, the tension between simultaneous compliance with AML and confidentiality obligations is addressed through the Interpretative Note to Recommendation 23, which excludes lawyers from the obligation to report suspicious transactions where they obtain information about them in privileged circumstances or subject to professional secrecy.³¹ The Interpretative Notes, like the Recommendations themselves, are also directed at countries implementing the Recommendations, rather than at lawyers. Further, the Interpretative Note to Recommendation 23 also states that “[i]t is for each country to determine the matters that would fall under legal professional privilege or professional secrecy”. Accordingly, knowledge of national laws relating to privilege or professional secrecy is key for lawyers concerned about breaching confidentiality when making an STR, as national laws will determine whether there is a concept of privilege or professional secrecy in the relevant jurisdiction and what circumstances it covers. As an example, the U.K. has a specific “privileged circumstances” defence to the requirement to report suspicions of money laundering.³² Lawyers should consult guidance published by their local bar association to determine the existence, and extent, of any privilege or professional secrecy exception in their jurisdiction.

Where national legislation does not provide an answer, the following three factors should help reduce the perceived tension between AML compliance and confidentiality obligations and highlight the common ground between the two duties:

- (i) AML obligations mostly arise in the context of activities that are criminal;
- (ii) the goal behind the FATF 40 Recommendations of trying to prevent lawyers from assisting clients in money laundering and terrorist financing activities is consistent with the ethical obligations of lawyers; and
- (iii) the ethical obligation to act in accordance with the client’s interests as the overriding imperative guiding professional behaviour is not necessarily absolute.

The IBA’s International Principles on Conduct for Lawyers make it clear that the principle of treating client interests as paramount is qualified by duties owed to a court and the requirement to act in the interests of justice.³³ The same concept is found in ABA Model Rule of Professional Conduct 3.3, in which certain specific obligations to the tribunal take precedence over obligations to the clients. The CCBE Code of Conduct lays down similar principles for European lawyers.³⁴ The ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 463 in May 2013 dealing with the ethical dimensions of the ABA’s voluntary AML good practice guidance and noting the tensions between compliance with AML obligations and the duty of confidentiality that lawyers owe to their clients.³⁵ While guidance from the IBA, CCBE and the ABA is not binding, it does underscore the fact that members of the legal profession are also guardians of justice and are expected by society to uphold the rule of law. Any duties owed by lawyers by virtue of the fact that they are lawyers should be interpreted in light

of the role that members of the legal profession are expected to play in society – such expectation does not include creating barriers that can be abused by persons engaging in money laundering and terrorist financing for their criminal gain. Although there seems to be a global consensus that lawyers owe obligations to multiple constituencies, there is great variation in how these competing interests are balanced in any particular country. All agree that a lawyer should not assist a client in criminal activities, but the details of how these obligations are implemented vary from country to country. The resolution is often the result of detailed policy considerations, input from stakeholders and consideration of the context and history within the jurisdiction. Accordingly, one can agree on the overarching principle that lawyers should not assist criminals in illegal activity, as FATF has sought to promulgate, but implementation should be appropriate to each jurisdiction. The key point is that it is vital that lawyers are not facilitating criminal financial flows and that, instead, they uphold the law.

D. Policy issues for the profession to consider

Additionally, there are certain other policy issues – related to the underlying criminal offence – for the legal profession to consider. Whether conduct is criminal has a bearing on whether proceeds flowing from such conduct constitute the “proceeds” of crime within the scope of AML regulations. Examples of these issues include:

- Should there be a standard for the types of criminal conduct subject to AML regulations? Given that there is such a wide spectrum of severity of criminal offences – ranging from breaches of technical regulatory regimes to drug trafficking – it is questionable if reports arising from certain predicate criminal offences (e.g., inadvertent breaches of technical regulatory regimes) aid FIUs in combatting money laundering.
- If there should be a standard, how should the line be drawn?
- Would it be helpful to instead focus on the proceeds resulting from such breaches and have a *de minimus* monetary figure before reporting is required?
- Should there be a global standard in relation to what is criminal for AML purposes? The difference in the types of criminal offences globally means that there is a disparity as to the types of offences that may trigger reporting obligations in different countries. This would be particularly relevant if the conduct is multi-jurisdictional and may only be criminal in one jurisdiction. Should the proceeds flowing from such a transaction trigger reporting obligations only in the jurisdiction in which the conduct is criminalised?

This Guide raises these policy issues because a discussion of them is helpful to understanding the impact of varying standards of criminal conduct on the scope and sources of AML regulations. This Guide does not, however, seek to provide answers to these policy issues.

III. Vulnerabilities of the Legal Profession to Money Laundering

III. Vulnerabilities of the Legal Profession to Money Laundering

368

Lawyers are potentially vulnerable to being misused and so unwittingly assisting in the money laundering activities of criminals. Criminals may seek legal services to lend a gloss of legitimacy to their crime-based financial, corporate and real estate transactions and are increasingly adopting sophisticated and complex means to channel illicit funds into and through the financial system. Special considerations apply to identifying persons who wish to access legal services to facilitate funding of terrorist activities. While awareness of the general instances of money laundering should help, there are additional vulnerabilities to consider in relation to terrorist financing. In particular, terrorist financing may involve low dollar amounts and the use of activities that present as innocent and aid in concealing the intentions of the client (e.g., masking financing as charitable donations).³⁶ This Guide does not comprehensively address the vulnerabilities of the legal profession to terrorist financing in particular and, instead, focuses on money laundering generally.

There are three main reasons why lawyers are exposed to misuse by criminals involved in money laundering activities. First, engaging a lawyer adds respectability and an appearance of legitimacy to any activities being undertaken – criminals concerned about their activities appearing illegitimate will seek the involvement of a lawyer as a “stamp of approval” for certain activities. Second, the services that lawyers provide, e.g., setting up companies and trusts, or carrying out conveyancing procedures, are methods that criminals can use to facilitate money laundering. Third, lawyers handle client money in many jurisdictions – this means that they are capable, even unwittingly, of “cleansing” money by simply putting it into their client account.

A. Types of services that are vulnerable to money laundering

FATF has identified certain legal services, though not necessarily accepted by the legal profession, as particularly susceptible to misuse by criminals in the context of money laundering and terrorist financing:



Figure 2:
Money laundering and terrorist financing –
susceptible legal services³⁷

Lawyers involved in real estate transactions should be particularly vigilant according to FATF. Data from STRs and confiscated assets reports compiled by FATF show that real estate assets formed 30% of all criminal assets in the years 2011–2013, highlighting that criminals tend to channel their illegal funds into the financial system through the guise of property purchases and sales.³⁸

Even the most vigilant of lawyers may have difficulty identifying transactions or funds that are tainted with illicit origin when criminal proceeds have already been “laundered” to a large extent to disguise any appearance of irregularity. Moreover, the patterns of money laundering and terrorist financing are rarely static, so the red flags that appear useful one day need to be updated the next. Lawyers should thus keep themselves up-to-date with the latest news and movements of criminal activity through resources provided by FATF and their own bar associations and law societies, as well as through appropriate educational programmes. This is an area where bar associations and law societies can play an extremely useful role to ensure that members are kept abreast of any developments.

B. How lawyers may be involved: from intentional involvement through wilful blindness / negligent involvement to unwitting involvement

The legal profession’s involvement in money laundering and terrorist financing transactions can be drawn across a spectrum, ranging from a lawyer being wholly complicit in the criminal activity to being unknowingly or unintentionally involved.

The legal profession does not, and never will, condone the actions of any lawyer who

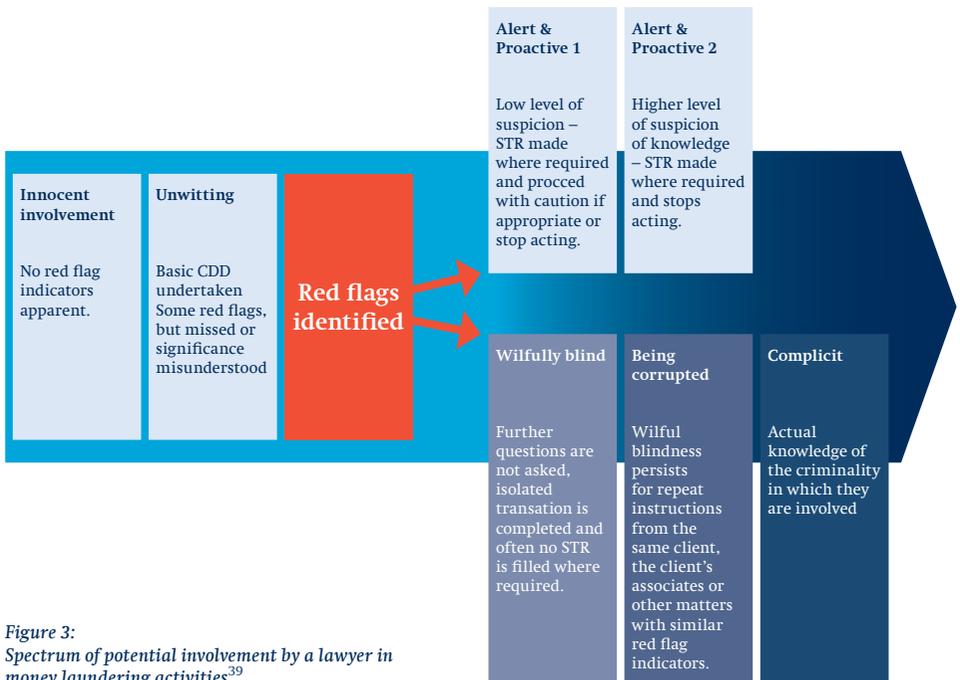


Figure 3: Spectrum of potential involvement by a lawyer in money laundering activities³⁹

knowingly participates in the criminal activity of a client, regardless of whether it is related to money laundering – they are likely to be directly guilty of a criminal offence. This Guide aims to provide information and guidance for lawyers who might unknowingly or unintentionally be involved in money laundering and terrorist financing activity because, for example, red flag indicators are not readily apparent as the transaction proceeds and funds have been “cleaned” of all traces of criminality, or because the lawyers fail to appreciate the significance of the red flags in front of them.⁴⁰

It is impossible for lawyers to avoid completely innocent involvement because in some circumstances, there are no red flag indicators apparent. There is nothing to alert even the most observant and suspicious lawyer. Further down the spectrum, lawyers who observe some of the practices suggested in this Guide should be able to avoid being accused of unwitting involvement or wilful blindness and should be better at questioning whether they are being wilfully blind. Wilful blindness should be guarded against and the lawyer who is vigilant will cease to be ‘wilfully blind’ and take appropriate action. The lawyer who is knowingly and wilfully blind to the situation is, for all intents and purposes, complicit with the criminal and could be prosecuted accordingly.

If the activities of a client or other party to a client’s transaction raise suspicions, a lawyer should file an STR (where this is required) and, depending on the level of information the lawyer has for the suspicion and the lawyer’s professional obligations in the given circumstances, either proceed with the transaction with caution, or cease acting for the client. The lawyer, however, must be careful not to disclose to the client the fact that an STR was filed given the no tipping-off provisions that typically accompany rules requiring suspicious transaction reporting.

Even where individual red flag indicators do not sufficiently raise the suspicion of money laundering, the lawyer ought to consider whether there are grounds to inquire more of a client to remove concerns about the source of funds being used in the transaction – i.e., are you asking enough questions and are you in danger of being accused of being wilfully blind?

A lack of information may also raise concerns. A client’s evasiveness or unwillingness to give answers may arouse suspicion that the lawyer’s services are being misused, especially where there are multiple red flag indicators present. Questioning why your client is not forthcoming will help you to establish whether the client has legitimate reasons for withholding information (e.g., concerns around breaching confidentiality agreements) or whether the client’s evasiveness is an indication of underlying criminal intentions.

IV. The Risk-based Approach and Money Laundering Red Flags

IV. The Risk-Based Approach and Money Laundering Red Flags

372

A. The Risk-Based Approach to Fighting Money Laundering

(i) What is the Risk-Based Approach?

A risk-based approach is widely accepted, including by FATF and the regulators, as the most effective way of tackling money laundering and terrorist financing, as it:

- reduces the “checklist” mentality inherent in a “rules-based” approach that requires compliance with rules irrespective of the underlying risk;
- ensures that the highest risk scenarios receive enhanced CDD and transaction monitoring; and
- allows lawyers and law firms to most effectively and efficiently deploy their resources and personnel to ensure compliance with the applicable AML regime.

The IBA, ABA and CCBE formed an informal working group that developed, with FATF, a risk-based approach guidance for lawyers. This resulted in FATF’s publication of the “Risk-Based Approach Guidance for Legal Professionals”⁴¹ (“Lawyer RBA Guidance”) in 2008. The Lawyer RBA Guidance divides risks into three categories – country/geographic risk, client risk and service risk – each of which has a number of elements or factors that should be evaluated separately.

Country/ Geographic Risk	Client Risk	Service Risk
<p>Countries subject to sanctions, embargoes or similar measures issued by, for example, the UN</p> <p>Countries identified by credible sources (i.e., well-known bodies that are regarded as reputable, e.g., International Monetary Fund, The World Bank, and OFAC) as:</p> <ul style="list-style-type: none"> • generally lacking appropriate AML laws, regulations and other measures; • being a location from which funds or support are provided to terrorist organisations; or • having significant levels of corruption or other criminal activity. 	<p>Domestic and international PEPs</p> <p>Entity, structure or relationships of client make it difficult to identify its beneficial owner or controlling interests (e.g., the unexplained use of legal persons or legal arrangements)</p> <p>Charities and “not-for-profit” organisations that are not monitored or supervised by authorities or SROs</p> <p>Use of financial intermediaries that are neither subject to adequate AML laws nor adequately supervised by authorities or SROs</p>	<p>Where lawyers, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they control</p> <p>Services to conceal improperly beneficial ownership from competent authorities</p> <p>Services requested by the client for which the lawyer does not have expertise (unless the lawyer is referring the request to an appropriately trained professional for advice)</p> <p>Transfer of real estate between parties in an unusually short time period</p>

Country/ Geographic Risk	Client Risk	Service Risk
	<p>Clients who:</p> <ul style="list-style-type: none"> • conduct their business relationships or request services in unconventional circumstances; • are cash-intensive businesses (e.g., money service businesses and casinos), that are not usually cash-rich but generate substantial amounts of cash; • have no address, or multiple addresses; or • change settlement or execution instructions. 	<p>Payments from un-associated or unknown third parties and payments for fees in cash where this would not be typical</p> <p>Consideration is inadequate or excessive</p> <p>Clients who offer to pay extraordinary fees for services that would not warrant such a premium</p>

Table 3:
Factors relevant to evaluating risks of money laundering and terrorist financing in the legal profession⁴²

For example, a transaction could have a “high” service risk because certain types of services (e.g., clearing money through client accounts) are involved, but a “low” country risk because it originates from a country that is not subject to UN sanctions and has appropriate AML laws.

This approach to risk analysis is not explicitly embedded in any national laws to which a particular lawyer may be subject. The Lawyer RBA Guidance generally serves as good guidance in terms of encouraging lawyers how to think about the risks they face in an AML or terrorist financing context. Further, it ties in well with the red flag indicators discussed in Part IV – a risk-based approach: (i) supports lawyers in identifying red flags through ‘onboarding’ processes such as CDD and (ii) provides a framework to alert lawyers to red flags at various stages of the transaction that money laundering may be an issue, prompting further analysis, questions and/or preventative action. Sections B, C and D below suggest how lawyers should use a risk-based analysis in practice and for training purposes. Where national laws do not have scope to allow for a risk-approach to be used, the following still provides a useful overview of how CDD may be best approached.

(ii) Key Risk-Based Approach Procedures

A risk-based approach can be effectively implemented by lawyers using certain procedures, assisting them with identifying and assessing the risks posed by red flag indicators.

Client Intake Procedure	<ul style="list-style-type: none"> • Identify and verify the identity of each client on a timely basis (particularly if the client identity changes) • Identify, and take reasonable measures to verify the identity of, the beneficial owner • Understand client's circumstances and business, depending on the nature, scope and timing of services to be provided. You can obtain this information from clients during the normal course of their instructions
Proceed with engagement?	<ul style="list-style-type: none"> • After completing the client intake procedure consider whether there is a risk for the lawyer of committing the substantive offence of money laundering though assisting the client • Make a risk assessment of any red flags present and clarifications sought from the client to decide whether to proceed, or continue, with the engagement
Monitor	<ul style="list-style-type: none"> • Continue to monitor the client's profile for signs of money laundering and terrorist financing, particularly if the client is a PEP or from a higher risk country • Adopt the risk-based approach of evaluating money laundering and terrorist financing risks by client, type of legal service, funds and client's choice of lawyer
If required and/or permitted, making an STR	<ul style="list-style-type: none"> • If there are grounds for suspecting criminal proceeds are being used in a transaction or in engaging the lawyer, the lawyer should, where required, make an STR to the FIU of the relevant jurisdiction • Consider whether the client should be advised to make its own STR to avoid committing a principal money laundering offence • Consider whether to stop acting for the client immediately after making the STR if the client is the subject of the STR or if the client insists on completing a transaction in violation of applicable law
Avoid Tipping Off	<ul style="list-style-type: none"> • When an STR is filed with the FIU, refrain from disclosing to the client or related parties that an STR has been filed

Figure 4:
Suggested practice for lawyers concerned about money laundering activities

(iii) Client intake procedures and monitoring

AML compliance begins with adequate client intake procedures, which should start with obtaining information about the client and verifying its identity. Beyond getting the client's name, address and telephone number, it may be necessary to get additional information, for example:⁴³

- client's past and present employment background;
- place and date of birth;
- past and current residential address;
- business address and phone numbers;
- marital status;

- names and other identification data of spouse(s) and children;
- name and contact details of the client’s certified public accountant;
- past criminal record;
- pending lawsuits; and
- tax filings with government authorities.

In addition to this basic information, the lawyer should check if the client’s name is on any relevant official database or “black list” concerning financial or economic sanctions, for example, the Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions maintained by the European Commission and the Specially Designated Nationals and Blocked Persons List and Sectoral Sanctions Identifications List maintained by the U.S. Treasury Department. Another good starting point is simply conducting an Internet search of the client’s name.

If any red flags about the client are raised, enhanced or additional review may be appropriate. Larger firms may do well to implement procedures for referral of higher risk clients to management levels or specially formed committees. Smaller firms may not be able to implement the same kind of procedures, but even sole practitioners should seek an additional review when red flags are raised or discuss your concerns with a colleague or a local bar association or representative of a specialist group, such as a sole practitioners association.

As briefly mentioned in the context of Recommendation 10 in Part II, CDD requires identifying not only the client but also its beneficial owner(s), i.e., the person(s) who ultimately own or control the client. Depending on whether a lawyer is dealing with a client that is a company, trust, partnership or other legal entity, the beneficial owner can exercise control over the client through ownership of shares, voting rights, or other forms of control over management. Conducting CDD on the client should alert the lawyer to the presence of a beneficial owner, (which he or she can also clarify directly by asking the client). Where the client has a beneficial owner, the lawyer should use the same CDD procedures that are used in connection with verifying the client’s identity and take reasonable steps to identify and verify the identity of the beneficial owner.

When dealing with clients who are individuals there is no need to identify potential beneficial owners as such. However, a similar concept applies – just as a beneficial owner will direct a corporate client’s activities, instructions that are seemingly coming from a client who is an individual may be directed by a third party. Lawyers must remember to establish that they are carrying out legal services for the client in front of them in accordance with that client’s instructions, otherwise lawyers will not be capable of verifying the motive of a client and the purpose for which their services are being engaged. Lawyers should be wary of ‘front guys’ or ‘agents’ who are merely used as a means of communicating a third party’s instructions.

Good practice indicates that lawyers should have appropriate internal “on-boarding” procedures. At a minimum, lawyers should have in place checklists of what basic CDD

measures should consist of so that they have a reference point for where to start. Law societies in various jurisdictions may provide a basic list of what CDD measures are required to be carried out by the law firms in that jurisdiction (e.g., the Law Society of Hong Kong). Lawyers could use these as a starting point to assist them in developing their own “on-boarding” procedures. Ideally, lawyers should aim to develop an internal policy and procedure for on-boarding so that CDD measures are consistently applied and that there is clear evidence of the approach taken. A lack of satisfactory procedures means that lawyers remain at risk of committing money laundering offences, and can in certain jurisdictions result in fines, civil penalties or even criminal prosecution by the authorities.

The same basic principles that apply in the client intake process are also applicable when monitoring the client relationship. As the profile (or even the identity) of the client may change over time, vigilant lawyers should, as circumstances change, re-evaluate and update the client profile. The goal of this ongoing monitoring is for lawyers to monitor and regularly re-assess whether they have been asked to facilitate money laundering and terrorist financing. If the lawyers conclude that this is why they have been retained, they should decline to continue the representation. Lawyers should evaluate the ongoing money laundering and terrorist financing risk of continuing to work for a client through the same risk-based approach used at intake – country risk, client risk and service risk.

B. How to use “red flags” to assess money laundering or terrorist financing

Looking for and recognising red flags helps alert lawyers to the potential for misuse and helps them to identify possible money laundering and terrorist financing activities. Hence, regardless of the area of law that is the focus of their practice, lawyers should be aware of certain red flag indicators that may arise in every day practice. When reading this Section B, it should be noted that:

- the red flags discussed are contextual – client risks and the source of funds may compel further inquiry by the lawyer; and
- the mere presence of a red flag indicator is not necessarily a basis for a suspicion of money laundering or terrorist financing – a client may be able to provide a legitimate explanation.

We will discuss red flags as they arise in the context of:

- the client;
- the services lawyers provide;
- the clients’ funds; and
- the clients’ choice of lawyer.

(i) Red flags about the client – is the client risky?

The major source of red flags is the “person” in front of you – whether an individual or a company. Clients may themselves have criminal intentions or they may, knowingly or not, become involved with entities that do, e.g., through investments. It is important to

scrutinise the person in front of you and the intentions behind their instructions to understand more about the person you are being engaged by and the context of the services that are being requested. Red flag indicators relating to client risk include:

Client's behaviour or identity	Concealment techniques	The relationship between the client and counterparties
<p>Client is secretive or evasive about:</p> <ul style="list-style-type: none"> • its identity or that of its beneficial owner; • the source of funds or money; or • why it is doing the transaction in the way it is <p>Client is:</p> <ul style="list-style-type: none"> • known to have convictions, or to be currently under investigation for, acquisitive crime or has known connections with criminals; • related to or a known associate of a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations; • involved in a transaction that engages a highly technical or regulatory regime that imposes criminal sanctions for breaches (increasing the risk of a predicate offence being committed); or • unusually familiar with the ordinary standards provided for by the law in satisfactory customer identification, data entries and STRs, or asks repeated questions on related procedures 	<ul style="list-style-type: none"> • Use of intermediaries without good reason • Avoidance of personal contact for no good reason • Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction • Use of false or counterfeited documentation • The client is a business entity that cannot be found on the Internet 	<ul style="list-style-type: none"> • Ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature/ reason for transaction • Multiple appearances of the same parties in transactions over a short period of time • The parties attempt to disguise the real owner or parties to the transaction • The natural person acting as a director or representative does not appear to be a suitable representative <p>The parties are:</p> <ul style="list-style-type: none"> • native to, resident in, or incorporated in a higher-risk country; • connected without apparent business reason; • of an unusual age for executing parties; • not the same as the persons actually directing the operation

Table 4:
Summary of client risk profiles

The nature of the client relationship will also be a factor in considering the client risk at hand. If the lawyer has been regularly representing the client for many years on certain types of transactions, there is low risk should the client request that the lawyer carry out the same, or similar, type of transaction again. Accordingly, reduced CDD would suffice

in the circumstances. By contrast, a sudden change in the transactions being undertaken by an existing client or taking on a new client that is reluctant to disclose information may raise red flags and call for heightened scrutiny.

Understanding whether substantial client risk exists also requires lawyers to keep track of country risk profiles – which country is the client from and where are they doing business? This will be particularly important where a lawyer’s clients are usually located in different jurisdictions from that lawyer. Rankings of corruption provided by Transparency International (a global civil society organisation that fights corruption), and reports collated by The World Bank annually may be useful resources in this regard.⁴⁴

Please refer to case studies 1, 2, 3 and 4 in Part V for examples of client-related red flags.

(ii) Red flags in the services provided – are the services risky?

Some services that are the “bread and butter” of a lawyer’s work are sought after by those seeking to launder money, as these services facilitate money laundering through, for example, creating structures in which money can be concealed (e.g., complicated company and trust structures), or providing excuses for depositing money into client accounts⁴⁵ (e.g., real estate transactions).

Criminals might try to misuse client accounts to convert the cash proceeds of crime into less suspicious assets or to swap “dirty money” for “clean money”. Attempts to misuse client accounts might occur in, for example, the case of ‘aborted transactions’ – criminals may avoid suspicion by appearing to conduct a purported legitimate transaction that, for one reason or another, collapses before completion, but after the transfer of illegitimate funds into a lawyer’s client account. It may be difficult to ascertain whether an aborted transaction was legitimate. Look out for circumstances where the client: (i) tells you that funds are coming from one source and at the last minute changes the source of funds; or (ii) asks you to send money received into your client account back to its source, to a third party or multiple recipients, sometimes according to the direction of a third party (in order to conceal the identity of the real criminal client). Remember that you should only handle clients’ money in connection with underlying legal work. If a client is eager to transfer money into your client account at the very outset of instructing you this should raise a red flag – make sure that you have had enough time to conduct CDD and establish the nature and purposes of a transaction before you share client account details with a client.

Please refer to case study 5 in Part V for examples of client account-related red flags.

Law enforcement authorities believe that the purchase of real estate is a common method for disposing of 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 funds.

Please refer to case studies 6, 7 and 8 in Part V for examples of real estate-related red flags.

The company and trust structures may be exploited by criminals who wish to retain control over criminally derived assets while creating impediments to law enforcement agencies in tracing the origin and ownership of assets. Criminals will often seek to have

lawyers create companies and trusts, as well as be involved in the management of companies and trusts, to provide greater respectability and legitimacy to the entities and their activities. The trusts typically involve a settlor or trustor (who creates the trust and funds it with his or her property), assets being transferred into a trust, one or more trustees (who are given responsibility for safeguarding the assets and making distributions pursuant to the trust document), and one or more beneficiaries (to whom distributions of income or underlying assets can or must be made).

In some countries, a lawyer may be prohibited from acting as a trustee or as a company director. In countries where this is permitted, there are differing rules as to whether that lawyer can also provide external legal advice or otherwise act for the company or trust. Where such rules exist, funds relating to activities of the company or trust are prevented from going through client accounts. Some countries strictly regulate who can form and manage companies and trusts while other jurisdictions have no, or comparatively lax, laws regulating these issues.

Shell companies are business or corporate entities that do not have any business activities or recognisable assets themselves. They may be used for legitimate purposes such as serving as transaction vehicles. However, they are also an easy and inexpensive way to disguise beneficial ownership and the flow of illegitimate funds and so are attractive to criminals engaged in money laundering. You should be suspicious if a client engages your services only in connection with the routine aspects of forming an entity, without seeking legal advice on the appropriateness of the company structure and related matters. In jurisdictions where members of the public may register companies themselves with the company register, this may indicate that they are seeking to add respectability to the creation of the shell company.

Please refer to case study 1, 9 and 10 in Part V for examples of company and trust structure-related red flags.

Litigation is not an activity covered by the Recommendations, i.e., it is not in the list in Recommendation 22(d) and does not trigger an obligation to conduct CDD or file an STR. However, in the English Court of Appeal case of *Bowman v Fels*,⁴⁶ it was held that while genuine litigation should be exempt from reporting suspicions of money laundering to the U.K. National Criminal Intelligence Service (predecessor to the National Crime Agency), such exemption should not extend to sham litigation, which is an abuse of the court's processes (the case of *Bowman v Fels* should be understood in the context of the English approach to AML legislation that may not apply in other countries)⁴⁷. Litigation may constitute *sham litigation* if the subject of the dispute is fabricated (e.g., if there is no actual claim and the litigation is simply a pretext for transferring the proceeds of crime from one entity to another possibly via a client account) or if the subject of the litigation is a contract relating to criminal activity that a court would not enforce.

Please refer to case study 11 in Part V for examples of litigation-related red flags.

iii. Red flags relating to our clients' funds

The third major source of red flag indicators that lawyers should be aware of are the funds received from clients in connection with transactions and legal proceedings.

Lawyers should consider whether there is anything unusual about the amount of funds involved, their source or the mode of payment used by the client.

Size of funds	Source of funds	Mode of payment
<p>There is no legitimate explanation for:</p> <ul style="list-style-type: none"> • a disproportionate amount of private funding, bearer cheques or cash (consider individual's socio-economic, or company's economic, profile); • a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company; • receipt by the company of an injection of capital or assets that is high in comparison with the business, size or market value of the company performing; • an excessively high or low price attached to securities being transferred; • a large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, the activity of the client or its group companies; or • the client or third party contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly. 	<p>The source of funds is unusual because:</p> <ul style="list-style-type: none"> • third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation; • funds are received from or sent to a foreign country when there is no apparent connection between the country and the client; • funds are received from or sent to higher-risk countries; • the client is using multiple bank accounts or foreign accounts without good reason; • private expenditure is funded by a company, business or government; or • the collateral being provided for the transaction is currently located in a higher-risk country. 	<ul style="list-style-type: none"> • The asset is purchased with cash and then rapidly used as collateral for a loan. <p>There is no legitimate explanation for:</p> <ul style="list-style-type: none"> • an unusually short repayment period having been set; • mortgages being repeatedly repaid significantly prior to the initially agreed maturity date; or • finance being provided by a lender, either a natural or legal person, other than a credit institution.

Table 5:
Summary of fund risk profiles

Please refer to case studies 12 and 13 in Part V for examples of client funds-related red flags.

(iv) Red flags relating to the client's choice of lawyer

Lawyers should tread with caution whenever clients are instructing them from a distance about transactions without legitimate reason for doing so. Other red flags relating to the client's choice of lawyer include:

- lawyers being engaged although they lack competence in the relevant area of law or experience in providing services in complicated or especially large transactions;
- a client being prepared to pay substantially higher fees than usual, without good reason;
- a client changing legal advisors a number of times within a short span of time;
- engagement of multiple legal advisers without good reason; and
- another lawyer refusing to enter into, or termination of, a relationship with the client.

If an instruction is “too good to be true” then maybe it is!

Please refer to case study 14 in Part V for examples of red flags related to the client's choice of lawyer.

C. Investigating red flags thoroughly

Where information may be difficult to obtain, you should still satisfy yourself that there is no money laundering, terrorist financing or illegal activity involved. You should not avoid seeking clarification in the interest of expediency.

Please refer to case study 15 in Part V for an example of investigating red flags thoroughly.

D. What to do when red flags lead lawyers to believe that money laundering or terrorist financing is at issue

(i) Making an STR and avoiding tipping-off

Lawyers who suspect that their clients are involved, or another party to the clients' transaction is using or is involved, with the proceeds of criminal or terrorist activity should, where required, make an STR with the relevant FIU and even if not required, should consider making a report unless filing such a report would violate the rules of lawyer-client privilege, confidentiality and ethics in the relevant country as it would in some jurisdictions. The decision to make an STR or other form of report may come before or after conducting CDD.

Assuming the jurisdiction's rules require making an STR, the lawyer making the report should not disclose to any person that an STR or related information have been shared with the authorities. This is to avoid tipping off and impeding the investigations that are carried out by the FIU or enforcement authorities. FATF guidance clarifies that if a lawyer seeks to dissuade a client from engaging in an illegal activity, this should not amount to tipping off the client.⁴⁸ Disclosure is also likely to be permitted where it would not prejudice any potential investigation. National laws and regulations should be consulted to verify the position in the relevant jurisdiction. After the making of an STR, the lawyer may be prohibited by applicable law from continuing to act with respect to a reported transaction until consent is received from the FIU or applicable waiting periods have elapsed.

(ii) Ceasing to Act

Irrespective of whether a lawyer is required to make an STR or chooses to make a report (and subject to tipping-off rules where they apply), a lawyer needs to consider carefully whether (and if so how) to cease acting for a client who the lawyer suspects is laundering money. This is often a difficult judgement call, especially for small firms and in situations where the client is powerful and/or the lawyer needs as many clients as possible. However, the ethical standards of the profession must prevail and as a profession we must guard against misuse by criminals even if this has financial consequences.

It would be improper, however, if lawyers collectively refused – as some banks have done – to decline to represent certain categories of clients because they initially present some risk and require enhanced CDD. All client situations should be evaluated on a case-by-case basis. Lawyers should be mindful of the UN Basic Principles on the Role of Lawyers (1990), the first principle of which is that “*All persons are entitled to call upon the assistance of a lawyer of their choice to protect and establish their rights and to defend them in all stages of criminal proceedings.*” This does not mean, however, that lawyers should act for clients who are seeking to launder money and misuse the provision of legal services to assist in the laundering of money.

(iii) When in doubt?

Lawyers can be put in very difficult situations with regard to their obligations for AML and terrorist financing. In larger firms there may be compliance officers and several other partners to whom a lawyer can turn. In smaller firms and for sole practitioners this is not so straightforward. Lawyers should always carefully consider taking advice from colleagues and/or approaching their bar associations and law societies for help and guidance in difficult situations.

When in doubt, lawyers should also consider if there is an appropriate body that can grant consent to continue acting for the client.

Please refer to case study 16 in Part V for an example of consent sought by a law firm.

V. Case Studies

In this Part V, we will look at various “real life” situations where lawyers could be unwittingly used in the furtherance of the criminal activities of clients. Some of the case studies are loosely based on real life examples that various bar associations have become aware of; others are drawn from training programmes that have been developed by bar associations and individual law firms. Obviously, these case studies are by no means exhaustive of the issues that might give rise to suspicions on behalf of a lawyer and are merely included to indicate the types of situations that lawyers should be on the lookout for and, equally importantly, should be training all the lawyers in their practice to be aware of and alert to.

A. Client risks

1. The importance of independent verification of clients – really “know your clients”

A lawyer agreed to act for company A, which was the holding company of several operating subsidiaries on a sale of those subsidiaries. A was owned by an individual, Mr X. During the course of advising A, the lawyer saw a press report that highlighted the existence of litigation brought in another country against some of A's subsidiaries. Upon searching for publicly available court documentation, the lawyer discovered that a court appointed insolvency practitioner of another company, B, which until recently was owned by Mr X, had brought claims against some of A's subsidiaries for the return of certain assets. The claim asserted that in the run-up to the insolvency of B, assets were transferred to A's subsidiaries for the purposes of putting the assets beyond the reach of the creditors of B. It later transpired that Mr. X was also the subject of claims as he had directed the asset transfers.

The lawyer questioned company A about the litigation. Company A indicated that: (i) its subsidiaries were defending it and inundated the lawyer with documentation that demonstrated that there was a good defence; and (ii) it was not itself involved in any proceedings. The lawyer continued on the condition that statements were made in the disclosure letter regarding the litigation. Company A put significant pressure on the lawyer to keep the disclosure to a minimum, based on the defence documentation provided, and given the urgent nature of the proposed deal.

It was subsequently discovered that the defence documents provided to the lawyer were falsified and A's subsidiaries had received assets that had been improperly transferred. It appeared that the whole arrangement had been set up by Mr. X to prevent him from losing money as a result of the previous mismanagement of B.

Red flags:

Insolvency of another company with a common beneficial owner; claims made regarding asset transfers to the subsidiary; no mention of the issue by the client initially, followed by an over willingness to provide a lot of documentation; urgency in getting the deal done.

What can you do?

Seek verification of documents provided or request originals (in the circumstances the lawyer could have requested a court-stamped copy of the relevant documents); talk to the insolvency practitioner (possibly only after seeking the client's consent).

2. Politically exposed person

A senior lawyer in a law firm was approached to act for an individual in the purchase of a football club. The client was a high net worth individual who had made his fortune in the mining industry in an emerging market. He then moved into politics before choosing to pursue some business interests. Due diligence was carried out on the individual that included searches of a subscriber database, which highlighted that the individual was a PEP. Accordingly, the issue of source of funds was raised. Upon enquiry, the individual responded that the acquisition was to be funded out of the proceeds of sale of one of his former mining businesses.

The law firm accepted the engagement. During the course of advising on the proposed investment, a junior lawyer highlighted a recent news article to the senior lawyer. In the article the client had been accused of bribery in obtaining the mining concessions on which his fortune was built. Further, during his time in politics, the client was implicated in an expenses scandal, although a parliamentary investigation found him not guilty of these accusations.

The senior lawyer raised this issue with the client and the client explained that the charges were politically motivated and had been made up by an opponent to discredit him. The lawyer was aware that this sort of thing happened in emerging markets, but raised it with his money laundering reporting officer. Upon advice from the money laundering reporting officer, the law firm did not proceed to act for the client.

A couple of years later, a foreign court convicted the client of bribery and corruption both in connection with the mining rights and the expenses investigation (which, as it turned out, had initially been led by the client's close associate) and sought to freeze the individual's assets. It also transpired that there were a number of press articles alleging that the result of the parliamentary enquiry had not been fair given the links between the client and the person leading it.

Red flags:

Mining and natural resource extraction in emerging markets are often high risk and associated with corruption. PEPs are recognised as needing more careful and thorough due diligence.

What can you do?

Carry out independent research into matters raising suspicion – in the case study, the lawyer carried out relatively little independent research into the circumstances of the acquisition of the licenses and the individuals who were leading the parliamentary investigation; explanations were taken at face value without further enquiry and it was fortunate that the individual spoke to the money laundering reporting officer.

3. Risky clients

A new client, A, drops into Law Firm B's office in person, without an appointment and requests legal advice in relation to setting up a business in Law Firm B's jurisdiction. The person is from Country X (an African country) and has a company incorporated there. A states that he has obtained funding from Company C which is located in Country Y (a Middle Eastern country) and the funding of €1 million will be wired from a Swiss bank account. Client A says that he has lost his passport and is in the process of applying for a new one. He produces a photocopy of some temporary papers in the meantime and agrees to send copies of the new passport when it is issued. He also produces the investment agreement with Company C – this agreement looks too basic to have been drafted by a lawyer.

The lawyer tries to perform an Internet search on A and A's company, but there is no information available.

Red flags:

Client and the investor are both located in high-risk countries; funding is arriving from a Swiss bank account; client has no proper identification papers; there is no information available on the client and his business; purported legal documentation is too simplistic for the relevant transaction; client's connection with the jurisdiction is unclear.

What can you do?

Conduct enhanced CDD on the client and the other counterparties to the transaction to identify who they are and ascertain the source of funds. Lawyers should decline to act where there are multiple high-risk factors and consider if a reporting obligation arises in their jurisdiction.

4. Transactions involving unexpected criminal offences

Lawyers should be aware that there may be criminal offences imposed for certain areas of law that one would not ordinarily expect. The potential criminal conduct may not be readily apparent to the advising lawyer in the first instance. Lawyers should be vigilant to this possibility when advising on transactions.

Mr. A, a high net worth individual who recently started investing in properties, makes an appointment with Lawyer B to discuss a dispute about a property Mr. A owns. The property is residential and divided into apartments that are leased to various tenants. Mr. A had bought 50% of the interest in the property from a company owned by Trust D (which Mr. A had settled for the benefit of his family members). The purchase agreement was only intended to transfer beneficial interest in the property to Mr. A, but was incorrectly drafted, resulting in the legal interest of the property being transferred as well. Mr. A purchased the property interest at slightly below market price.

One of the tenants has now complained that the transfer of interest to Mr. A has breached his rights under Legislation X. Legislation X requires a landlord to notify his tenant if he intends to sell the property, and give the tenant a first right to purchase the property – breach of Legislation X is a potential criminal offence.

In addition to advising Mr. A on the dispute, Lawyer B also advises Mr. A that he may have potentially committed a money-laundering offence. Although the criminal offence (if any) would be committed by the seller, Mr. A may have derived a "benefit" from the criminal offence. If Legislation X had been complied with and the property purchased by the tenant at market value, the difference in value between Mr. A's purchase price and the market value might be a "benefit" that constitutes proceeds of crime.

Red flags:

Dispute or a transaction involving a technical regulatory regime that has an unexpected potential criminal offence; parties derived some form of benefit from the transaction.

What can you do?

Where a potential criminal offence may have taken place, analyse if a criminal offence has inadvertently been committed and if a "benefit" was derived from the transaction. If so, the "benefit" may be the proceeds of crime and lawyers should consider if their clients will need to make an STR.

B. Attempts to misuse client accounts

5. Aborted transactions and transfer of funds without underlying legal work

A law firm was approached by a new client with instructions to assist on a number of asset purchases. The client was dealing with a junior lawyer at the firm who, at the request of the client, supplied her with the account details of the firm before completing CDD on the client or entering into an engagement letter with her. The client did not give any further instructions following the deposit of funds. Subsequently, the client explained that she no longer intended to purchase the relevant assets and asked for the deposited money to be provided to a third party, rather than returned to her personal account.

Red flags:

Once funds received in client account, the transaction is aborted. Client requests that deposited funds are sent to a third party, rather than returned to it. The client is avoiding personal contact without good reason.

What can you do?

Do not allow clients to deposit funds in a client until you carry out CDD, establish the purpose of the transaction and satisfy yourself that there are no money laundering risks attaching to the funds. Alternatively, do not send the funds to the third party but instead return them to the original source.

C. Property purchases

6. Investment of proceeds in real estate

Criminals may be aware that lawyers cannot directly handle large sums of money. However, criminals will still seek to use the purchase of real property as a means of depositing cash obtained from criminal activity. This is seen as part of the layering process of laundering whereby the property purchase is wholly or predominantly funded through private means rather than through a mortgage or loan.

A client deposited the total purchase price, in cash, with his lawyers at the very outset of the engagement with the law firm and well before final agreement was reached on the purchase price for the property. The lawyers' CDD indicated that the sum that was deposited was a large amount relative to the client's employment income. The purchase of the property went ahead for a sum smaller than that deposited and the remaining funds were returned to a third party indicated by the client. It subsequently turned out that the funds deposited were the proceeds of crime.

Red flags:

Unusual manner of execution – the deposit of funds for the purchase price occurred unusually early in the transaction and before the purchase price had been agreed between the parties. Amount being deposited large compared to client's modest income. Surplus funds were deposited. Remaining funds remitted to a third party, not to the client.

What can you do?

Lawyers should be wary of clients who are ready to deposit funds into their client account at the very outset of an engagement. When lawyers have reason to believe that the funds the client has deposited are a large amount compared to their socio-economic profile, lawyers should consider conducting enhanced verification of the source of funds.

7. Back-to-back sales

Quick successive sales of property, either with or without a mortgage, enable criminals to inflate the value of a property, thereby justifying the injection of further criminal funds into the purchase chain and enabling value to be transferred to other parts of an organised crime group or re-invested within the group.

Mr. A, a lawyer, was approached by an individual to act on the purchase of a number of real estate properties. The client claimed to be funding the purchases from previous real estate sales and presented a bank cheque to pay the purchase price. Shortly afterwards, the client instructed Mr. B, also a lawyer but who was not connected to Mr. A and unaware of the client's previous instructions to Mr. A, to re-sell the properties at a higher price.

It transpired that the properties were being bought from, and then sold to, people that the client knew in order to launder the proceeds of crime.

Red flags:

Back to back property transactions, which were out of sync with normal market dynamics - the purported value of each property rapidly increased with each subsequent transaction (despite the short period of time in between transactions). Client changes legal advisor a number of times in a short time period for no apparent reason.

What can you do?

In the circumstances, the lawyers ought to have made further enquiries about the client's source of funds and the motivation for the transactions.

8. Non-clients transferring proceeds into client accounts

Lawyers acting for sellers of property are not required to carry out CDD on the purchasers because this is completed by the lawyers acting for the purchaser. However, if the proceeds are transferred directly to the law firm's client accounts without prior authorisation, the funds could be 'cleaned' and there could be a risk of the law firm committing a money laundering offence.

Law Firm A acts for the seller of a property. The purchaser is located in country X, which is an emerging market. The purchaser transfers the purchase price to Law Firm A's client account rather than the seller's bank account without first informing Law Firm A. The purchase price was paid entirely in cash and no bank financing was taken out.

The senior lawyer advising on the transaction raises this issue with the firm's money laundering reporting officer. Law Firm A decides that it must make an STR to the FIU and temporarily hold on to the funds. It cannot return the funds to the purchaser as this would 'clean' the funds. Law Firm A also needs to consider whether it can inform its own client of the situation as this could amount to "tipping off" and prejudice the investigation. Law Firm A may also need to consider how it suspends the transaction without "tipping off" the purchaser.

Red flags:

The purchase price is paid entirely in cash and transferred to the law firm's client account rather than the purchaser's bank account; purchaser is located in a high risk jurisdiction; purchaser did not seek prior approval for the transfer.

What can you do?

Where funds are transferred directly into client account without any prior notice, lawyers should not immediately return the funds. The facts will need to be investigated further and lawyers should consider if any reporting obligations arise. Lawyers should seek guidance when in doubt.

D. Trust structures

9. Creation of a private trust to disguise proceeds of crime

In Country A, an elderly female national from Country B with the appropriate visa, consults with a trust lawyer. She found the lawyer's name through an Internet search. She asks the lawyer to prepare a trust to handle an inheritance she has in Country B; the trust will be funded via wire transfer from Country B into the law firm's client account in Country A. Country B is a country that scores lowly on Transparency International's Corruption Perceptions Index and is subject to various sanctions programs. She will be the trustee and her children in Country A will be beneficiaries. She asks for a memorandum on tax issues and filing requirements. She also wants an introduction to a certified public accountant and to a banker in Country A.

The type of trust requested by the client is a normal structure familiar to most trust lawyers. The goal of the client appears to be asset management for the benefit of the client's children. While the tax consequences may be complex, the plan itself is relatively typical.

The lawyer agrees to act for the client.

Red flags:

Client is not well known to the lawyer nor does the source of the connection add any comfort. Client comes from Country B, a jurisdiction where there is geographic risk. The funds are being wired from outside of the lawyer's jurisdiction (Country A) into the lawyer's trust fund account. Can the lawyer rely on the CDD being conducted by the paying bank?

What can you do?

Here, as is true with other case studies, the obligations of the lawyer will depend on the jurisdiction where the lawyer practices. Where the lawyer has a STR regime, the lawyer must determine if the facts justify a report. Where such a regime is not in place, the lawyer must consider the applicable legal and ethical responsibilities. Here, the presence of geographic risk, client risk and service risk should steer the lawyer away from representation.

10. Management of an existing trust that may contain criminal property

A client comes into the trust lawyer's office to hire the lawyer in connection with terminating a trust established by his deceased mother, under which trust the client is the sole beneficiary. When asked about the source of the funds in his mother's trust, the client is evasive. When pressed, the client informs the lawyer that he suspects that a majority of the trust estate was the product of a decades-long fraud and scheme of embezzlement perpetrated by his mother against her former employer's business and personal assets as a result of her close personal relationship with the employer. The client asks the lawyer for advice regarding the disposition of the assets in the trust and the client's legal obligations to the former employer.

Red flags:

Client is not well known to the lawyer. The funds in the trust may be the proceeds of crime.

What can you do?

Again, the obligations of the lawyer will depend on the jurisdiction where the lawyer practices. Where the lawyer has an STR regime, the lawyer must determine if the facts justify a report. Where such a regime is not in place, the lawyer must consider the applicable legal and ethical responsibilities. Here, the lawyer may properly decide to advise the client regarding the rights of the defrauded employer and the impact of those rights on the trust assets (and on the client to whom the trust assets are to pass).

E. Fictitious claims

11. Unexpectedly short procedure

A foreign company retained a lawyer to file a claim against another foreign company. The defendant did not contest the claim so that a default judgment was entered. The defendant immediately paid the sum into the law firm's client account. The defendant even paid the amount in question twice - when the second payment was made, the defendant informed that the second payment was made erroneously and asked the law firm to forward the funds to another subsidiary of the defendant company.

Red flags:

Two foreign companies without obvious connection to the place of litigation.

Very short procedure – defendant does not contest default judgment. Unusual error in paying large sum twice and then request to forward funds to a different entity than that which made the payment.

What can you do?

The lawyer should have been alerted by the ease with which the litigation was settled. It may be difficult to establish whether one is dealing with fictitious claims, but lawyers must keep an eye out where matters seem to be proceeding too smoothly.

Whenever clients ask that payments made in error be returned to third parties, lawyers ought to question why they are requesting this.

F. Sources of funds

12. Size of funds provided are disproportionate or inexplicable

When there has been a significant increase in capital for a recently formed entity, successive contributions over a short period of time have been made to the same entity or contributions have been made that are high in comparison with the business, size or market value of the entity, a lawyer should ascertain the reasons behind these increases.

A lawyer is acting for a company from an emerging market that is trying to make an IPO. As a result of concerns over the financial viability of the company and a potentially messy dispute over ownership of the company, the company is struggling to make the IPO a success. At the last minute a previously unknown wealthy investor comes along. In reality, arrangements had been made between representatives of the company and the investor to promote the investment and that the money being offered by the wealthy investor was actually the company's money. The individual received the money plus an incentive payment in order to assist.

Red flags:

Unexplained financing arrangements. Involvement of a high risk jurisdiction. Appearance of sudden willing investor when previous interest was lacking.

What can you do?

When faced with a sudden willing investor or other source of funds not previously available, consider conducting measures akin to CDD to verify the identity of the 'source of funds' and the reasons for their sudden appearance in the transaction.

G. Choice of lawyer

13. Failure to consider who controls the client

ABC Ltd. “passed” a law firm’s CDD/client process and has provided confirmation/documentation indicating who ultimately owns the client. During the course of the transaction, the lead partner becomes less involved and starts to hand over work streams to her lead associate (as it would be valuable experience for this individual who is looking for partnership). A previously unidentified individual starts to attend meetings and appears to be leading many of the discussions/decisions on behalf of the client.

The client is in fact ultimately controlled by the individual’s father who turns out to be subject to an arrest warrant in another country. The purpose of the deal was to put assets beyond the reach of law enforcement.

Red flags:

Documented ultimate beneficial owner owns shares on behalf of another or takes instructions from another individual. Other related red flags could include the client requesting that an apparently unrelated individual is copied into all emails or attends meetings, without their involvement being explained.

What can you do?

Most jurisdictions allow lawyers to take instructions from third parties only in very limited circumstances. However, as in the scenario in this case study, sometimes a third party will be dictating the actions of the client on record in more overt ways. Understanding the motives of a client will be important in establishing whether the client really is the instructing party.

14. Instructions from overseas clients

Lawyer A is an employment specialist and has acted for Client B in relation to some employment matters. After a few months, Client B contacts Lawyer A, requesting that he act for a friend, C, in relation to the purchase of some high-value properties.

Friend C lives in another country, which is an emerging market, and does not intend to travel to visit the properties being purchased. Friend C would like the purchases to be completed as soon as possible and he assures Lawyer A that financing will not hold the time table up as no bank loans will be required. He also promises to pay Lawyer A an extra fee if the purchases are completed by a certain date.

Red flags:

Lawyer being asked to advise on an area of law in which he lacks expertise; client is not visiting the properties despite the high value of the transaction, client paying large value of funds in cash; client promises to pay extra fees for speedily completing transaction; client will be transferring funds from a jurisdiction where there are difficulties ascertaining AML compliance.

What can you do?

Perform CDD on the prospective client. Where there are high risk indicators, lawyers should seek senior approval before accepting engagement and determine the source of funds. Where such cases are referrals from previous clients, lawyers may also need to review the previous transactions with such clients for AML risks.

H. Investigating red flags

15. Performing thorough due diligence

A long standing client was acquiring a middle eastern construction entity. On performing due diligence a number of contracts and payments were noted for services from consultant companies. It was very difficult to establish the identity of the individual consultants or establish the exact nature of the services provided beyond generic descriptions.

While it may have been expedient to stop at the generic descriptions, the legal advisers involved advised their client that more substantive answers were required from the seller concerning the consultant contracts and fees paid under those contracts. On a more detailed analysis of the consultant entities it became apparent that some were linked to individuals known to be part of the government organisation responsible for licensing and permits and that the consultant fees were in fact bribes. Accordingly, the lawyers advised their client that the contracts the entity they were purchasing had won may represent the proceeds of crime (bribery).

Red flags:

Involvement of a higher-risk jurisdiction. Difficulty in obtaining satisfactory information as to services being provided by the target company.

What can you do?

Lawyers must remember that they have an obligation to satisfy themselves that all issues involved in a transaction are legal. Resist the temptation to avoid seeking further clarification of matters in the interests of expediency.

Note also that in the circumstances seeking further clarification was part of the lawyer's duty of care to its client – had the lawyer not sought further clarification as to the services being provided by the target, the client would have unwittingly invested in an entity involved in criminal activities. Consider whether there is an obligation under local law to make an STR even when the client abandons the transaction.

I. Reacting to red flags

The following case study illustrates a situation in which lawyers were alerted by red flag indicators and took appropriate action in response to their concerns.

16. Requesting consent to proceed with a transaction from the relevant authority when in doubt

An established London jewellers and longstanding client was in the process of being bought by a private equity entity. As part of the due diligence, queries were raised regarding the insurance arrangements for the movement of high value goods between stores and ad-hoc VIP viewings across the world. On further probing it transpired that the client was, on occasion, sending its sales staff to offices and VIPs wearing the jewellery that was to be offered for sale. This meant that the client did not pay the relevant import duties in those countries, a potential criminal offence resulting in the company being tainted by the proceeds of crime. The client informed the law firm that the practice was one of convenience and speed rather than a deliberate attempt to avoid taxes and only occurred on a limited number of occasions.

Consent was requested by the law firm from the Serious Organised Crime Agency (the predecessor of the U.K.'s National Crime Agency, the U.K. body tasked with overseeing AML compliance) to proceed with the sale of the business.

Red flags:

Unusual practice in relation to the transport of jewellery, avoidance of import duties.

What can you do?

Pay attention to the information discovered during CDD processes and during the business relationship with the client.

If a lawyer's suspicions are raised, he or she must ask further questions and consider whether there is an appropriate body which can grant consent to his or her further engagement with the client. The lawyer must also consider if he or she should advise the client to self-report the violation.

VI. Glossary and Further Resources

VI. Glossary and Further Resources

ABA	American Bar Association
AML	Anti-Money Laundering / Countering the Financing of Terrorism (also used for Combating the financing of terrorism)
CCBE	Council of Bars and Law Societies of Europe
CDD	Customer Due Diligence
FATF	Financial Action Task Force, intergovernmental body that develops and promotes policies to combat money laundering and terrorist financing
FIU	Financial Intelligence Unit
IBA	International Bar Association
PEP	Politically Exposed Person

Recommendations	<p>“International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations” published by FATF; references to 40 Recommendations are references to the 2012 revision of the Recommendations currently in force available at www.fatf-gafi.org/recommendations</p>
STR	Suspicious Transaction Report
SRO	Self-Regulating Organisation
ABA’s International Law Section’s Anti-Money Laundering Committee	http://apps.americanbar.org/dch/committee.cfm?com=IC700500
ABA’s Task Force on the Gatekeeper Regulation and the Profession	http://www.americanbar.org/groups/criminal_justice/gatekeeper.html
ABA, Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing (2010)	http://www.americanbar.org/content/dam/aba/migrated/leadership/2010/annual/pdfs/116.authcheckdam.pdf .
CCBE Money Laundering Committee	http://www.ccbe.eu/index.php?id=94&id_comite=20&L=0

CCBE Position papers and resources

http://www.ccbe.eu/index.php?id=94&id_comite=20&L=0.

Working Document of the Commission of the European Communities, 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 (2006)

http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/commission_report_la1_1183722383.pdf.

FATF

<http://fatf-gafi.org>

IBA Anti-Money Laundering Forum

<http://www.anti-moneylaundering.org/>

IBA's AML resources

<http://www.anti-moneylaundering.org/ReadingRoom.aspx>.

Law Society of England and Wales – AML Toolkit

<http://www.lawsociety.org.uk/advice/anti-money-laundering/>

Endnotes

- 1 A United National Office on Drugs and Crime 2011 report estimated that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or US\$ 1.6 trillion) being laundered:
http://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html
- 2 OECD. "Money Laundering Awareness Handbook for Tax Examiners And Tax Auditors, Organisation For Economic Co-Operation and Development". 2009. Available at *www.oecd.org/dataoecd/61/17/43841099.pdf*
- 3 The mandate of 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. The FATF 40 Recommendations 2012 are available at *www.fatf-gafi.org/recommendations*
- 4 Neil Jensen, Cheong-Ann Png, "Implementation of the FATF 40+9 Recommendations: A perspective from developing countries", *Journal of Money Laundering Control*, 14.2 (2011): 110 – 120
- 5 A ninth special recommendation was added in October 2004 to address cash courier related concerns.
- 6 The term "lawyers" is used throughout this Guide to refer to all legal professionals, including civil law notaries.
- 7 Broadly, the 40 Recommendations define DFNBP as: legal professionals, casinos, real estate agents, dealers in precious metals and stones and trust and company service providers (for further detail, please refer to Part III).
- 8 Shepherd, Kevin L. "Guardians at the Gate: The Gatekeeper Initiative and the Risk-based Approach for Transactional Lawyers." *Real Property, Trust & Estate Law Journal* 43.4 (2009).
- 9 "Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals" (FATF, 2013), available at: *http://www.fatf-gafi.org/topics/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html*
- 10 See also Part VI (Further Resources) of this Guide for a list of electronically available AML resources.
- 11 Sources of information:
ABA website (*http://www.americanbar.org*);
CCBE website (*http://www.ccbe.edu*); and
IBA website (*http://www.anti-moneylaundering.org/*)
- 12 Such materials include the *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing*, 2010. Available at *http://www.americanbar.org/content/dam/aba/migrated/leadership/2010/annual/pdfs/116_authcheckdam.pdf*
For additional items, see Laurel S. Terry, "U.S. Legal Profession Efforts to Combat Money Laundering & Terrorist Financing". (2014/2015). 59(3) N.Y.L.S. L.Rev. (Forthcoming).
- 13 Available at *http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/commission_report_la1_1183722383.pdf*

- 14 This package includes a dedicated AML website (<http://www.lawsociety.org.uk/advice/anti-money-laundering/>), a bi-monthly AML newsletter and training events and country-wide national networking groups for money laundering reporting officers.
- 15 Information provided by the Law Society of England and Wales.
- 16 For instance, transactions may involve highly technical and regulated regimes, where certain breaches may result in criminal sanctions (e.g. breaches of certain environmental laws in the UK may have criminal consequences). Due to the technical and complex nature of the industry, the client may be unaware that it has committed such a breach. See Section B of Part IV and case study 4 of Part V for more discussion. Lawyers will need to pay particular attention to AML risks when advising on such transactions as any proceeds generated from such offences would be proceeds of “crime” thereby possibly triggering reporting obligations.
- 17 Tatsu Katayama, Anderson Mori and Tomotsune. “Never to Whistleblow – JFBA’s Approach: When to whistle-blow – a lawyer’s guide.” IBA Annual Conference, Dubai, November 2011. Available at <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=0EE69B97-7740-4EF9-ADE7-9D4FD3A85222>
- 18 Lawyers in jurisdictions that are party to other international conventions must be aware of AML offences thereunder. For example, the 1988 Vienna Convention and the Palermo Convention 2000, require countries to criminalise the concealment, or changing the true nature, source or location of, property that is derived from drug trafficking. For more detail see Paul Alan Schott, *Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism*, World Bank Publications, 2006; Jean-François Thony “Money laundering and terrorism financing: an overview.” *International Monetary Fund* 1 (2002).
- 19 The glossary to the 40 Recommendations clarifies that this refers to sole legal practitioners and partners, or employed legal professionals within professional firms. The term does not capture “internal” (i.e., in-house) professionals that are employees of other types of businesses, nor legal professionals working for government agencies
- 20 For an examination of various definitions of PEPs, see Kim-Kwang Raymond Choo, (2008) “Politically exposed persons (PEPs): risks and mitigation”, *Journal of Money Laundering Control*, Vol. 11 Iss: 4, pp.371 – 387
- 21 A list of such countries can be found at: <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/>. These include Iran, the Democratic People’s Republic of Korea, Algeria, Ecuador, Indonesia and Myanmar.
- 22 European Commission, Commission Directive 2001/97/EC. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0097>

- 23 European Commission, “Proposal for a directive of the European parliament and of the council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.” Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0045&from=EN>
- 24 Lawyers do not fall under the Bank Secrecy Act (31 USC §§5311) which applies to “financial institutions”. However, they are subject to prohibitions in regulations issued by the Office of Foreign Assets Control. Information from Anti-money Laundering Forum, http://www.anti-moneylaunders.org/northamerica/United_States_of_America.aspx
- 25 See Formal Opinion 463 (May 2013), ABA Standing Committee on Ethics and Professional Responsibility.
- 26 18 U.S. Code § 1957 and 31 U.S.C. §§5331-32.
- 27 U.S. Department of the Treasury, Sanctions Program and Country Information. <http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>
- 28 “Risk Based Approach Guidance for Legal Professionals” (FATF, 2008). defines a self-regulatory organization as “A body that represents a profession (e.g., lawyers, notaries, other independent legal professionals or accountants), and which is made up of member professionals or a majority thereof, has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions.”
- 29 Blake Bryant Goodsell. “Muted Advocacy: Money Laundering and the Attorney-Client Relationship in a Post 9/11 World.” *J. Legal Prof.* 34 (2009): 211.
- 30 Karin Svedberg Helgesson. “Public-Private Partners Against Crime: Governance, Surveillance and the Limits of Corporate Accountability.” *Surveillance & Society* 8.4 (2011).
- 31 Note that in many jurisdictions confidentiality is an ethics concept while professional secrecy and legal professional privilege are evidentiary concepts.
- 32 Proceeds of Crime Act, section 330(6)
- 33 International Bar Association. “Commentary on IBA International Principles on Conduct for the Legal Profession.” 28 May 2011
- 34 CCBE. “Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers”. 2013. Available at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_CCBE_CoCpdf1_1382973057.pdf
- 35 *Supra* n 25.
- 36 American Bar Association, “Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing”. Available at http://www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_taskforce_gtfgoodpracticesguidance.authcheckdam.pdf
- 37 Please see Section B of Part IV for a discussion of sham litigation. FATF refers to “sham litigation”, whereas a more accurate term is “fictitious claims”, as *bona fide* litigation is outside the scope of the Recommendations and the EU Directive. See also, Section A of Part II.
- 38 FATF Typologies Report 2013 available at <http://www.fatf-gafi.org/topics/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html>

- 39 *Supra* n 33.
- 40 For more information and examples of lawyers who have been involved in intentional money laundering, see David J Middleton and Michael Levi, “The role of solicitors in facilitating ‘Organised Crime’: Situational crime opportunities and their regulation,” *Crime, Law & Social Change* (2004) 42:123-161.
- 41 Available at :
<http://www.fatf-gafi.org/topics/fatfrecommendations/documents/riskbasedapproachguidanceforlegalprofessionals.html>
- 42 Source of information: Lawyer RBA Guidance
- 43 American Bar Association, “Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing”, 2010. Available at <http://www.americanbar.org/content/dam/aba/migrated/leadership/2010/annual/pdfs/116.authcheckdam.pdf>
 See also Kevin L. Shepherd, “The Gatekeeper Initiative and the Risk-Based Approach to Client Due Diligence,” (2012) *The Review of Banking and Financial Services* 28(4) 33-42.
- 44 Transparency International’s Corruption Perception Index is available at <http://www.transparency.org/research/cpi/overview>
 The World Bank produces Worldwide Governance Indicator reports for over 200 countries over 1996–2012 that are available for download at <http://info.worldbank.org/governance/wgi/index.aspx#countryReports>
- 45 According to FATF, client accounts can be susceptible to misuse by criminals in the context of money laundering and terrorist financing. In some jurisdictions, client accounts, i.e., segregated accounts in the name of lawyer or law firm into which client funds are placed, are referred to as “client trust accounts”.
- 46 [2005] EWCA Civ 226 available at www.bailii.org/ew/cases/EWCA/Civ/2005/226.html.
- 47 As indicated in endnote 38, FATF refers to “sham litigation”, whereas, a more accurate term is “fictitious claims” as *bona fide* litigation is outside the scope of the Recommendations and EU Directives.
- 48 Interpretative Note to Recommendation 23 (DNFBPs – Other Measures), FATF 40 Recommendations 2012.

Anti Money Laundering Report

May 2016

Contents

Foreword	3
Introduction	4
Summary of our findings	10
Money Laundering Reporting Officer	13
Policies	17
Client Due Diligence	21
Training and Awareness	27
Reporting	30
Suspicious Activity Reports	32
Record Keeping	35
Conclusion	37

Foreword

Paul Philip

Chief Executive



The proceeds of corruption and crime have no place in our economy and markets. As our report says, law firms are attractive to criminals because they are seen as adding legitimacy and credibility to transactions, and they do of course handle significant finance.

As the regulator of some 10,300 law firms and 170,000 solicitors in England and Wales, we are a supervisory authority with a key role in making sure law firms and their staff are meeting their anti money laundering obligations under our Code of Conduct and in legislation. We do that through raising awareness, through monitoring and through taking robust action when we identify a concern. As part of that, this report sets out the results of an intensive review of solicitors' anti money laundering compliance.

We share examples of both best and poor practice in our report in order to help firms – and I am pleased that the overall picture is positive. But neither we, nor the firms we regulate, can be complacent. It is important that public confidence is well placed and that solicitors are meeting the high professional standards we expect. Those standards have to be set independently in the public interest.

Against the backdrop of Government proposals to separate out regulation and representation in the legal sector, it is timely to remind ourselves that any perception of a conflict of interest will undermine public confidence. Although we operate independently, our status as part of the Law Society, which represents solicitors and their interests, is thrown into sharp relief in this difficult area. Truly independent regulation is all the more necessary as the need to fight corruption and money laundering becomes ever more important.

For us, preventing money laundering, with its connections to crime, corruption and terrorism, is a priority. The public, Government and the vast majority of the profession clearly agree with us.

A handwritten signature in black ink, which appears to read 'Paul Philip'. The signature is stylized and written in a cursive-like font.

Introduction

In September 2014, we announced our plan to undertake a thematic review of anti money laundering (AML) compliance by solicitors.¹ The principal aim was to gain knowledge and understanding of the AML compliance policies, procedures and controls implemented by a wide range of law firms, and determine how effectively firms were managing risks in this area. We also wanted to ensure that solicitors and their firms were fully aware of their statutory and regulatory obligations in relation to AML, and were up to date on forthcoming changes, such as the 4th Money Laundering Directive.

This report outlines what we found and also includes several examples of the good and poor practices that we encountered.

The AML thematic review builds on our previous work in this area. This report should be read together with our earlier publications ([see here](#)). Money laundering remains one of our priority risks for 2016², and this is not likely to change. We have produced a detailed overview of the risk which money laundering poses,³ two warning notices,⁴ and case studies illustrating practice risks.⁵

The aim of this report is to highlight the requirements of the Money Laundering Regulations 2007 (MLR), the Proceeds of Crime Act 2002 (PoCA), the Terrorism Act 2000 and the internal practices and procedures that can help solicitors and their staff to comply. This, in turn, will ensure that the legal profession plays its part in protecting itself, the public and society in general from the laundering of the proceeds of crime.

The key areas we discussed with firms were:

Money Laundering Reporting Officers (MLROs)

AML policies

Client due diligence (CDD)

AML training and awareness

Reporting

Suspicious Activity Reports (SARs)

Record keeping

These areas are covered in this report.

Why have we done this?

Money laundering is an essential tool of serious and organised crime and terrorism. Solicitors are respected professionals who regularly handle large numbers of financial and other transactions. Criminals wish to take advantage of this and in particular the credibility and legitimacy given by lawyer participation in transactions. Solicitors' firms are an attractive target for those wishing to launder the proceeds of crime, as has been highlighted by the Financial Action Task Force (FATF).⁶

1. [SRA steps up anti money laundering work](#), 8 September 2014

2. [SRA Risk Outlook 2015/16](#)

3. [Cleaning Up: Law Firms and the Risk of Money Laundering](#), November 2014

4. [Warning notice: Money laundering and terrorist financing](#) 8 December 2014 and [Money Laundering and terrorist financing - suspicious activity reports](#) 8 December 2014

5. Case studies: [Money laundering - inadequate systems and controls over the transfer of money](#)

6. [Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals](#), June 2013

Solicitors have obligations under the MLR and PoCA which are directed at minimising the laundering of the proceeds of crime. Aspects of this regime are technical and complex.

In addition, the SRA Code of Conduct 2011, specifically requires compliance with money laundering legislation.⁷

Finally, the 4th Anti Money Laundering Directive⁸ has been adopted and must be brought into force in European Union member states by 26 June 2017. It requires a number of changes to national AML regimes. These will impose greater demands on those in the legal profession in England & Wales who conduct business covered by the directive.

Internal Drivers

As a regulator and supervisory authority, we have a statutory duty under the MLR to effectively monitor legal professionals and their activities that fall under the regulations. We must take necessary measures to secure their compliance with them.⁹

We continue to receive a high number of reports regarding suspected money laundering and related activity. These reports are received from a wide variety of sources including the public, law firms, other regulators, law enforcement agencies and our own supervision and investigation of the profession. Each allegation is assessed on its facts before any further action is taken, which may include forensic investigation.

Money laundering is a serious crime and participation can result in severe penalties. Additionally, The Solicitors Disciplinary Tribunal (SDT) views it particularly seriously, even where the solicitor's participation was naïve and involved no personal gain. Cases that reach the SDT can result in suspension or strike-off.¹⁰

Reports to the SRA relating to money laundering 2012-2015

Nature of report	2012	2013	2014	2015	Total
Breach of Money Laundering Regulations or Proceeds of Crime	78	74	101	85	338
Money laundering (perpetrator or facilitator)	24	68	82	63	237
Providing banking facilities through client account	5	22	16	22	65

7. Outcome 7.5 of the Solicitors Code of Conduct 2011

8. [DIRECTIVE \(EU\) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL](#)

9. ML Reg 24

10. For example, [SRA v Olayemi Daniel \(2015\)](#) 11343-2015; [SRA v Tidd \(2013\)](#) 11178-2013

External Drivers

There was, and remains, a high level of external focus and increased activity on AML compliance from HM Government and law enforcement agencies. There is a genuine expectation that regulators should do more and this message was reinforced during the course of the consultation for the National Risk Assessment (NRA) on AML compliance.

The Government's Serious and Organised Crime Strategy¹¹

This highlighted that a small number of complicit or negligent professional enablers, such as bankers, lawyers and accountants, can act as gatekeepers between organised criminals and the legitimate economy. To tackle this threat, the Home Office, wider government and law enforcement agencies, worked together with us and the Law Society to develop and deliver a communications campaign between October 2014 and February 2015 in order to:

- increase law firms' ability to recognise emerging money-laundering threats
- promote existing good practice
- encourage the legal sector to submit high-quality SARs.

The campaign received strong support from the legal sector, with influential professionals from a range of legal firms joining with representatives from the regulatory bodies, law enforcement and government, to promote key messages. This was achieved through:

- existing forums
- conferences and newsletters
- the legal sector press
- dedicated events such as round-tables and webinars.

During the campaign, an increase in law firms accessing the AML Guidance provided by the Law Society was identified. There was also an increase in SARs reporting to the National Crime Agency's UK Financial Intelligence Unit (NCA) in comparison to the previous year. The campaign period also coincided with our thematic review. Therefore it is likely both of these initiatives improved overall AML awareness and in turn led to an increase in SARs from the legal sector.

From November 2015, a second phase of the communications activity began and was delivered jointly with the legal and accountancy sectors. It aimed to promote and reinforce best AML compliance practice.

The Serious Crime Bill

The Serious Crime Bill had been progressing through Parliament during 2014 and received Royal Assent on 3 March 2015. Part of the Act is designed to "discourage corrupt and complicit professionals who support or facilitate organised crime". The Act contains a new offence of participation in the criminal activities of an organised crime group which carries a maximum custodial sentence of five years.

11. [Serious-organised-crime-strategy](#). Gov.uk publication October 2013

The 4th Anti Money Laundering Directive

In December 2014, following a substantial period of negotiation, the European Union agreed the final text of the 4th Anti Money Laundering Directive. It was formally adopted on the 5 June 2015. EU member states have two years to transpose the new standards into their national legislation. Some key requirements of the directive, that are of relevance to the legal sector, include:

- an increase in the emphasis on a risk based approach in which law firms will be required to have written AML/CFT (Counter Financing of Terrorism) risk assessments, policies, procedures and controls in place proportionate to the nature and size of the firm
- a widening of the definition of Politically Exposed Persons (PEPs) to include both domestic and foreign PEPs
- changes in the application of simplified due diligence (SDD). Firms will need to provide justification for SDD after conducting a risk analysis to determine that a business relationship or risk presents a lower degree of risk
- an increase in transparency around beneficial ownership of companies and trusts and the maintenance of a central beneficial owner registry.

The Financial Action Task Force Mutual Evaluation Review (FATF MER)

In December 2006, the United Kingdom was the subject of a FATF MER which reported in June 2007. The next FATF MER of the United Kingdom was originally scheduled for spring

2016, but is now due to take place in spring 2017. It was anticipated that HM Treasury and the Home Office in preparation for the review, would (as has now happened) set up a series of engagements with regulators, including us.

The National Risk Assessment (NRA)

This was to be published late in 2015 and would have an aligned UK Action Plan to drive activity forward in anticipation of the scheduled FATF MER in Spring 2016.

Our Approach

Our thematic review was undertaken over a period of eight months (from 1 October 2014 to 31 May 2015) and we engaged with 252 firms in total.¹²

We specifically did not select a representative sample of firms but instead adopted a risk based approach, focussing our review on those firms identified as being either high impact and or higher risk. Historically, firms which have a potentially high impact owing to their size, turnover and volume of client base have been included in the Regulatory Management programme. Although, the fact that these firms are potentially high impact does not necessarily mean that they pose a high AML risk. The sample also included all firms that were then subject to a Forensic Investigation in the review period. Such investigations often involve alleged serious breaches of the SRA Handbook and thus, these firms already represented a higher risk.

12. This equates to just over 2% of our total regulated community

The sample firms comprised:

- 128 firms within our Regulatory Management (RM) portfolio at the time of the review period. This engagement was carried out by our Regulatory Managers.
- 124 firms which were subject to a Forensic Investigation during the review period. This engagement was carried out by our Investigation Officers.

The firms visited varied in size and structure from sole practitioners to City and international firms. A breakdown of the types of firms we visited is shown on the next page.

These firms provide a wide range of legal services. Some were involved in high-risk services and transactions on a frequent basis, whereas others only occasionally did work in which there was a risk of money laundering. It should be noted that the MLR do not apply to all legal services which may be conducted by law firms.¹³

Under the Proceeds of Crime Act 2002 (PoCA) the primary money laundering and terrorism financing offences apply to everyone. However, different reporting obligations apply depending upon whether the activity is regulated under the MLR or not. Since the case of *Bowman v Fels*,¹⁴ we have noted that some firms have assumed that litigation, in particular personal injury work, is exempt from AML compliance. During our visits, firms were made aware that they were still at risk of committing money laundering offences under PoCA if, for example, they become involved in facilitating sham litigation such as staged road accident claims or dealing with bogus clients.

The scope of the review was to:

- gain a good understanding of the policies, procedures and controls put in place by firms to identify and prevent potential money laundering
- evaluate the level of knowledge, training and awareness in relation to AML compliance.

Our visits were designed to involve constructive engagement with the firms and to provide them with examples of best practice where appropriate that might improve their systems and controls.

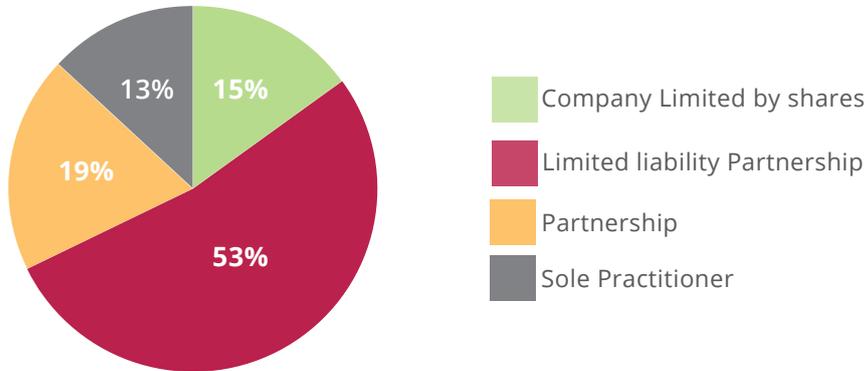
We did not specifically review client files, or attempt to proactively uncover incidents of money laundering or breaches of MLR or PoCA. We did, however, reserve the right to investigate any conduct issues that came to light during the evaluation, including those related to money laundering.

13. Only that which falls within the definition in MLR regulation 3

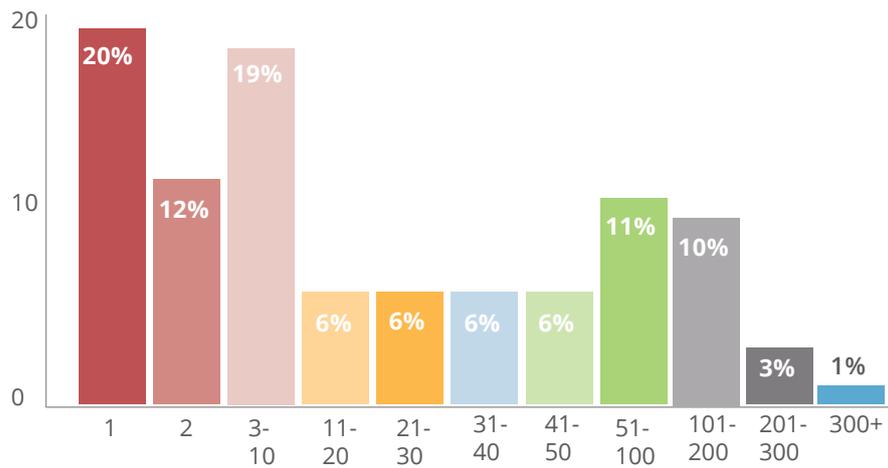
14. [2005] EWCA Civ 2006

A breakdown of the types of firms visited

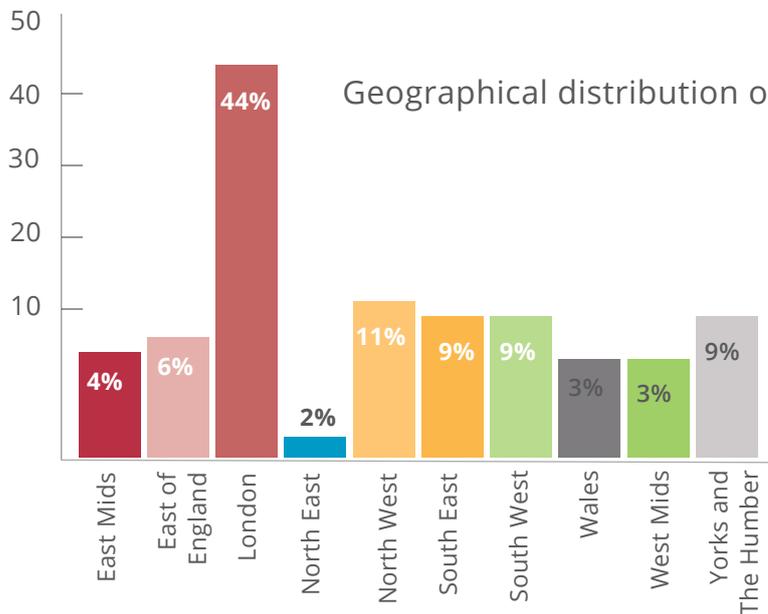
Composition of sample firms by structure



Composition of sample firms by no. of partners (or equivalent)



Geographical distribution of sample firms



Summary of our findings

All firms visited had a designated MLRO.

We found that most of firms we visited had effective AML compliance frameworks in place.

AML policies and procedures are only one element of an AML framework and their effectiveness is dependent on having a healthy compliance culture embedded within a firm. In general, we found that firms and their staff displayed a positive attitude towards AML compliance and were trying hard to meet all of their duties and obligations under MLR and PoCA.

We found there was an adequate application of Client Due Diligence (CDD). As we expected, each firms' processes and procedures in relation to CDD varied according to:

- the size of the firm
- types of legal services offered
- available resources.

Most large firms had dedicated client inception teams which undertook a large part of the CDD activity. By contrast, in smaller firms, the individual fee earner was responsible for carrying out due diligence on each of their clients.

All but a few firms that we visited had good controls in place to restrict work being conducted on a client matter prior to CDD being completed in accordance with the MLR.

Most firms had a good understanding of their recording and reporting obligations under both PoCA and the MLR.

Almost all of firms had suitable processes and procedures in place to enable staff to report suspicions of money laundering.

We did however find weaknesses in some areas. These are highlighted on page 11.

Action taken and next steps

As a result of our thematic review, our general conclusion was that whilst the legal sector is viewed as a high risk for being used by criminals for money laundering, the profession itself and the way it manages AML compliance is mitigating this risk.

The very fact of our proposed engagement with firms, particularly those within RM, often prompted a review and updating of policies. It also led to a refresh and more thorough roll out of training in advance of our visit. This moved the AML issue up the risk agenda of many firms.

In many instances, at the outset of our meetings, we met with the managing partners of firms in addition to MLROs, Compliance Officer Legal Practice (COLPs) and Compliance Officer for Finance and Administration (COFAs). This ensured that our interest in the firm's work in relation to AML and the drivers behind our thematic engagement were explained and discussed with representatives of senior management.

As part of the structured AML engagement by RM, we provided the firms we visited with examples of best practice, where necessary, to enable them to improve their AML processes and procedures. Often this feedback session was attended by managing partners (in addition to the MLRO, COLP or other risk personnel) who were instrumental in demonstrating a firm's commitment to minimising the risk of money laundering.

As part of their ongoing engagement with firms, the RM team will, where appropriate, continue to share best practice.

In a limited number of instances we are actively investigating evidence of potential money laundering in firms.

We have shared, anonymously, a number of our findings and conversations with firms with law enforcement agencies and the NCA, particularly with regard to some challenges in relation to firms making SARs.

We are aware that some aspects of the MLR prove more challenging for smaller firms, for example, MLRO succession planning or providing relevant training for staff. However, both of these are mandatory under the MLR. Despite these challenges, we have seen many instances of good practice among small firms. We encourage firms with limited resources to participate in peer groups where information on AML issues and best practice can be obtained, and to access the online resources available to the profession. We will continue to support small firms via the Small Firms Portal.

Ultimately, AML compliance should be appropriate to a firm's needs and based upon a thorough assessment of the risks presented by, but not necessarily limited to:

- individual clients
- the type of legal services offered
- the method of service delivery (eg where the client is not met face to face)
- jurisdiction risk.

Different clients, legal services, delivery methods and jurisdictions (and combinations of these factors) pose varying levels of risk. These should be identified and managed in a firm's policies and in the implementation of appropriate controls. The higher the level of risk, the greater the rigour needed in CDD, ongoing monitoring and control to mitigate any risk.

A risk-based approach enables firms to have flexibility in choosing the areas to concentrate their resources and how best to apply AML controls. There is no reason why AML procedures such as CDD should not be cost effective, and we saw many good examples of this on our visits.

We are committed to working with firms in this area and in preparation for the FATF MER. We hope that solicitors and firms will use this report as a spur and guide to continue to improve their AML processes and procedures.

Weaknesses found in some areas

- We identified that the responsibilities, visibility of, and support provided to, the MLRO varied amongst the firms. Many of the smaller firms, and also a number of the larger firms, did not have a deputy MLRO or a contingency plan in place to provide cover in the MLRO's absence.
- Most MLROs displayed a good understanding of AML, despite not having any formal qualification. However, we did find that, in several cases, an inexperienced or inadequately trained MLRO had a detrimental effect on the overall adequacy of their firm's AML compliance.
- We identified some weaknesses in relation to the low frequency with which firms reviewed their AML policies in order to ensure that they were up to date, relevant and fit for purpose.
- Additionally, a number of firms had either no or inadequate processes in place to test and measure the effectiveness of their systems and controls.
- In some firms, there was a lack of understanding and weaknesses in applying enhanced due diligence, identifying and dealing with Politically Exposed Persons (PEPs) establishing source of funds and source of wealth, ongoing monitoring and the requirements under the sanctions regime.
- Most firms we visited treated AML training as a priority and this training was usually mandatory with staff attendance monitored, recorded and action taken if not completed. However, in some instances the MLRO did not have sight of the level of attendance at AML training or the identity of non-attendees as this was managed by the HR or training function. We also identified a general lack of appropriate training for finance staff who are also a key line of defence in mitigating the risk of money laundering.

Money Laundering Reporting Officer

Regulatory and Legislative Framework

- Solicitors' firms that conduct work under the MLR (in the regulated sector) are required to have a 'nominated officer' to receive and make disclosures to the National Crime Agency (NCA).¹⁵
- Nominated officers are commonly referred to as The Money Laundering Reporting Officer (MLRO).
- The MLRO is central to a firm's AML risk control framework.

The extensive role and responsibilities of an MLRO, when carried out effectively, will assist firms in maintaining compliance with statutory and regulatory AML obligation and minimise participation in the laundering of the proceeds of crime.

MLRO key responsibilities

- Implement AML compliance policies, procedures and controls
- Monitor and assess the effectiveness of a firm's AML policies, procedures and controls
- Receive and evaluate internal SARs
- Maintain a confidential register of internal SARs including complete and thorough records of all enquiries made and document decision-making / the rationale and the method of closure (i.e. disclosure made to the NCA or no further action required)
- Make external SARs to NCA, as necessary
- Maintain a confidential register of external SARs to NCA
- Advise solicitors and staff of their obligations
- pending the outcome of consent SARs and following receipt of the outcome of consent SARs
- Act as a main point of contact for law enforcement agencies when dealing with formal and informal requests for information
- Ensure all staff are appropriately trained in AML and maintain staff awareness
- Keep fully up to date with developments in AML, for example, changes in legislation, current fraud typologies and emerging risks.

15. Regulation 20 (2)(d) MLR; Part 3 TA; Part 7 PoCA

Key findings from visits

Each firm we visited had AML policies and processes in place which included the appointment of an MLRO. We identified however that the role, responsibilities, visibility of and support provided to the MLRO varied amongst firms.

The majority of MLROs combined their role with other posts held at their firm, in particular that of COLP or COFA and in some cases both. This is not necessarily a problem in principle, but might become a potential issue if the MLRO is overburdened. If the MLRO is carrying out several roles, he or she might be unable to give sufficient time and consideration to AML duties, which carry a heavy personal liability.

Additionally, there were MLROs who held other posts which could present a conflict of interest, such as heads of business divisions in which there was a higher risk of money laundering. This may adversely impact their ability to carry out AML duties effectively and impartially. Several firms mentioned that they actively minimised this risk by appointing an MLRO who was independent of their transactional property work, which was acknowledged as their highest risk for money laundering.

The MLRO acts as the single point of contact for all AML related activity within a firm. A single point of contact however is also arguably a single point of weakness.

We found that a number of firms had not appointed deputy MLROs. This is a particular risk. The NCA has cited significant challenges in relation to MLROs at law firms, including inaccurate or out of date contact details, the unavailability of MLROs during working hours and no alternative point of contact when the MLRO is on leave or otherwise unavailable

during the consent SAR notice period. It is essential that there is always an individual available at firms to carry out the MLRO functions. In particular, firms should consider how they could mitigate the risks posed by the sudden and/or prolonged absence of a sole MLRO.

Some firms had appointed deputy MLROs. Such firms and MLROs believed that a deputy provided useful support, oversight and cover. Deputy MLROs were also considered to be an opportunity to develop and train potential future MLROs.

We also visited some firms, who had deputy MLROs in place, but with low visibility in the firm. Some fee earning staff stated to us that they were not aware of the post of deputy MLRO or who they should contact in the MLRO's absence or unavailability.

Most MLROs displayed a good understanding of AML matters. We found that in several cases, a weak MLRO with little or no previous AML experience or training had a detrimental effect on the overall adequacy of their firm's AML policies, systems and controls.

Unsurprisingly, we often found that firms which had more robust processes and procedures and compliance monitoring in place were those in which the MLROs had AML training and attended relevant professional development courses. These MLROs generally also had a genuine practical interest in AML compliance, and were strong supporters of what the legislation and regulatory requirements were aiming to achieve.

Good practice

At one large firm which conducted more than 90% property work, the MLRO was a senior manager without the responsibility of managing a client base in order to have the time capacity to deal with AML issues. The MLRO spent approximately five hours per week on AML matters and had attended numerous courses (at least biannually) run by The Law Society and other external training providers. The firm regularly measured the effectiveness of its controls and AML issues were reported at monthly management meetings where AML was a standing item on the agenda.

At one smaller firm, the MLRO was a senior equity partner who attended training courses on a regular basis throughout the year and regarded their MLRO duties as an, “essential part of good business management”. It was for this reason that the MLRO stated he was not a fee earner so as to ensure, “that good practice and procedure is fully embedded across the firm”.

At one large city firm we identified that improvements had been made by appointing a deputy MLRO to assist the MLRO. Closer monitoring was put in place to ensure that the MLRO was not overburdened or compromised between fee earning and MLRO duties. Generally the firm had good systems and controls in place.

Poor practice

We visited a sole practitioner’s firm which had three fee earners and conducted residential conveyancing work. The sole practitioner, who was also the MLRO, had no previous AML experience and was not a member of any AML network or professional forum. The firm had AML policies in place, but we identified weaknesses in the firm’s implementation and controls in relation to

- recording CDD
- continuing to act in a transaction before full CDD had been carried out
- insufficient CDD checks on companies.

The MLRO had provided staff with basic AML training, but their understanding of the content was not tested by the MLRO.

There were also some concerns in relation to MLROs who lacked regular, specific training and were also generally not members of any professional groups or forums where AML issues could be considered. Such networks are a good source of support for MLROs, in particular for sole practitioners, and are a cost-effective way of keeping up to date and sharing best practice.

Inevitably, we found that MLROs' AML knowledge and understanding varied. Key areas where some MLROs needed to improve their knowledge were as follows:

- The threshold for reporting
- Understanding the difference between 'source of funds' and 'source of wealth' and the extent to which enquiries ought to be carried out to verify each
- Appropriate levels of CDD
- The scope of the sanctions regime
- The need for, and extent of, ongoing monitoring.

✓ Good practice	✗ Poor practice
<ul style="list-style-type: none"> • The MLRO is independent, of sufficient seniority to influence management and access relevant information, able to devote sufficient time to the role and has a deputy MLRO to assist. • The MLRO is visible, approachable and resilient. • The MLRO is an AML expert and can provide clear advice and training. • The role and responsibilities of the MLRO and Deputy MLRO (and any other AML support staff) were recognised in performance appraisals. 	<ul style="list-style-type: none"> • The MLRO lacks credibility and authority due to inexperience, insufficient knowledge or lack of seniority or respect within the firm. • The MLRO does not have the relevant autonomy and is not given any practical or senior management support. • The MLRO does not keep their technical AML knowledge up to date. • There is no Deputy MLRO or contingency plan in place to provide cover in the MLRO's absence.

Policies

Regulatory and Legislative Framework

Firms that conduct work in the regulated sector must establish and maintain appropriate and risk sensitive AML policies and procedures in relation to the following areas:¹⁶

- Customer due diligence measures and ongoing monitoring
- Reporting
- Record keeping
- Internal control
- Risk assessment and management
- Monitoring and management of compliance with, and the internal communication of, such policies and procedures.

AML systems and controls should be proportionate to risk, and do not need to be expensive.

Key findings

A positive consequence of our thematic review was that it prompted several firms to review and where necessary, update their policies in advance of our visit.

We found firms differed in their views about what constituted 'high-risk' work. The definition of high-risk work will depend to some extent on each firm's particular circumstances. Firms who carry out a high percentage of transactional or property work should consider the risk of their workload overall, even if they do not act for international, high net-worth clients or PEPs.

A number of larger firms had produced specific guidance for a wide range of areas of work, including conveyancing, corporate work and

litigation. This guidance identified the particular AML issues and risks that were practice area specific and so better-equipped fee-earners to spot potential issues in their practice area.

Some international firms created policies for different jurisdictions to reflect the circumstances and risks of each jurisdiction. Others developed a universal AML policy based on the highest available requirements (often described as a 'gold standard') that they implemented across all of their offices irrespective of whether the local requirements were less demanding.

16. [Regulation 20 MLR 2007](#)

We found a small number of firms provided their client account details on their website or in their initial client care letter. This practice raises a number of risks. It increases the opportunity for money to be transferred prior to the completion of CDD. In addition, it could be used by criminals as a mechanism to launder money by sending money to a firm and then reclaiming the funds on the purported basis that the transfer had occurred in error, thus creating a veneer of legitimacy for those funds, which could now be shown to have come from a regulated professional.

Most firms had appropriate policies in place and also reviewed their policies annually. A small number reviewed policies more frequently, every six months. Some firms stated that they would review on an ad hoc basis or when events occurred which prompted a review, for example after submitting a SAR. During our visits, we found a few firms still referred to the Serious Organised Crime Agency (SOCA) rather than the NCA, which replaced SOCA in 2013. This suggested a failure to review and amend policies regularly, and raised questions about their use and effectiveness and the firm's commitment to AML generally.

We identified that some firms did not have any formal processes in place to test and measure the effectiveness of their AML policies and procedures. Several MLROs stated that the fact that their firm had not had any money laundering or terrorist finance issues was sufficient evidence to show that the firm's procedures were understood and being positively applied by staff. Equally, this could be that policies and staff understanding was

inadequate to identify even common concerns or suspicious activity. Some firms had quality assurance processes and were actively testing their systems, notably CDD procedures. We consider a failure to do this as a risk and firms should ensure that they maintain, review and test the effectiveness of their policies and procedures on a regular basis.

The policies and procedures also need to be supported by senior management. This was the case in the majority of firms we visited. Having the policies agreed and endorsed by senior management is important, but there also needs to be a commitment to ensure that they are followed. Those firms that managed the risks well also ensured that staff were aware of potential disciplinary consequences if they failed to follow the firm's policies, in addition to any criminal or regulatory consequences.

Good practice

At one small firm we visited we observed that the AML policies were reviewed by the MLRO every six months. The effectiveness of the policies and procedures were also monitored every time a concern was raised by a fee earner about transactions they were working on. The MLRO cascaded a firm wide email on AML updates including any changes made to policies and procedures.

One large firm had comprehensive AML policies. Each policy was clear and well written. The policies were designed specifically for each local audience and contained both references to the law but also featured summaries of the key risks to fee earners and partners. The policies were available in an electronic format, clearly indexed and regularly reviewed. These were produced by the MLRO, the AML Committee and ultimately signed off by the Professional Practice and Risk Committee. The firm did not rely on mechanistic processes. The mitigation of risk involved both qualitative and quantitative measures. The firm had a mature system of controls in place. The system and policies were interconnected with no reliance on a single control or person.

Poor practice

One large firm we visited, that had undergone a merger, had not updated its AML systems and processes to ensure that consistent policies, systems and processes were being applied across the merged firm.

✓ Good practice	✗ Poor practice
<ul style="list-style-type: none"> • Policies are up to date, easily accessible, user friendly and easily understood by a wide audience. • Systems and processes are subject to regular quality assurance and independent testing and review to ensure they remain up to date and are effective (for example, dip sampling and exception reporting). • Policies ensure consistency in the reporting of concerns to the MLRO. • Regular and flexible approach to the review of policies to ensure they remain relevant, valid and effective. For example, reflect any changes to legislation or regulations, firm structure changes, changes in type of legal services offered, following the filing of a SAR to the NCA and emerging risks. • Senior management sets the right tone by demonstrating their own AML compliance to the rest of the firm and clearly communicating and enforcing the firm's commitment to minimising money laundering. 	<ul style="list-style-type: none"> • Policies and procedures are out of date, inaccurate or generic. • Over reliance on external parties to design and implement policies and procedures with minimal input from the MLRO. • The firm does not conduct adequate risk assessments of their work in order to tailor appropriate and effective policies, systems and controls. • A mechanistic approach to compliance resulting in a poor firm culture of compliance. • Disinterest from senior management and poor role modelling.

Client Due Diligence

Regulatory and Legislative Framework

- Firms undertaking work in the regulated sector must establish and maintain appropriate and risk-sensitive policies and procedures relating to CDD measures.¹⁷
- Generally, a firm must apply CDD on a risk sensitive basis when they establish a “business relationship” with a client, carry out an occasional transaction, suspect money laundering or terrorist financing, or doubt the veracity of identification documents previously supplied.¹⁸
- Firms must apply Enhanced Due Diligence (EDD) and ongoing monitoring in all matters that present a higher risk of money laundering or terrorist financing, where the client has not been physically present for identification purposes or the client is a PEP.¹⁹

Key findings

The firms we visited were generally aware of the importance of CDD and many applied their CDD procedures across both regulated and unregulated work.²⁰ One benefit of this was that it mitigated the risk of unregulated work developing into regulated work without appropriate CDD and other enquires being undertaken. It also gave firms confidence regarding their entire client and transaction base.

It is important to highlight that individual experience, number of years in practice, size of firm, demographics of clients and a good reputation will not in themselves deter criminals from trying to launder money through a law firm.

Many firms have adopted a centralised client take on process and sometimes separate departments. Such processes can be efficient and promote consistency. However, there is a risk that fee earners may become detached from the CDD process and lack a detailed knowledge of their client and the transaction. This in turn may have an impact on the ability of the firm to conduct ongoing monitoring appropriately.

We encountered some conflicting views about what constitutes a business relationship. Many firms did not conduct any work prior to completion of CDD and larger firms often had automated systems designed to minimise the risk of fee earners working where CDD was not satisfactorily completed.²¹ CDD should be completed before work is started for a client.²²

17. [Regulation 7 MLR 2007](#)

18. [Regulation 7\(1\)\(a\) MLR 2007](#)

19. [Regulation 14 MLR 2007](#)

20. Regulation 3 specifies when the MLR applies. It applies to “independent legal professionals” who participate in financial or real property transactions (- [Regulation 3 \(9\) MLR 2007](#)) and also to tax advisers, insolvency practitioners, trust or company service providers and estate agents. All of which may be business activities conducted by firms.

21. [Regulation 11 MLR 2007](#) sets out the requirement to cease a transaction where CDD is not completed

22. Regulation 9(2) MLR

However, the MLR permit CDD to be completed during the establishment of a business relationship in some circumstances but not if the work is an occasional transaction. Even so, it is permitted only if the specified conditions are met.²³ Therefore, firms should take care to ensure that they understand how these provisions work, what is permitted and that they are compliant.

However, some firms permitted fee earners to work up to 14 days before completion of CDD.²⁴ We recognise that in transactions where speed is important, it may be necessary to conduct some preliminary work that is not of a business nature, so as not to interrupt the normal course of business, as permitted by the MLRs if the other conditions are met. This could include things like preparing documentation. It is not appropriate, however, to take any money from the client, progress the transaction or bill the client for any services rendered, prior to the completion of CDD. Clients should be informed of any limitations that prevent the firm from working prior to the completion of CDD. In all cases, CDD should be completed as soon as practical. If CDD cannot be completed, work must cease except in the limited circumstances provided in the MLRs.²⁵

Often where a matter file was opened pending completion of CDD, within the finance function a block or flag appeared on its system to ensure that no funds were processed on that matter until CDD was completed. However, in at least one instance we identified the absence of any such restrictions in the finance system exposing the firm to the risk of processing funds before successful completion of CDD.

Some MLROs and their firms had a lack of knowledge and understanding of when and how to establish a client's source of funds and source of wealth, with some firms failing to distinguish between the two. This is a concern given that this is a requirement under the MLRs in respect of PEPs and best practice for all other high risk clients or matters. We identified that in most cases fee earners were making enquiries of clients in respect of their source of funds and source of wealth. However, the client's response was often taken at face value with no request for any supporting documentation or corroborating information. This is of relevance to small firms as the definition of a PEP is broad (and will be wider following implementation of the 4th Money Laundering Directive) and will trigger these requirements.

On a number of our visits we noted that some firms were charging their clients the cost of undertaking CDD. In relation to regulated activity and in accordance with the MLRs, law firms are legally required to undertake CDD. It is our view that the cost of undertaking CDD cannot therefore be treated as a disbursement, since it is not a cost incurred on behalf of the client. Firms will be at risk under Outcome (8.1) if CDD payments are described in their bills to clients as disbursements. As a general rule, we would expect such charges to form part of a firm's overheads. There may on occasion be circumstances in which the cost of the CDD is particularly high (for example, when you have to carry out an overseas company search) and firms may wish to seek agreement with their client that the cost will be payable by the client.

23. Regulation 9 MLR deals with the timing of verification of identity.

24. In one case a firm allowed up to a month for the completion of CDD.

25. Regulation 11(2) MLR

In order to comply with Outcomes (1.12) and (1.13) firms should explain the likely cost with their client and obtain their client's informed consent at the outset of the retainer. If the client agrees to meet the cost of the CDD then firms should record it in their bill as part of profit costs. Some firms undertake CDD for all clients as a matter of course, irrespective of the nature of the retainer and whether it is a requirement of the MLRs. Whilst there may be good reasons for doing this, it is questionable as to whether there would ever be justification for passing the cost on to the client where such checks are not a requirement, even if the client agrees.

There are clients for whom firms should not act regardless of the level of risk that is assessed and applied. These clients are those subject to sanctions. The sanctions regime is absolute and stands outside any risk based approach. HM Treasury issues a consolidated list²⁶ of all individuals and entities that are subject to sanctions effective in the UK. Firms can only act for a client who is on the list with a licence from the HM Treasury Asset Freezing Unit.

During our visits we identified that some MLROs had a lack of knowledge and understanding of the sanctions regime and the requirements for sanctions screening both at the outset of engaging with a client and throughout the course of a retainer. When we asked the MLROs working in smaller firms whether their firm checks clients against the relevant sanctions lists, just over a third stated that they screened clients and of these most applied a risk based approach. In contrast the larger City firms

evidenced a far better understanding of the sanctions regime and had often implemented automatic and ongoing sanction screening processes.

Several MLROs held the view that it was not necessary to screen locally based clients or that they simply did not deal with clients from high risk overseas jurisdictions. We drew these firms' attention to the fact that there are UK nationals and UK residents on the consolidated list.

Similarly, MLROs in firms which conducted predominantly non-regulated work for the purpose of MLR, for example personal injury work, believed wrongly that the sanctions regime did not apply to them. The regime applies to all payments received and made by a firm regardless of the nature of the transaction and there is no de minimis financial limit. For example, settlement payments for damages, legal aid payments, payments to beneficiaries of a will or payment of proceeds from a property transaction to a third party could fall within the regime. If these are paid to persons on the sanctions list, and the firm does not have a licence to act, it will be an offence.

Firms must conduct ongoing monitoring on a risk sensitive basis throughout the life cycle of a client matter. Ongoing monitoring means scrutinising transactions to ensure that they are consistent with:

- the firm's knowledge of their client
- the expected nature of the retainer
- the appropriate risk assessment remaining valid.

26. [Financial-sanctions-consolidated-list-of-targets](#) Gov uk publication

Inevitably, practices varied across firms. Some firms left the obligation for ongoing monitoring to the discretion of the matter partner. Other firms had automated processes requiring the lawyer responsible for a relevant matter to review it and report formally on a three or six monthly basis.

Similarly, where firms had identified high risk matters or clients there was a difference in how firms communicated that conclusion to fee earners. Sometimes it was reported only to the matter partner but it was rarely formally communicated to other team members who might in some instances be better placed to spot potential money laundering concerns during a transaction.

We identified that most firms had a time limit on the validity of CDD, and conducted checks again after a defined period or when taking a new instruction. There were a few firms, however, that did not conduct any ongoing monitoring. Some criminal organisations may target existing clients of firms to launder money on their behalf and a person may undertake both legitimate and non-legitimate transactions at the same firm. The requirements of ongoing monitoring can mitigate this risk.

Poor practice

At one large firm we identified that CDD recording was inconsistent amongst departments. The firm had a good standard template CDD form which could be made compulsory across the firm. We identified that the department with highest risk, residential conveyancing, did not use the form at all.

At one large firm, it was the partner's responsibility for ensuring CDD evidence had been obtained. However, there were no checks made to ensure that fee earners had obtained the appropriate CDD. The fee earners could open a file number before all CDD was in place, and therefore it was possible to work on the file with no limitations. The MLRO only reviewed the list of files where CDD was not in place on a quarterly basis. There was no system of file audits. Partners were not appraised on their attitudes to compliance.

In one city firm, CDD checks were only carried out in respect of new clients and there was no internal expiration date on the proof of identify obtained. Set expiration dates should be given to proof of identity used for repeat clients where that proof is held on file. The firm were over reliant on their reputation to protect them from approaches from clients who may want to use the firm to launder money.

Good practice

At one small firm, the CDD requirements were set out in the firm's manual and related to the level of risk of the matter as identified through the firm's risk matrix spreadsheet. The risk score determined the level of CDD to be applied to an individual client. The firm did not solely rely upon an electronic CDD check. Fee earners were also encouraged to review the risk score throughout the duration of the transaction.

One large firm we visited had a procedure that if a client was dormant for two years, when they returned to instruct the firm, they were treated as a new client. High risk clients were subject to renewed CDD on every new or change of instruction. A monthly review and mid transaction review of high risk clients and matters was carried out. The firm would not "grandfather in" any clients if they came with lateral hires or from other firms.

One large firm had procedures in place requiring that all prospective new clients had to be authorised by a partner and subject to CDD. UK requirements were applied worldwide subject to local additional requirements with the exception of the US. Each international office had its own MLRO. All high/medium risk matters were flagged and batch screened against a compliance database. A six monthly review was automatically run by the central team and if there were any ownership changes, for example, the central team would contact the fee earner.

At one large firm that we visited if a high risk client was approved and taken on, it would be flagged on the system that they were only approved for that one matter. The firm regularly interrogated the system and carried out bulk matter closures. They looked for periods of inactivity and closed matters down. The firm had a general policy not to act as escrow agents.

✓ Good practice	✗ Poor practice
<ul style="list-style-type: none"> • A centralised, accessible and user-friendly database for CDD. • Systems in place to bar matter progression, time recording and receipt of monies until CDD has been completed appropriately. • A coordinated and active engagement between fee earning and finance staff to prevent monies being received on client account prior to CDD being completed • Policies to escalate concerns to management, to cease relationships where appropriate, and to recognise and value CDD activity. • Appropriate procedures to enable effective ongoing monitoring of business relationships to be conducted and for concerns to be escalated. • Terminate the client relationship when an action of a client exceeds the firm's risk appetite or is subject to sanctions. • Staff performance and appraisal processes that recognise and rewards effective CDD activity. 	<ul style="list-style-type: none"> • A superficial and mechanistic tick box approach to CDD. • A tendency to view CDD as a one-off exercise, and consequent failure to keep it up to date. • A failure to ensure that CDD is completed before the commencement of a 'business relationship', an occasional transaction is carried out and/or receipt of money on account. • An ineffective or hands-off MLRO who fails to assess and authorise high-risk clients. • A failure to distinguish between clients' source of funds and clients' source of wealth or obtain verifying evidence. • A failure to properly assess clients' risk, PEP(s) status or check the sanctions list. • Detachment of fee earners from the process that affects ability to adequately conduct ongoing monitoring.

Training and Awareness

Regulatory and Legislative Framework

- Firms undertaking work in the regulated sector must ensure that all relevant employees receive appropriate training. Employees must be aware of the law relating to money laundering and terrorist financing. They must also be given regular training on how to recognise and deal with transactions and other activities that may be related to money laundering or terrorist financing.²⁷
- The upcoming EU 4th Directive stresses the importance of training. Both MLROs and other staff will need to be updated on the legislative changes including those relating to risk assessment and beneficial owner registers.

Key findings

We found that most firms had provided appropriate and relevant training to staff. Another positive consequence of our thematic review was that it prompted a number of firms to undertake refresher AML training of their staff in advance of our visit.

Training methods and materials varied from firm to firm and included one or more of face-to-face training, e learning, case studies and department or practice area specific training. Some employees commented that where possible, having both face-to-face and online training was valuable as different people had different learning styles.

We noted that the frequency of training varied between firms. Firms should regularly review their AML training requirements and take account of developing experience, changes in firms' work mix or changes in circumstances. For example, following mergers, we noted that some firms had failed to refresh and review

the new firm's AML training. Consequently, staff had varying degrees of knowledge and understanding about the new firm's policies and procedures.

During visits, we inspected training records. Training records allow firms to review and determine who requires training and potential areas for future training. It is important that firms take steps to ensure all staff receive training and non-attendees are offered alternative training.

During our visits to larger firms, we also met with finance staff and employees. Most staff were satisfied with the level and frequency of training and demonstrated a good understanding of their firm's AML policies and procedures. We did note, however, that generic training might not be appropriate to enable finance staff to spot warning signs of money laundering in a finance context.

27. [Regulation 21 MLR 2007](#)

Good practice

At one large firm we visited, the MLROs delivered ad hoc sessions and department by department training on an annual basis. There was also an annual risk lecture which was well attended and combined a number of compliance issues including AML. The MLRO relied on a variety of different methods to ensure that staff were aware of AML issues via bulletins, lectures and e learning. Members of the compliance team took the International Compliance Association's qualification which included AML and a range of other topics. This was funded by the firm. Compliance/risk management was part of expected fee earner competency. The compliance team reported to the risk committee every quarter on its observations. A relationship of trust existed between the MLRO/compliance team and the fee earner community. The MLROs had also drafted very good, practice-specific scenarios highlighting AML risks

At one small firm, which undertook mostly foreign property and immigration work, we observed that the managers had organised specialist training for staff by the police in relation to false passports and other red flags in relation to money laundering.

Poor practice

In one large firm we identified that training records indicated that some staff had not undertaken AML training since 2008. This included staff within a high risk commercial sector. Staff interviewed also confirmed they could not recall when they had last undertaken AML training.

One large firm stated that they provide both online and face to face training at regular intervals. The firm's training records however suggested that a number of individuals had not received training for some time; in particular several partners and associates who undertook transactional work had not received AML training for up to seven years.

✓ Good practice	✗ Poor practice
<ul style="list-style-type: none">• The MLRO delivers bespoke training including practical and practice specific examples and case studies.• AML training is mandatory, monitored, recorded and reviewed with mop-up training sessions being provided.• AML training is repeated on a regular cycle for staff.• AML training attendance and compliance is referred to in staff KPIs and appraisals.• The MLRO maintains awareness of issues through regular staff updates through a range of information streams.	<ul style="list-style-type: none">• Training is not appropriate to the staff involved.• Training is not mandatory and the firm keeps no or inadequate training records.• The firm does not carry out testing to ensure that training is understood.

Reporting

Regulatory and Legislative Framework

- If you undertake regulated work, you must disclose any suspicions of money laundering.²⁸ Suspicions should be reported initially to the MLRO who will then decide whether a SAR is required to be made to the NCA.
- If you work in the unregulated sector, although the disclosure regime is different, you will also need to consider whether they are required to make a disclosure.²⁹
- You are also required to make disclosures to the NCA of suspected terrorist financing,³⁰ regardless of whether you work in the regulated or unregulated sector.
- If you suspect that a transaction may involve money laundering or terrorist financing, you must apply to the NCA for consent to proceed with the transaction. This is called a “consent SAR” and requires the regulated person to provide information about the transaction and those involved.

Key findings

In general, we found that the firms we visited complied with the reporting requirements. Firms had procedures in place to enable staff to report suspicious transactions, and MLROs ensured that staff had the knowledge to make reports to them and did so. Most of the firms we visited had designed and implemented internal suspicious activity reporting template forms. The MLROs tended to occupy senior positions within the firms and were visible and known to staff. Feedback from staff emphasised that it was important that the MLRO was both authoritative and above all accessible and approachable to staff at all levels.

It was also important that staff understood how to deal with client enquiries once a report had been made and ensure that procedures were in place to prevent ‘tipping off’.³¹

28. ss.330-332 PoCA 2002

29. s.337-339 PoCA 2002

30. ss.19-20 TA 2000

31. s.333A PoCA 2002

Good practice

One large firm had clear reporting lines in place. It was clear from the interviews that each individual knew the identity of the MLRO/deputy and the relevant procedure on how to report an issue. The MLRO was considered to be very approachable. One of the interviewees commented that the firm welcomed an inquisitorial and cautious approach to understanding clients and instructions and there was never any pressure to take short cuts on AML to achieve a commercial result. The finance staff commented that AML processes were not an add-on, "its part of our everyday role to do it". The MLRO and the deputies moved around the offices and were regularly approached to discuss matters.

Poor practice

At one large firm, the MLRO stated that queries regarding AML issues were infrequent. This may reflect the fact that the partners would raise issues with the MLRO, the fee earners, however, were more likely to speak to the compliance manager. When we spoke to the fee earners and asked who they would approach if they had any AML concerns, they said that they would speak to their supervising partner and then the head of department.

Suspicious Activity Reports

It is the legal responsibility of law firms to submit SARs to the NCA in accordance with legislation contained within PoCA.

The NCA publishes figures in its SARs Annual Report each October. In its report for 2014, it identified that SARs submitted by law firms had reduced that year by 8% (from 3,615 in 2012/13 to 3,328 in 2013/14), against a backdrop of SARs increasing nationally. SARs submitted by law firms now represent less than 1% of all SARs nationally, and equate to only 0.3 SARs per firm, per year.

The 2013/14 figures are not an exception, as SARs submitted by law firms have reduced year-on-year from 6,460 in 2007/08 to 3,328 in 2013/14. Although the reduction is not exclusive to the legal sector,³² the reduction in the number of SARs submitted by law firms is a concern.

During our visits we asked MLROs whether they were aware that SARs in law firms have been decreasing and what they considered might be the reasons for the decline. The responses are summarised as follows:

- General settling down in the AML environment since the MLRs were introduced in 2007, which has resulted in a better understanding in law firms of what is required under the SARs regime and a move away from reporting simply as a precaution.
 - An overall reduction in transactional work post the financial crisis of 2008/9 has meant fewer SARs, particularly in relation to property transactions, a high-risk money laundering area of work.
 - Firms increasingly refusing to act in particular matters in which there is a suspicion of money laundering or where clients or transactions are assessed as 'high risk' at the outset. This may have led to a reduction in consent SARs.
 - A better understanding of the application of legal professional privilege (LPP).
 - A better understanding of MLRs and PoCA.
- A significant number of firms stated that in their view SARs had reduced because when the MLR were first implemented, law firms had been over-reporting in a defensive or precautionary manner. These firms stated that in time they had learned from experience which matters to report to the NCA and which were not appropriate to report. Some firms, on the other hand, stated that they were still submitting a similar number of SARs compared to those they were making when the regulations were introduced.
- Some firms stated that they were more confident in assessing risk, identifying red flags and were refusing to act (or continue to act) for clients in matters in which there is a suspicion of money laundering or evidence of high risk. This may to some extent explain a reduction in consent SARs.
- Several MLROs stated that the number of SARs had reduced due to improved controls when clients first came to the firm. MLROs should, however, consider submitting an intelligence SAR where the firm has refused to act. Refusing to act is effective in disrupting crime, but it could also displace criminal activity and criminals may seek to target another law firm.

32. For example, accountants' SARs have reduced from 7,354 in the period 2007/08 to 4,834 in the period 2013/14

Good practice

One firm had a clear and standardised process for dealing with and recording AML enquiries and reports regarding suspicions of money laundering. The firm ensures that staff file internal reports separately to client files, and keep a central database of money laundering reports. These include a complete internal record of each report, even if they do not ultimately lead to a SAR being made. This firm also provides fee earners with an anonymised annual overview of reports made to the NCA, to illustrate what they need to look out for.

Poor practice

One firm we visited had an inconsistent approach to reporting. Some reports and enquiries were routed to the MLRO, some to the internal risk team. Both keep separate records. Like its other policies, the firm's reporting policy was not kept updated. This approach meant that staff did not know how to make a report and may not have complied with their legal obligations. Staff did not feel that their suspicions would be taken seriously, and were under pressure to retain valuable clients. As a result, suspicious transactions were not appropriately considered, recorded or reported to the NCA. The MLRO will not be able to justify his internal AML decisions, if criminal or regulatory allegations arise.

If appropriate evidence is available to support a suspicion then an intelligence SAR should be submitted to the NCA in accordance with PoCA and in order to assist law enforcement agencies with intelligence analysis, trends and tracking criminal activity.

Several firms commented that the profession now has a better understanding of LPP and the privileged circumstances defence under PoCA S.330 and this may have impacted on the level of SAR reporting. We also identified a lack of understanding when speaking to MLROs at a small number of firms around the appropriate use of the crime/fraud exception.

Some firms stated they had not experienced a decline in their own submission of SARs and some had in fact seen an increase in their reporting. Other firms mentioned very specific factors relating to a change in their own SAR trends such as specific tax reforms and changing client bases.

In addition to the reduction in the number of SARs, in February 2014, the NCA produced a report in which concern was raised about the quality of some consent SARs submitted by the legal sector. The poor quality in some cases meant that the NCA was not able to make a judgement as to whether or not consent should be given. A common problem was insufficient detail being provided, particularly in relation to SARs concerning conveyancing transactions.

According to the NCA, approximately 75% of all SARs from the legal sector were consent SARs. The NCA's analysis of SARs from the legal sector found that 42% of these SARs required follow up with firms because the initial report was incomplete. At times, the poor quality of SARs indicated a lack of understanding or compliance with the MLR and PoCA by the solicitor or firm submitting the SAR.

The situation did not significantly improve after 1 October 2014, following the publication of a guidance note outlining the minimum level of information required to enable consent to be considered and given. As a result the NCA has been returning consent SARs that do not contain sufficient information to enable them to decide whether or not to grant consent. This, of course, means additional work for the NCA and in turn presents a dilemma for solicitors and firms in whether to resubmit a returned consent SAR. This inevitably means additional work for firms and could hold up business. Or it could lead to an individual taking the risk of not resubmitting the consent SAR and potential subsequent criminal and disciplinary consequences.

The Law Society and others have produced guidelines which provide law firms with advice on how to complete an NCA consent SAR request.

✓ Good practice	✗ Poor practice
<ul style="list-style-type: none"> • The firm has an effective procedure of which staff are well informed which enables them to report suspicious transactions to the MLRO. • Records of reports are accessible by the MLRO and others as appropriate, yet secure and backed up. • The MLRO is visible and approachable, reports regularly to management and is well supported. • Confidentiality of reports is maintained with appropriate safeguards in place to prevent tipping off. • Reporting to NCA is timely. • SARs are sufficiently detailed to enable the NCA to determine whether to grant consent or not. • MLRO acts as a main point of contact in liaison with Legal Enforcement Agencies when dealing with formal and informal requests for information. 	<ul style="list-style-type: none"> • A hands-off or poorly-qualified MLRO. • Staff are unclear about reporting procedures and obligations, and do not feel confident to use them. • The MLRO keeps inaccessible, incomplete or inaccurate records. • A poor AML compliance culture, with no policy framework. • No policies or procedures in place to prevent tipping-off.

Record Keeping

Regulatory and Legislative Framework

- Record keeping is a fundamental element of an effective AML framework. Firms undertaking work in the regulated sector must keep comprehensive records of CDD, EDD and the supporting records (original documents or copies) about business relationships or occasional transactions that are the subject of CDD or ongoing monitoring.³³
- To ensure that the requirements specified in Regulation 19 MLR are met, these records should be maintained in a format that is easily accessible. The records should be backed up securely.
- CDD records should be retained for five years beginning on a specified start date, generally the date an occasional transaction completed or the business relationship ended.³⁴ Accurate records are also important in order to defend any criminal charges of money laundering, terrorist financing or acting in breach of the MLR.

Key Findings

Firms had adapted their retention of records policies to ensure that they complied with their obligations under the MLR, Data Protection Act 1998 and SRA Handbook 2011.³⁵

The firms we visited varied in their processes and procedures on recording CDD. The majority of firms maintained a centralised record of CDD in which records were quickly and easily retrievable to appropriate staff including the MLRO. Others kept CDD on individual client files with an electronic copy held on their case management systems.

We found that the standard of records in relation to internal suspicious activity reports that were held and maintained by MLROs varied. We noted that often verbal advice provided to fee earners, and discussions relating to money laundering issues, were not recorded in a

written format. This applied particularly when no further action was taken in regard to the enquiry. In other instances, exchanges of emails relating to internal Suspicious activity reports were stored in a specific email folder.

It is imperative that detailed records are kept by the MLRO when an employee submits an internal Suspicious Activity Report. These should include:

- the circumstances on which the suspicion is held
- the further enquires undertaken
- the information obtained
- the rationale behind clearly documented decision-making.

33. Regulation 19(2) MLR 2007

34. [Regulation 19 \(3\) \(a\) and \(b\) MLR 2007](#)

35. Outcome 7.5 of the Solicitors Code of Conduct 2011

Good practice

One firm ensured that CDD information is recorded centrally and securely. The firm also ensured that the information is backed up. Staff who need to access information were able to do so, and use the system to ensure that CDD is up to date and accurate.

The MLRO used CDD records to ensure that staff training was relevant and targeted to the firm's needs.

Poor practice

The CDD records of one firm were not easily accessible and were incomplete. Staff were unable to accurately say what CDD had been collected. Staff could not easily access the system to check and update CDD.

This firm could not show compliance with the MLR. Its CDD records were incomplete.

✓ Good practice

- Records are in a format that is secure but accessible.
- Records are backed up securely.
- CDD is recorded in a central location.
- MLRO maintains a register of internal SARs and external disclosures to the NCA including complete and thorough records of all enquiries made documenting key decision-making, rationale and action taken.

✗ Poor practice

- Records are inaccessible or hard to find.
- Records are incomplete or inaccurate.
- MLRO does not maintain any records in relation to internal SARs and external disclosures.

Conclusion

Honesty, independence and sound judgment are at the heart of the legal profession and it is therefore a fundamental requirement that it continues to demonstrate a rigorous approach to the prevention of money laundering.

Effective AML measures are essential to maintain the profession's global reputation as an open and competitive but safe market. Solicitors are often in the front line for providing this protection.

Overall, the results of our engagement are encouraging. The profession showed a good grasp of its obligations and regulatory requirements. However, this is not a reason for complacency. The methods used by criminals to launder money are constantly evolving and being refined. Firms will need to keep themselves updated about new developments and, with the impending enactment of the 4th Anti Money Laundering Directive, new regulatory requirements. Firms need to guard against seeing AML as a tick-box exercise rather than a continuing duty needing constant vigilance, active engagement and judgement. The reputational risk to firms, their principals and staff if they are found to have been used to launder criminal proceeds is obvious. The presence of an informed, engaged and approachable MLRO, an effective CDD policy, and regular staff training are essential requirements to safeguard firms.

We are aware that some aspects of the MLR prove more challenging for smaller firms, for example, MLRO succession planning or

providing relevant training for staff which is mandatory under the MLR. Despite these challenges we have seen many instances of good practice among small firms. We will continue to support small firms via the Small Firms Portal.

The risks faced by solicitors need to be minimised by ensuring they comply with the measures outlined in the legislation and the SRA Handbook 2011.

The profession needs to be alert to the risks of money laundering. Through constant vigilance, and embedding good AML practice at every level, firms can minimise the risks faced by the profession and the public. We will continue to work with the profession to promote good practice and compliance.

Ultimately, good AML practice will protect you, your firm, and the profession.



Preventing Money Laundering and Financing of Terrorism

A thematic review

March 2018

Contents

Glossary.....	3
Introduction	4
Executive Summary	7
Governance.....	10
Risk Based.....	15
Customer Due Diligence	18
Source of funds and wealth	25
Training.....	28
Suspicious Activity Reports	33
Conclusion	36
Appendix 1 – Sample data	37

Glossary

AML	Anti Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
DAML	Defence Against Money Laundering
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation 2018
MLCO	Money Laundering Compliance Officer
4MLD	Fourth Money Laundering Directive
MLR 2017	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
MLRO	Money Laundering Reporting Officer
NCA	National Crime Agency
PEP	Politically Exposed Person
POCA	Proceeds of Crime Act 2002
PQE	Post Qualification Experience
PSC	Persons with Significant Control
SAR	Suspicious Activity Report
TACT	Terrorism Act 2000
UBO	Ultimate Beneficial Owner
UKFIU	United Kingdom Financial Intelligence Unit

Introduction

The strength of the United Kingdom's (UK's) legal and financial institutions has made it a centre of world commerce.

As a key stakeholder within the UK's financial market, solicitors of England and Wales are central to many transactions and must be vigilant to the risks of money laundering and terrorist financing. The government have acknowledged this and assessed the legal profession to be a high-risk sector.

The legal profession plays a vital role in tackling money laundering. Solicitors handle large sums of client money and the reputation of the profession can give a sense of credibility to any transaction carried out through a solicitor's firm. This makes solicitors' firms an attractive target for criminals seeking to launder the proceeds of crime into the legitimate economy. In addition to the damage done to wider society, security and the economy by failing to identify and address money laundering, any loss of confidence in the solicitors' profession could be catastrophic not only nationally, but globally.

Money laundering is not a victimless crime and effective anti-money laundering (AML) processes and procedures help to disrupt terrorism and crimes such as drug dealing and people trafficking.

The vast majority of firms take steps to prevent money laundering and play their part in tackling this issue. The tiny minority who fail to do so and damage the trust placed in the profession will be subject to robust enforcement action by us.

Our role

We set and enforce against the high professional standards we and the public expect from solicitors. The 186,000 solicitors and 10,400 firms we regulate must adhere to our principles and code of conduct.

In addition to taking action when solicitors or firms fall short of the standards we set, we provide guidance, raise awareness of risks, issue warning notices about activity that causes us concern and undertake thematic reviews of key parts of the legal market.

Money laundering is a high risk for both society and the profession. We have highlighted it as a Priority Risk in our Risk Outlook 2017/2018¹. We also issued a warning notice to the profession in December 2014² (Warning Notice). The Warning

¹ <https://www.sra.org.uk/risk/outlook/risk-outlook-2017-2018.page>

² Money laundering and terrorist financing – SRA warning notice – December 2014

Notice identified an increasing number of firms failing to have adequate systems and controls to prevent, detect and report money laundering.

Solicitors must comply with their legal obligations under the Proceeds of Crime Act (POCA) 2002, the Terrorism Act (TACT) 2000 and, where applicable, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)³. This includes not facilitating money laundering, and applies to high risk services, such as conveyancing and offering trust and company services.

The Law Society is the named supervisor for solicitors in the MLR 2017 and delegates supervision of AML to us. The MLR 2017 places obligations on supervisory authorities to monitor and ensure the compliance, via regulatory measures, of their members with the AML and Countering the Financing of Terrorism (CFT) requirements.

In addition to our investigatory work, we also proactively visit firms to check compliance and understand the risks and difficulties the profession faces. We carried out a thematic AML review in 2015. During this exercise, we engaged with 252 firms in total and produced a thematic report in 2016 of our findings⁴. During July and August 2017, we visited 50 firms across the profession to examine their AML and CFT processes and procedures. This report contains our findings from those visits and builds on our 2016 thematic AML report.

The wider world

On 26 June 2017, the UK government introduced the MLR 2017. These regulations implement the Fourth Money Laundering Directive (4MLD) and reflect the standards required by the Financial Action Task Force (FATF).

The FATF is an independent international body which develops and promotes policies to combat money laundering and terrorist financing. In Spring 2018, the FATF will conduct a peer review of the UK to assess the effectiveness of our systems and legislation for preventing financial crime.

In 2013, the FATF produced a report highlighting the vulnerabilities of the international legal profession. It concluded that law firms are attractive targets for those wishing to launder the proceeds of crime or otherwise disguise improper transfers of money. The legal sector will come under further scrutiny during the 2018 visit.

³ Outcome 7.5 of the SRA Code of Conduct 2011

⁴ Anti-Money Laundering Report, May 2016

www.sra.org.uk/documents/SRA/research/anti-money-laundering-report.pdf

Summary of the new MLR 2017

The newly implemented MLR 2017 requires relevant firms to adopt a greater risk based approach to AML and CFT compliance. The new requirements are also more prescriptive and firms must make sure that decisions and policies are recorded in writing.

Some of the more substantial changes that have been introduced include:

- a requirement for a practice-wide risk assessment
- the obligation to appoint an individual at the level of 'senior management' as the officer responsible for compliance with the MLR 2017. This individual will be the Money Laundering Compliance Officer (MLCO) and is required by a firm where it is appropriate “with regard to the size and nature of its business⁵”
- amendments to the way in which simplified due diligence may be applied.

⁵ Regulation 21(1)

Executive Summary

Our approach to the review

AML and CFT compliance is an important area and as the methods of criminals develop, so too must the response.

The MLR 2017 were introduced in June 2017 following a short lead-in time. We acknowledge that firms have been given a limited opportunity to implement the new requirements and will take a proportionate approach to enforcement. However, firms must make sure the new requirements are met as a matter of urgency. We expect firms to show us the steps they have and will take to meet their new obligations.

In July 2017, following the introduction of the MLR 2017, we began visiting 50 firms. During the visits we met with the management at each firm, interviewed 50 fee earners and reviewed 100 client matters. The firms were made up of 25 large firms and 25 medium and smaller firms (including two sole practitioners). Twenty-five of the firms we visited were revisits from our 2016 thematic AML review. We wanted to examine their progress in the last two years and build on our 2016 review and report. We also wanted to provide firms with self assessment questions to assist them with their work to fully comply with the MLR 2017.

Headline summary

- Overall, most firms we visited are taking appropriate steps to understand and reduce the risk of money laundering, and to comply with the new regulations.
- We were also encouraged that some firms are going beyond the minimum requirements, for example to test training and compliance.
- We found examples of good practice, including having a variety of ways to establish the source of a client's funds and wealth.
- Yet we did find areas of concern. Not all firms were keeping records of their decisions, and many had not made progress with putting a firm-wide risk assessment in place. We recognise that they had been given limited opportunity to implement the new regulations, but we expect firms to move towards compliance as a matter of urgency.
- Firms are generally carrying out appropriate customer due diligence (CDD).
- There were also a small number of firms who have a significant amount of work to do to improve both processes and practice. These issues ranged in scale. In six of the most serious cases we have taken firms into our

disciplinary process. We will take appropriate action against individuals and firms who fail to meet the minimum standards and fail to comply on an ongoing basis.

- We urge firms to be continually vigilant and review their systems and processes on a regular basis. Any weakness in a firm's systems or processes could have significant consequences.

Summary of findings by area

Our discussions during our visits centred around the following key areas:

Governance

Most firms we visited had appropriate systems in place to reduce the risk of money laundering and terrorist financing. From 2018, many firms will be required to register MLCOs with us. This is a new role and will be in addition to the Money Laundering Reporting Officer (MLRO). The MLCO will be at board level (or hold equivalent status) and will be responsible for AML and CFT compliance. Encouragingly, many firms had already considered and identified their likely nominees.

Risk based approach

Firms continue to respond to the new prescriptive requirements of the MLR 2017. Most firms had an appropriate understanding about the risks their firms faced. We encourage firms to consider the risks at a firm and department level. Although some firms must still make changes to meet the new obligations, we were generally satisfied by the plans and timescales we saw. It is important that firms prioritise these changes and in particular the newly required written risk assessment for the firm.

The requirement for a practice-wide risk assessment is separate to the need to risk assess clients or transactions. Of the 100 files we reviewed, there was evidence that the level of risk was assessed on only 69 of these files, which was less than we would have liked to have seen. All firms should consider keeping written records of decisions, risk assessment processes and what due diligence was undertaken for each client/matter.

Customer due diligence

Overall, we were satisfied by the approach of firms to this area. Although the MLR 2017 has introduced significant changes, firms largely appear to be dealing with this area soundly. Firms acknowledge that this activity was an everyday practice and clients expected these checks.

Firms are obliged to continually monitor CDD and most firms dealt with these requirements well.

Source of funds and wealth

Most firms understood these areas and took steps to investigate the source and origin of client funds. Firms noted that clients largely expected these checks and client refusal to provide information about source of funds and wealth caused many firms alarm. Most firms understood the distinction between funds and wealth and we were pleased to see the depth of the fee earner's investigations. Some firms said that these checks, although onerous, could be turned into a positive marketing opportunity to cross market other services that the firm could offer.

Training

AML and CFT training was undertaken regularly and fee earners were universally positive about the firms' approach. Firms must continue to update their training and consider whether specific individuals require enhanced training. We also expect firms to consider how relevant and useful their training is. We saw good examples of firms tailoring training to address the specific risks that their staff faced in different areas of practice.

Suspicious Activity Reports

Many firms had developed effective internal processes and demonstrated appropriate AML/CFT risk tolerances. We were pleased to see that most MLROs took appropriate steps to safely record and store the decisions they took.

There was no typical number of Suspicious Activity Reports (SARs) and the nature of our visits did not allow us to make qualitative assessments about the number of reports made. However, firms should continue to challenge themselves and consider the implications of the volume of internal reports that are made. We consider the challenges and opportunities of the modern-day profession should inevitably lead to internal queries from fee earners.

We will continue to work with the National Crime Agency (NCA) to address individual concerns about the quality of SARs from law firms and promote best practice.

The future

This project represents just part of our ongoing work in this area. We will continue to work with firms who fall short of the expected standards, and take action where appropriate.

We also continue to respond to complaints and concerns raised by clients and other third parties. If you have concerns and would like to raise them with us, you can do this by e-mail (report@sra.org.uk) or anonymously via our red alert line on 0345 850 0999 or e-mail (redalert@sra.org.uk).

Governance

“It is very time consuming but that is fine. You have to be on the ball. The risks are too great and the impact of doing it wrong could end your career.”

A strong AML/CFT culture reduces risk, aids compliance and protects reputation. Firms should create an environment where staff are aware of their AML/CFT responsibilities and can understand and fulfil them. Building a strong AML/CFT culture involves several elements. Key strands include having a well-briefed, trained MLRO and appropriate policies and procedures in place based on the firm’s risk assessment. These need to be monitored, improved and enforced.

MLRO selection, preparation and support

Firms chose MLROs based on various qualities. This included selecting:

- a partner because of their seniority and level of responsibility (31 firms)
- individuals with previous MLRO/deputy MLRO experience (11 firms)
- individuals from a compliance background (20 firms)
- individuals with a senior management role (44 firms).

Firms also chose individuals because of their practice experience. Fourteen firms chose litigators and four chose a conveyancer. Some firms believed that a contentious background helped provide the MLRO with the skills to carry out the technical role and interact with third parties. Other firms preferred a conveyancing background because they felt this area represented the highest money laundering risk.

MLROs must make sure that they have sufficient time to devote to the role and consider any other positions they hold. Many MLROs had other roles:

- Compliance Office for Legal Practice (nine firms)
- Compliance Officer for Financial Accounts (four firms)
- both compliance officer roles (five firms)
- partner (20 firms)
- a management role (28 firms).

This is not necessarily a problem in principle, but might become a potential issue if an MLRO is overburdened. If the MLRO carries out several roles they may not be able to give sufficient time and consideration to the role.

The MLRO role is important and onerous. We expect individuals to properly prepare for the role. MLROs said they did this by:

- undertaking training
- serving as deputy MLRO
- reading AML/CFT legislation and guidance
- joining an AML/CFT group.

An effective MLRO needs time to carry out the role. Firms should consider offering practical support to MLROs by reviewing their workload and responsibilities. We saw various examples of this:

- MLROs could seek advice from external experts (28 MLROs)
- a reduction in billable hours (14 MLROs)
- no fee earning commitments (14 MLROs).

Sixteen firms did nothing specifically to assist the MLRO. We acknowledge that this may not always be necessary given the circumstances of each firm. Appropriate systems and processes can reduce the emphasis placed on the MLRO and help the firm build a coherent approach to AML/CFT compliance.

A deputy MLRO provides important support to the MLRO, cover in the absence of the MLRO and helps to address succession planning. We highlighted this in our 2016 AML report⁶. Six firms said they had no deputy MLRO. Firms should also make sure that everyone knows who the MLRO and deputy is. While 49 of the 50 fee earners were aware of the MLRO only 38 fee earners knew the firm's deputy MLRO. This highlights the need for firms to promote both roles. Firms should consider appointing a deputy MLRO if they have not already done so and address how they can mitigate the risks posed by the sudden and/or prolonged absence of an MLRO.

⁶ Anti-Money Laundering Report, May 2016, pp.14
www.sra.org.uk/documents/SRA/research/anti-money-laundering-report.pdf

AML/CFT policy

All relevant firms should have:

- a clear and up to date AML/CFT policy in place
- undertaken a firm-wide written AML/CFT risk assessment of their business⁷. This should include consideration of their geographic areas of operation, customers, the types of services and products, and the nature of transactions. There should be a clear link between the risk assessment and the resultant policy.

This is a vital aspect of compliance. Not only is it a legal requirement but it also provides members of staff with a clear understanding about the firm's expectations. The policy should be accessible to all relevant staff and signposted so that it can be easily found.

Forty-eight firms had an AML/CFT compliance policy. One firm had no policy in place (although this was under review) and the other had extensive guides but no overall AML/CFT policy. We were encouraged that 45 firms had reviewed their AML/CFT policies in the last 12 months and 34 firms had reviewed the policy within the last month.

It was disappointing to note that only 11 firms said they had a firm-wide risk assessment in place and a further six firms were in the process of implementing one. This is a requirement under the MLR 2017 and firms must take urgent steps to comply.

Firms explained that they had taken various steps to incorporate changes brought in by the MLR 2017. Fourteen firms have purchased IT equipment and obtained specialist advice to help them comply. We were pleased to see that twenty firms have already considered and determined who will be the MLCO under the new regulations⁸. The level of progress amongst other firms varied.

We expect firms to comply with their legal obligations and are urging them to familiarise themselves with the new regulations and act as soon as possible. However, we recognise the short lead-in time businesses have been given to implement the new requirements and will take a proportionate approach with firms as they work to meet the requirements.

⁷ Reg 18 MLR 2017

⁸ Reg 21 MLR 2017

Monitoring and enforcement

We looked at what steps firms took to enforce their AML policies and procedures. Compliance is an ongoing activity and firms should make sure that staff meet the standards that are set. Enforcing a policy sends a clear message about expectation and is also a deterrent to individuals who might seek to cut corners or ignore the requirements. We consider this to be good practice and it helps evidence that firms are running their business in accordance with proper governance and sound risk management principles. Thirty-five firms had a designated audit function that monitored AML/CFT compliance:

- twenty-three firms said that the audit function was internal
- four said that it was external
- eight firms had both an internal and external audit function.

Thirty-three firms said they took other steps to test compliance with the firm's AML/CFT policies and procedures. That included:

- regular AML meetings with fee earners
- training and testing
- reviewing client opening forms
- undertaking an annual firm risk assessment
- technical file reviews
- monitoring by the finance/internal compliance teams
- weekly exceptions reporting.

The MLR 2017 has introduced a formal requirement for some firms to appoint an independent audit function to assess the adequacy and effectiveness of its policies, make AML and CFT recommendations and monitor compliance with the regulations. These requirements are proportionate depending on the size and nature of the firm's business and not all firms may need to have these controls⁹. We also asked firms if staff had breached the firm's AML/CFT policies. Nineteen firms said staff had. Issues were mainly resolved by way of discussions with staff. Other actions included providing additional training, referring the matter to us or reprimanding the individual.

⁹ Reg 21 MLR 2017

Develop and improve – self assessment questions

Roles

- Have you appointed a MLCO?
- Who is your deputy MLRO? How would others know?
- What support do you provide to the MLRO and the deputy?

Policies

- Have you updated your AML and CFT policies following the MLR 2017?
- Have you created a written firm risk assessment? Does it highlight the risks your firm faces and the mitigation you have taken?
- Is it easy for all staff to access and understand these policies?

Monitoring and Enforcement

- Could you prove staff understand and follow your policies?
- What do you do if staff fail to follow your policies?

Risk Based

“We do high volume work and the risk is too high to not do it properly. It isn't worth cutting corners.”

Understanding money laundering and terrorist financing risks are an essential part of developing and implementing a rigorous AML/CFT strategy. Different clients and transactions will present different AML/CFT risks. The MLR 2017 require firms to take a risk based approach to the risks presented by a client or transaction to make sure they are identified, assessed and mitigated.

Identifying and assessing risk

Firms considered a variety of factors when assessing the risks presented by clients and matters. Common risk factors reviewed included the:

- geographical location of the client
- client being based overseas or in a high risk jurisdiction
- appearance of the client on any sanctions list
- source of funds and source of wealth
- area of work involved (for example property)
- identity of the client and the circumstances in which they are instructing the firm
- nature of the transaction including complexity, value and purpose
- involvement of any Politically Exposed Person (PEP).

We found that firms assessed client/matter risks in several ways. This included:

- a review of the client/matter by the fee earner as part of the file opening procedure. Firms used risk checklists, risk matrices, point based scoring systems or an overall risk rating. Files are then categorised as either low, medium or high risk. High risk files tended to be passed by the fee earner to a more experienced individual or the MLRO for approval
- a review of the client/matter by the central risk team
- the partner in charge taking responsibility for risk assessment

- designating every matter/client as high risk so Enhanced Due Diligence (EDD) is applied to all transactions
- categorising all clients/matters in a particular area of work (for example conveyancing) as high risk
- applying specific additional departmental risk guidelines to each matter
- the firm's business acceptance team undertaking detailed research and assembling a comprehensive profile of the client. This report is then sent to the MLRO with a recommendation on whether the firm should act and, if so, what ongoing monitoring is required.

Recording risk

Forty-six firms performed risk assessments on new matters and 21 firms said they recorded those assessments in writing. Reasons for not performing a risk assessment included:

- the firm knew all their clients
- there was no tick box risk assessment
- the partners were responsible for sourcing all new work and would not bring in risky work
- the firm only undertook general risk assessments for introducers.

It is important that firms can demonstrate a consistently compliant approach with the MLR 2017. There is an inherent danger of over reliance on individual partners or fee earners assumed knowledge of the client.

Of the 100 files we reviewed, there was evidence that the level of risk was assessed on only 69 of these files, which fell short of expectations. All firms should consider keeping written records of decisions, risk assessment processes and what due diligence was undertaken for each client/matter.

High risk matters

Firms should understand and respond to high risk AML factors. Firms may categorise risks differently but the rationale should be clear. Firms should also consider how to mitigate the risk.

Firms considered the following factors when assessing if a matter was high risk:

- whether the client was a PEP

- whether the client was based overseas, in a high risk jurisdiction or appears on a sanctions list
- the area of work (for example property, sale of art or classic cars)
- the nature of the transaction including complexity, value and purpose
- unusual payment patterns.

Importantly, these factors need to be assessed at the outset and reviewed throughout the life of a matter.

Forty-seven firms said that senior managers at the firm had to approve certain high risk transactions. Firms also said that senior management approval was required for:

- any matter involving a PEP (14 firms)
- transactions with an overseas element (five firms)
- high-risk matters, for example unusual transaction, large value, high risk client or cash transaction (17 firms)
- high risk areas of work, for example commercial property (two firms).

Significantly, the MLR 2017 place a specific duty on firms where they seek to act for a PEP or their family or known associate. The fee earner must have approval from senior management, establish the source of wealth and conduct ongoing EDD. Firms must adhere to this process¹⁰.

Develop and improve – Self assessment questions

- Does each file have a written record of the AML/CFT risk?
- Do you consider and review the client, the transaction and the funds in each matter?
- How do you acknowledge and monitor the unique AML/CFT risks in different work areas?
- How do you control and monitor high risk matters?

¹⁰ Reg 35(5) MLR 2017

Customer Due Diligence

“It is built into our work. It all begins with the client.”

CDD is the information that firms must gather about their clients¹¹.

Where the client is an individual, firms must do all the following:

- **identify** the customer unless the identity of that customer is known to the firm, and has been verified by the firm
- **verify** the customer’s identity unless their identity has already been verified
- **assess**, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

Where the client is a commercial entity, firms must:

- **obtain** and **verify** the name of the body corporate, its company or registration number, and the address of its registered office, and if different, its principal place of business
- **identify and verify** the people with control of the body corporate, and the ultimate beneficial owner (UBO).

CDD information must be kept under regular review¹² to make sure that any transactions match the profile of the client and check the information is correct and up to date. This is referred to as ‘ongoing monitoring’.

CDD must be completed as soon as practicable after first contact, however the identity of the client can be completed during the establishment of the business relationship if it is low risk and necessary not to interrupt the normal conduct of business¹³. A business relationship is one expected to have an element of duration¹⁴. In practical terms, this means even the shortest instructions will form a business relationship, due to the solicitor's continuing obligations to the client after the retainer has ended.

EDD is explained in the MLR 2017¹⁵. It must be applied where a customer is high-risk, for example if they are a PEP or from a high-risk jurisdiction. What constitutes EDD depends on the risk factors of the client.

¹¹ Reg 28 MLR 2017

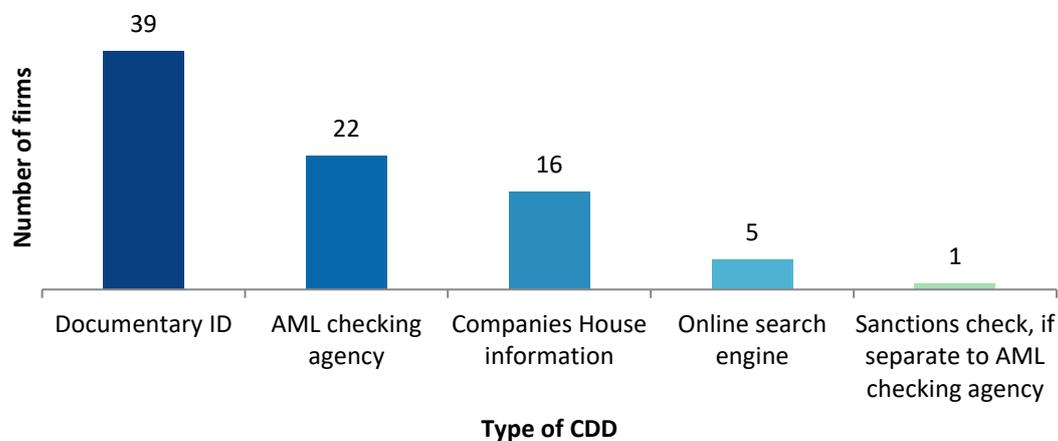
¹² Reg 28(11) MLR 2017

¹³ Reg 30 MLR 2017

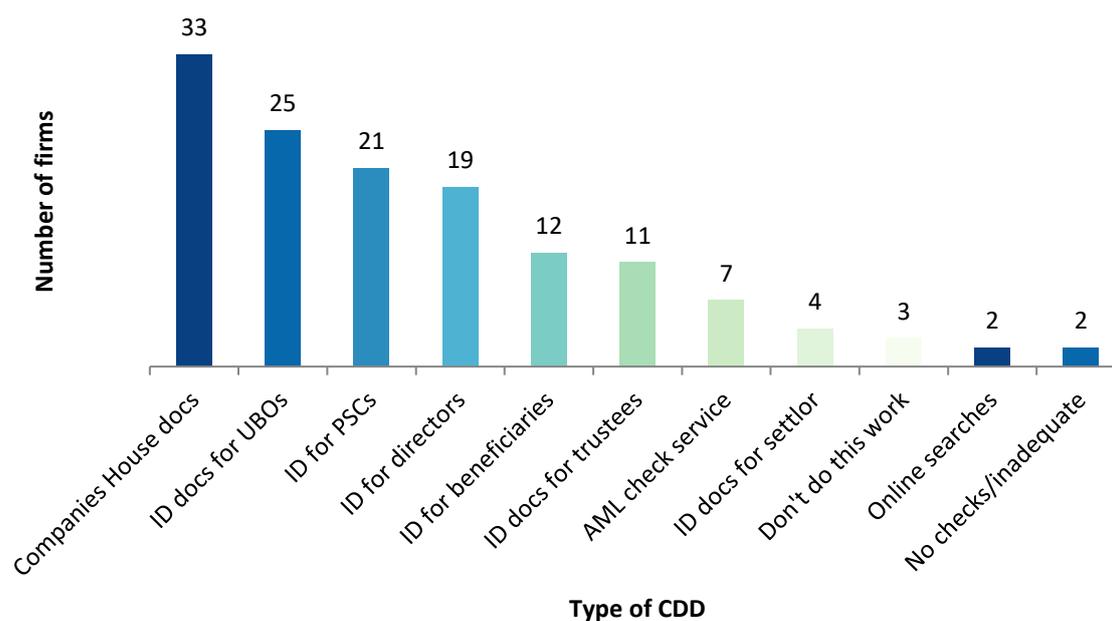
¹⁴ Reg 4 MLR 2017

¹⁵ Reg 33 – 35 MLR 2017

How do you collect CDD about clients?



How do you collect CDD about corporate and trust clients?



As the graphs above indicate, most firms used more than one method to identify the client. Using a variety of methods means that firms can verify information between documents. This improves the understanding of the firm and reduces the risk of unwittingly being involved in money laundering.

Several firms emphasised the importance of identifying persons with significant control (PSC) and UBOs of corporate clients. They characterised this as understanding the people behind the companies. This is particularly important where a client company may have several layers of corporate ownership.

A minority of firms only collected CDD for work in the regulated sector. While this is within the letter of the MLR 2017, it may increase risk. Unregulated work is still within the scope of the POCA 2002. Firms should consider the risk profile of work falling outside the scope of the MLR and take a proportionate approach to CDD.

Occasionally, clients were unable to provide photo ID in person. In these cases, firms would accept copies certified by a professional, for example another solicitor, accountant or notary. Prudent firms insisted that the copies should be sent in by the person who certified them. It is important to be clear that a firm relying on the due diligence carried out by a third party remains responsible for any failure¹⁶.

In most cases, CDD was completed when files were opened. Most firms had some form of system to prevent work being carried out before CDD was complete. This included:

- six firms not passing files to fee earners until CDD was complete, making work before this impossible
- twenty firms restricting all work, billing or receipt of funds prior to CDD completion
- four firms allowing only some administrative work, for example client care letters, before CDD was complete
- eight firms restricting the receipt of money on file until CDD was complete.

Although a firm may have a policy that prohibits work from being carried out, this range of measures physically prevented work from being carried out. We consider this best practice.

When we spoke to fee earners we found that 19 said they would do some work before CDD had been completed. Two of these said only administrative work was done, for example client care letters. The remaining 17 said that they would complete some substantive work, albeit with some restrictions, for example time limits or limits to money billed. CDD must be completed before a business relationship is established unless there is a low risk of money laundering and it's necessary not to interrupt the normal course of business¹⁷.

Ten fee earners said that a client had put them under undue pressure to begin work before CDD had been completed. Although there may be a rational explanation for this urgency, our Warning Notice highlights this as a suspicious behaviour. We were pleased that each fee earner said that they had refused to take the matter further until CDD was complete. One had also come under pressure from a partner who had sided with the client, but she had been able to refer to the firm's policies for support.

¹⁶ Reg 39 MLR 2017

¹⁷ Reg 30 MLR 2017

One fee earner told us that in this situation he said to clients: "If it is really urgent, you will comply urgently".

Of the 100 files we examined, six did not have complete CDD on file, and two involved work where CDD was not required. Of the six files without CDD, most had it stored centrally or on a previous client file. Two files relied entirely on a partner's knowledge of the client acknowledged in a signed statement. We consider:

- it is questionable whether anyone but that person signing those statements can genuinely identify the client
- even where the statement may identify the client, it arguably cannot verify their identity.

Several of the files had some sort of complex factor to the CDD. These included:

- a substantial house purchase funded by the client's father who lived overseas
- some cases involving high net worth client companies, their directors and beneficial owners spread across several jurisdictions
- one PEP
- overseas trusts and their controllers.

In all, 14 firms told us that they had refused instructions from a client because of failing to meet CDD requirements. This was for a variety of reasons, including:

- the documents provided showed three different dates of birth for one client
- monies to complete a property transaction were supposedly received as gifts from various relatives who would not provide CDD
- name changes on documentation completed by the client
- a complex company structure where the identity of beneficial owners was unclear.

Where firms refuse to act, firms should also consider whether they should make a SAR. There is an obligation to make a report where an individual knows, suspects or has reasonable grounds to know or suspect that another individual or person is engaged in money laundering. This is a broad requirement and firms should be able to explain why a matter was not reported in these circumstances. This requirement is discussed further below.

We also asked firms whether they checked clients against HM Treasury's sanctions list¹⁸. Forty-five firms checked the sanctions list. Of the remaining five:

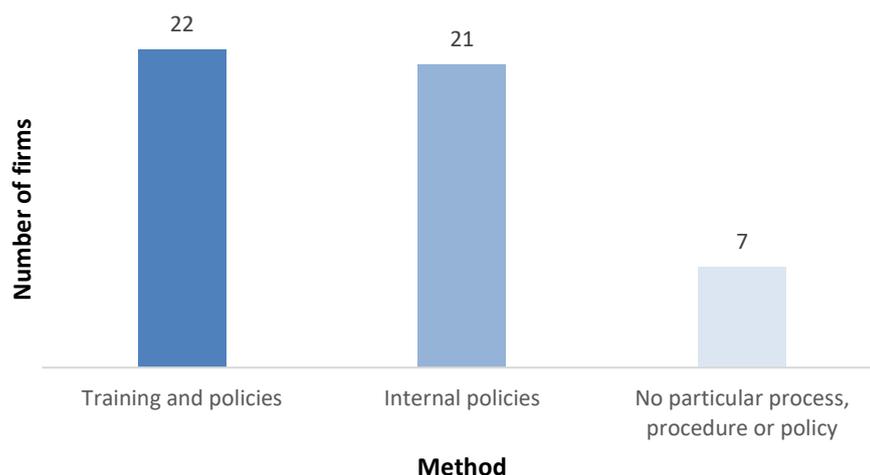
- three said that their clients would never appear on the sanctions list. We consider this to be a dangerous assumption
- one said that the matter had never arisen, but it was unclear how they would know without checking the sanctions list
- one said that their policy was under review.

The firms who did check the sanctions list tended to do so as part of an ID checking service, which typically also checked for media reports and creditworthiness. These agencies sometimes draw false positives as part of a search, for example when a client has the same name as a PEP. Firms said that when this happened, they would check the ID against the information they held, further online checks and/or speak to the client.

EDD is a live issue for many firms. Of the 50 we visited, 24 had clients who were PEPs.

Only 16 firms kept a central list of PEP clients. This is a useful practice which can help to assess and monitor the firm's risk more effectively. It may also speed up the CDD and EDD process for these clients.

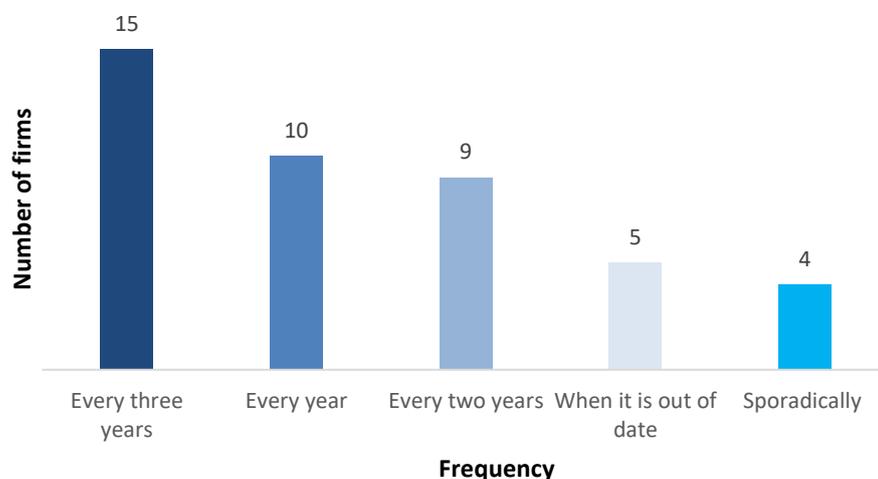
We asked firms how they made sure that staff knew what EDD was and when they should apply it:



Most of the firms had a process in place for monitoring CDD on an ongoing basis.

¹⁸ www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

When we spoke to firms, the majority (43) said they renewed CDD at regular intervals:



Three firms also had a risk based approach to ongoing monitoring ranging from three years for cases deemed to be medium or low risk but quarterly for high-risk files. For life events, such as change of name, change of gender, or change of address, only 34 firms said they would renew CDD - a lower proportion than we expected given the requirement under the MLR 2017. Seven firms would renew CDD for each new matter a client opened, but not otherwise. One firm had no renewal procedure at all.

From 25 May 2018, firms will be subject to the General Data Protection Regulation (GDPR)¹⁹. These regulations will have an impact on the data which firms must retain for AML/CFT purposes. The rights to erasure and objection will have a bearing on what information firms can hold about their clients. Firms will need to consider how to balance the requirements of the MLR 2017 and GDPR.

The MLR 2017²⁰ states that firms must make provision for data protection policies in relation to AML. Firms must also train their staff in relevant data protection legislation²¹. This will naturally include GDPR once it comes into force, though prudent firms are already doing this.

¹⁹ ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

²⁰ Reg 20(1)(b) MLR 2017

²¹ Reg 24(1)(a) MLR 2017

Develop and improve – Self assessment questions

- Does each file show how you have identified and verified the client?
- How do you identify a PEP, a family member or known close associate?
- Do your staff access the sanctions list?
- Can you monitor how frequently CDD is undertaken on high risk clients?
- Can you show how and when you undertake ongoing monitoring?

Source of funds and wealth

“It’s a major thing we have to deal with and it can take time for our clients to get the documents together.”

Solicitors may need to investigate source of funds and wealth as part of CDD²².

These terms are not defined in the MLR 2017, but the FATF gives the following definitions²³:

- *The source of funds refers to the origin of the particular funds or other assets...Normally it will be easier to obtain this information but it should not simply be limited to knowing from which financial institution it may have been transferred. The information obtained should be substantive and establish a provenance or reason for having been acquired.*
- *The source of wealth refers to the origin of the...entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the PEP acquired such wealth. Although [firms] may not have specific information about assets not deposited or processed by them, it may be possible to gather general information from commercial databases or other open sources.*

We consider that establishing both the sources of funds and wealth are a key part of a risk based AML regime. They are particularly helpful in establishing ongoing monitoring of CDD and transactions.

When reviewing files, we checked whether source of funds and wealth had been obtained:

	Yes	No	Not applicable
Source of funds	39	22	39
Source of wealth	28	28	44

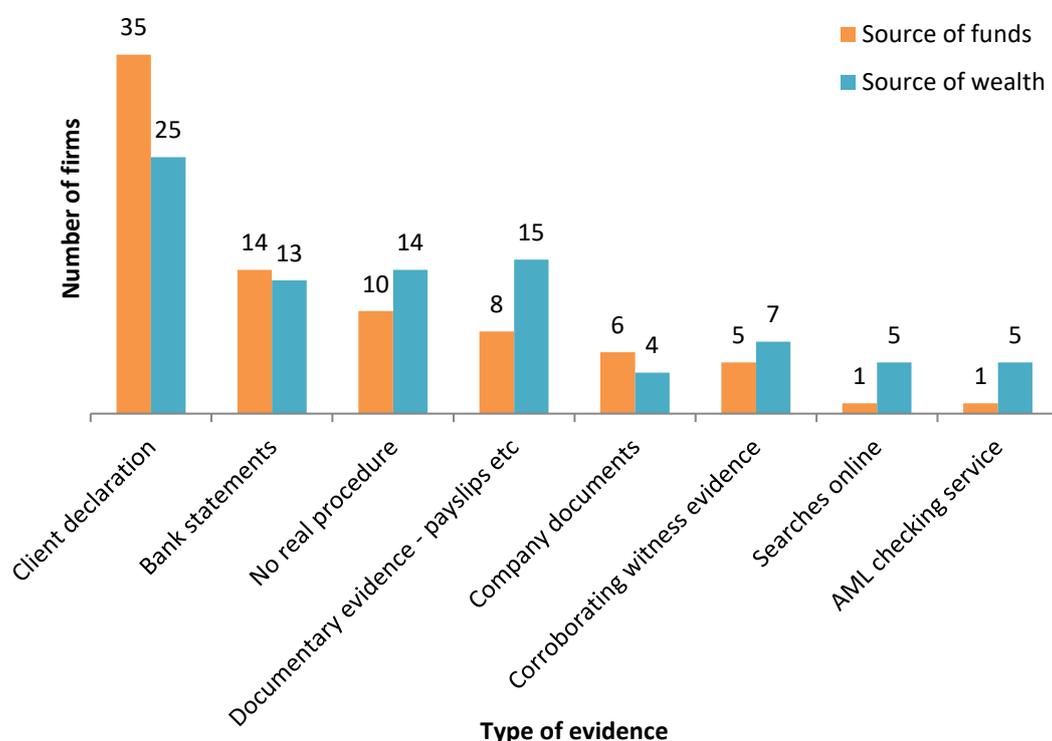
Where firms answered 'no' to source of funds, this was for legitimate reasons, for example where clients were selling a house and purchasing another the source of funds was obvious.

²² Reg 28(11) MLR 2017

²³ FATF Guidance: Politically Exposed Persons

www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

What evidence is gathered?



Client declarations are gathered by firms and include information from clients about the transaction, their source of funds, or whether they consider themselves to be a PEP. While these discussions can be useful they should not be relied upon exclusively. A money launderer is unlikely to worry about making a false declaration.

When firms attempted to establish the source of wealth they were more likely to carry out searches online and seek corroborative evidence. Firms were, however, less likely to have a set of specific procedures for establishing the source of wealth. By contrast, firms investigating source of funds tended to rely more on client declarations. However, most firms employed more than one method of establishing source of funds and wealth. Using a variety of methods gives a more rounded view of the client.

Five firms had difficulties separating the concepts of source of funds and source of wealth, and did not distinguish them. Two of these firms were reported into our disciplinary processes (as there were also other concerns) and the matter was directly addressed with the other three. Firms must understand and record where funds will be provided from and how those funds were obtained. This is a legal requirement. If a client cannot satisfy either part of this requirement the firm should not act. This type of client behaviour is expressly mentioned in our Warning Notice.

Thirteen firms requested both sources of funds and wealth at the same time and as part of the same process. This can be time-saving and beneficial and reduce requests of information from the client. A few firms provided clients with a sheet showing what evidence was likely to be asked for in different transactions.

One firm stated that: *“if the transaction makes sense, and there are no grounds to suspect that the monies are the proceeds of crime, there's no need to investigate the source of funds or the source of wealth”*. This is a misconception. For example, where a client is a PEP, source of funds and wealth must be established in each case regardless of suspicion. The decision whether to establish source of funds and wealth should also be based on risk, rather than suspicion. Solicitors and firms do not need to decide whether the client is guilty of money laundering, but they must assess the risk.

Develop and improve – Self assessment questions

- What is the difference between source of funds and source of wealth?
- Does each file record in writing where/who funds are from and how they were originally created?
- Do the fee earners understand the client, the transaction and the funds? If not, how do they continue to monitor and assess this information during the lifetime of the transaction?

Training

“Fee earners don’t view AML as exciting but they understand and appreciate the importance of doing it.”

Firms must provide staff with appropriate training about AML/CFT. The MLR 2017 requires that relevant employees are:

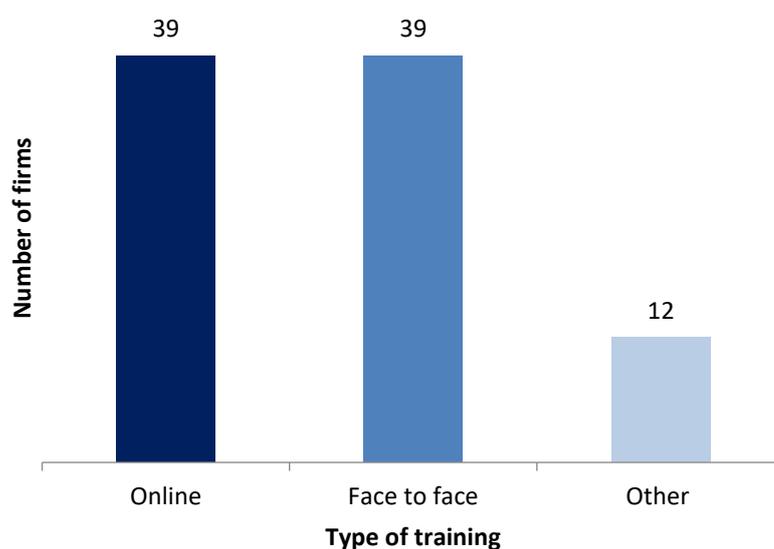
- made aware of the law relating to money laundering, terrorist financing and the requirements of data protection; and
- regularly trained about how to recognise and deal with transactions and other activities which may be related to money laundering and/or terrorist financing²⁴.

Firms must keep a record in writing about:

- how employees have been made aware of the law relating to AML/CFT; and
- the training given to employees.

AML/CFT training

Firms delivered training to staff in a variety of ways:



²⁴ Reg 24 MLR 2017

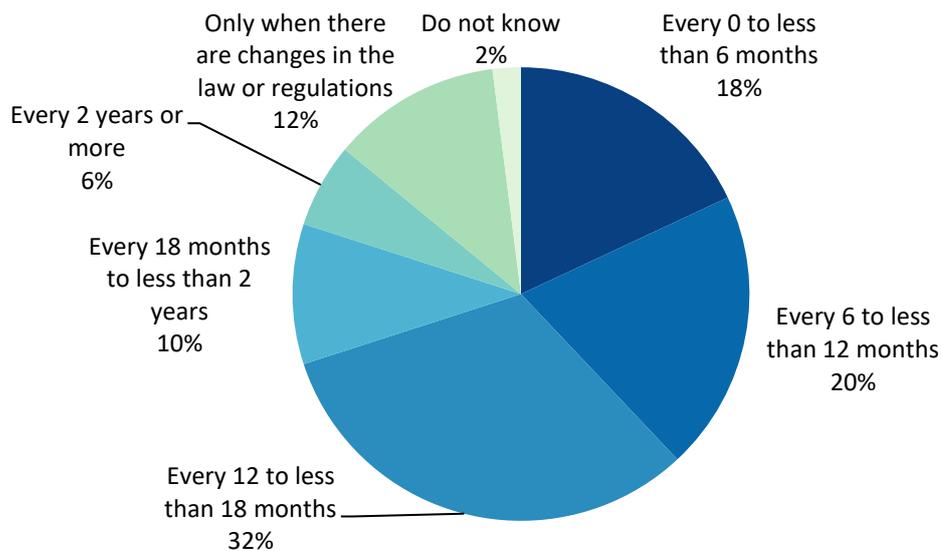
Other training included attending courses, circulating updates by email and memo as well as the use of training booklets and newsletters.

Forty firms said that AML/CFT training was compulsory for all staff including accounts and secretarial staff. Some firms delivered training to individuals based on their level of exposure to AML/CFT. For example, introductory training was provided to IT and facilities staff and fee earners and finance staff received advanced training.

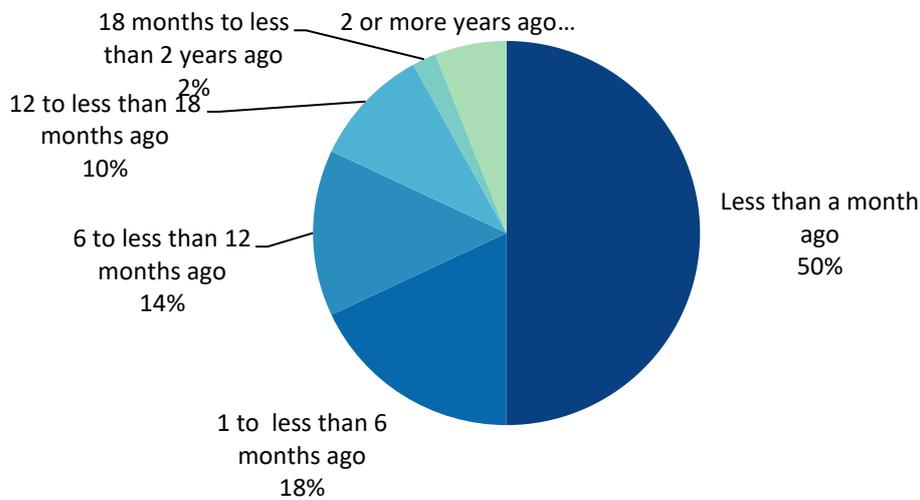
Ten firms did not make AML/CFT training compulsory for all staff because they had no, or limited, exposure to AML/CFT issues, for example staff working in IT, the post room or on reception were not given AML/CFT training. All staff who could potentially be involved in AML/CFT prevention should receive training. At one firm, for example, we found that secretaries were not trained in AML/CFT, even though they played a key role in collecting and processing CDD.

Frequency of training

Firms provided AML/CFT training with the following frequency:



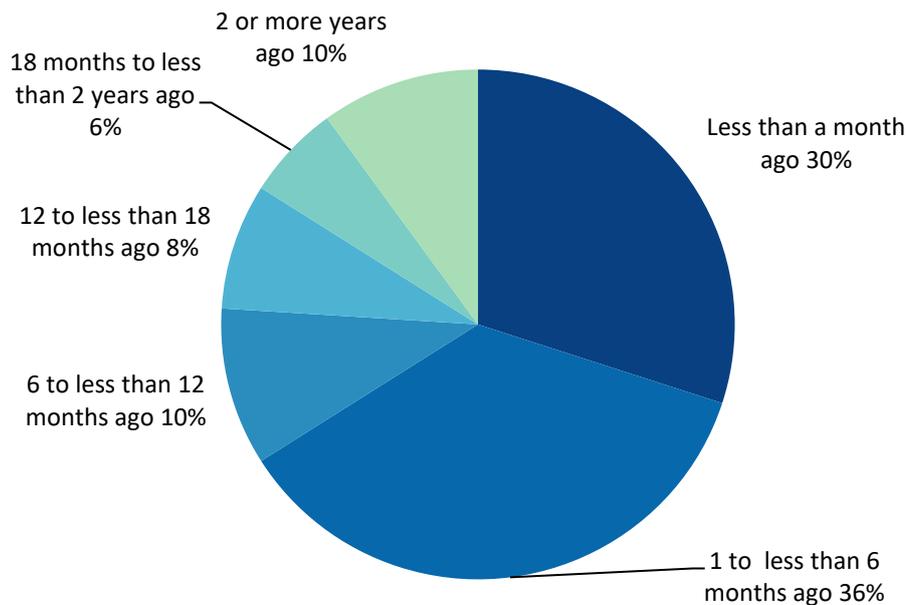
Staff were last provided with AML/CFT training:



Twenty five firms provided AML/CFT training less than a month before our visit which reflects steps they have taken to update staff on the changes introduced by the MLR 2017. Other firms confirmed they would provide further training once the guidance issued by the Legal Sector Affinity Group, which comprises the AML supervisors for the legal sector, was published.

MLRO training

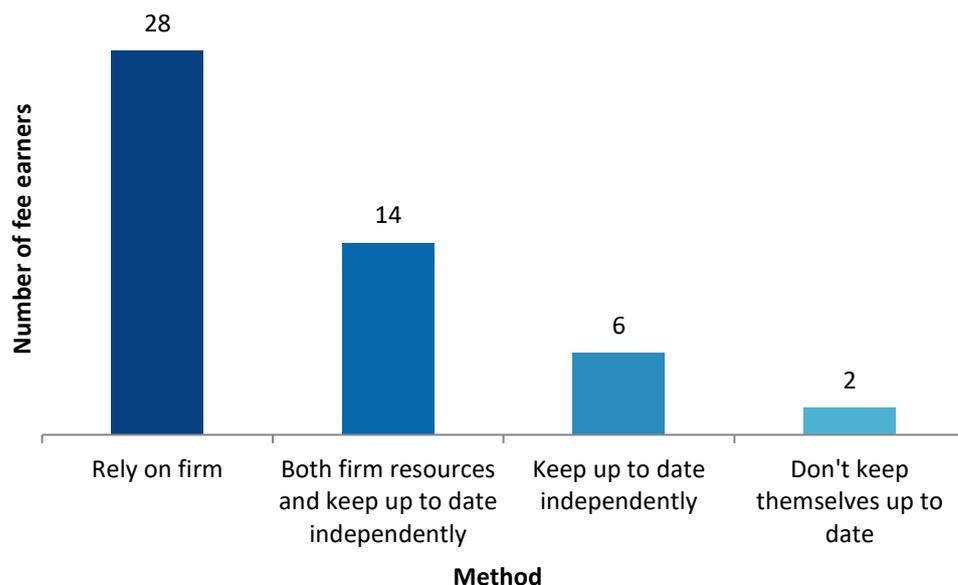
MLROs provided details of when they last attended AML/CFT training:



Thirty-eight MLROs attended training in the last 12 months which, in part, was to better understand the changes brought about by the MLR 2017.

Fee earners

Fee earners said they kept up to date with AML/CFT in different ways:



Record keeping

Forty-three firms kept records of staff attendance at AML/CFT training. Those who did not keep records gave a variety of reasons for not doing so including that the MLRO could easily identify these individuals or that the firm was a small practice so attendance records were unnecessary. Other firms stated that while they did not currently keep records they are in the process of introducing a new centralised record. Keeping a written record of attendance at AML/CFT training serves as a useful way of recording what AML/CFT training has been given to staff and will show the steps the firm has taken.

Testing knowledge

Thirty-six firms said they undertook testing to make sure that staff members understood the training. Thirteen firms did not undertake any testing and one firm did not know. Testing usually comprised of an assessment, file reviews/audits or a review of the client inception forms. Firms used one or a combination of these methods. Thirty-three firms did online tests, seven firms undertook audit/file reviews, one firm did it by reviewing CDD inception forms and two firms had a verbal test after the training had been completed. Firms that did not carry out any testing gave a variety of explanations:

- their online AML/CFT training package did not offer an assessment
- they felt they were too small for it to be necessary
- testing is not part of the firm's culture
- a test is not a fair reflection of understanding
- they prefer to do regular refresher training.

Testing knowledge is significant. It encourages individuals to invest time and effort in to the training and provides firms with an overview of where further training may be necessary. We consider this to be good practice.

Develop and improve – Self assessment questions

- Who is the vulnerable link at your firm and are they trained?
- Does the training relate to the specific risks at your firm?
- How long can a member of staff avoid AML/CFT training?
- Do you record if people have completed training? If so, when do you review the record?
- Does the MLRO review and contribute to the training?

Suspicious Activity Reports

“I see AML/CFT as an important component in a lawyer’s wider responsibilities - it builds integrity into the legal system.”

A core part of the AML/CFT system is the reporting of suspected money laundering activities.

The United Kingdom Financial Intelligence Unit (UKFIU)²⁵ is responsible for gathering reports about these activities. To make a report an MLRO must make a SAR. Firms may make either a defence against a money laundering (DAML) SAR or an intelligence SAR.

There are two parts of the process:

- internal reports by staff to their MLRO
- reports by the MLRO to the UKFIU.

Significantly, a report by an employee may not necessarily result in a referral to the UKFIU. It is part of the MLRO’s role to decide which reports should be taken forward.

Making referrals

There are several obligations that individuals at firms must meet:

- staff must make a disclosure to the MLRO where they know or suspect a person may be involved in money laundering
- the MLRO must make a disclosure to the UKFIU where they know or suspect a person may be involved in money laundering
- it is an offence to bring a disclosure to the subject’s attention – this is known as tipping off.

The NCA has produced detailed guidance on how to make an effective SAR²⁶.

Overview

As expected the large firms in the sample have greater experience of this area because of the amount of work they carry out and this was reflected in the data:

²⁵ The UKFIU is part of the NCA

²⁶ www.nationalcrimeagency.gov.uk/publications/732-guidance-on-submitting-better-quality-sars?file

- 59% of MLROs had submitted a DAML SAR (this included 78% of MLROs at large firms and 46% of MLROs at other firms)
- 38% of MLROs had submitted an intelligence SAR (this included 50% of large firms and 30% of other firms)
- A total of 337 DAML SARs had been made (large firms: 156 DAML, the remaining firms had made 181). We asked firms whether they had ever had a DAML SAR refused by the NCA. Three large firms had been refused consent to act on four occasions. Five small/medium firms had been refused consent on six occasions
- A total of 92 intelligence SARs had been made (large firms: 49).

We asked firms about two specific scenarios and whether they had ever made a report:

1. Have you ever needed to stop acting for a client due to a risk factor? (Yes: 66%). Did you make a report? (Yes: 28%)
2. Have you ever ended a business relationship as a result of being unable to satisfactorily apply CDD? (Yes: 28%). Did you make a report? (Yes: 21%).

Firms did not believe that either scenario automatically required a report to the UKFIU. Firms told us that they might turn away a client due to the work exceeding the firm's risk appetite. This is particularly likely where firms calculate risk scores with a mathematical matrix. Despite exceeding the risk threshold for the firm, they told us that this did not mean that the individual was suspected of carrying out criminal activities. However, each firm commonly assessed whether there was any suspicion of criminality.

Firms also explained that clients might not complete the firm's CDD process for numerous reasons. Clients may have decided not to carry on the transaction or continued the matter at another firm. Again, firms did not suspect that clients were engaging in criminal activity.

As mentioned above, there is an obligation to make a report where an individual knows, suspects or has reasonable grounds to know or suspect that another individual or person is engaged in money laundering. While firms may consider that individuals are not carrying out criminal activities, we consider this to be a broad requirement and firms should be able to explain why a matter was not reported.

Tipping off

It is an offence for a person in the regulated sector to tell a person suspected of money laundering that a SAR has been made or that a money laundering

investigation is under way. The penalty for tipping off can be an unlimited fine and/or up to five years' imprisonment.

When a MLRO makes a DAML SAR, progress on a client's matter must be suspended until the NCA provide consent to act. During this time period, the firm are unable to carry out any further work which would be a principal money laundering or terrorist property offence, or explain the true reason for the delay. This problem is likely to increase as recent changes to the law extend the amount of time that the NCA may take to reply to a DAML SAR. The NCA have seven working days following the working day after the disclosure to process the transaction. If consent is refused, the NCA have a further 31 calendar days to carry out further work.

Most firms – 88% – had specifically addressed the risk of tipping off. This included providing specific training or processes that were designed to help staff. Given that many firms had faced this practical issue it is important that firms and fee earners understand the risks and their obligations.

Records about internal disclosures

We expect many firms will have to deal with an internal SAR. This simply reflects the nature of the work. The data we gathered suggested our assumption was correct and firms had taken steps to prepare themselves:

- 88% of MLROs had a system in place to record internal discussions with staff
- 72% of MLROs had received an internal SAR within the past five years from staff (this included 90% of MLROs at large firms and 60% of MLROs at small/medium firms).

We consider it good practice for MLROs to keep records about the referrals they receive and the reasons for onward reporting, or not, regardless of whether they subsequently refer the matter to the UKFIU. Significantly, these records may provide the MLRO, fee earner and firm with a defence to an allegation of failure to disclose, so they should be thorough, clear and stored somewhere securely and safely.

Develop and improve – Self assessment questions

- Are you registered with SAR online?
- Do all staff understand tipping off?
- Can you show which matters have not been referred to the NCA and why?
- In the event of an emergency how would referrals be made and/or reviewed?

Conclusion

There is no substitute for reading and understanding the MLR 2017. The AML and CFT obligations are required by law for those firms within scope and they must be followed. We also encourage firms to go beyond the minimum requirements of the MLR 2017 and consider best practice.

Significantly, it is not possible to prescribe a universal method or system of compliance because the size and nature of firms varies. However, the new rules are clear. Firms must consider the risks they face and take steps to record and mitigate them.

We were satisfied generally that most firms had showed the right approach to AML and CFT compliance. Despite the relatively new legislation, the majority of firms had already made changes to their systems and procedures. This was encouraging and we expect all relevant firms to prioritise complying with the new AML and CFT requirements. Firms must take steps to comply with the new obligations as soon as possible and in the meantime be in a position to show progress and future plans.

We were encouraged by the number of firms who had decided to implement policies and procedures well above the minimum requirements. These firms recognised that good AML and CFT processes and procedures could generate business opportunities. Where firms took time to know their client, it provided them with a chance to market other services to individuals such as private client and conveyancing work.

There are a small number of firms that will require additional attention from us and we will continue to work with them. A failure to meet the minimum standards required by the MLR 2017 is a serious issue and we will take appropriate regulatory action against individuals and firms who fail to implement them. As a result of this review, we have referred six firms into our disciplinary processes.

Appendix 1 – Sample data

We visited 50 firms with a combined total of 11,731 fee earners (the largest firm we visited had 1390 fee earners). Further information about the firms and fee earners are provided below.

Firms

(i) *Type of firms*

Type of firms	Percent	Count
Partnership	12.0%	6
Limited Liability Partnership	72.0%	36
Limited Company	12.0%	6
Sole Practitioner	4.0%	2

(ii) *Firms by number of managers*

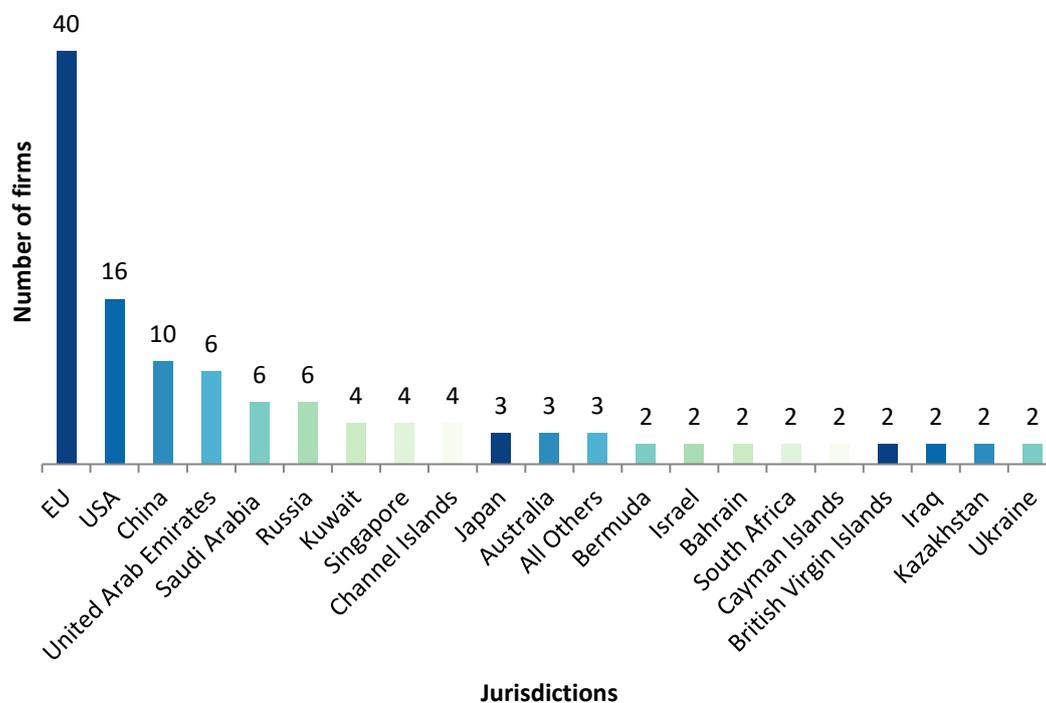
Number of managers	Percent	Count
1 to 5	34.0%	17
6 to 10	10.0%	5
11 to 25	14.0%	7
26 to 50	16.0%	8
50 +	26.0%	13

(iii) *Firms by client location*

3. Forty-one firms had overseas clients. Of these firms:

- Eleven did not keep a specific central record of where their clients were located. A record of a client's location is useful because it might help firms to assess and monitor various compliance risks.
- Twelve had clients from high risk and non-cooperative jurisdictions designated by the FATF.

We asked firms to provide information about the location of their top three overseas clients:



(iv) *Firms by work type area*

Firms operated in a broad range of areas:

Area	Total responses
Bankruptcy/insolvency	31
Civil litigation	40
Commercial	39
Corporate	39
Consumer	26
Criminal	28
Debt collection	28
Discrimination/civil liberties/human rights	26
Employment	41
Family/matrimonial/children	38
Financial advice and services	28

Intellectual property	33
Landlord & tenant	35
Litigation - other	36
Mental health	27
Immigration	30
Personal injury	30
Planning	28
Probate and estate administration	38
Property - commercial	45
Property - residential	43
Social welfare	28
Trust and company service providers	28
Wills, trusts and tax planning	42
Other	35

Fee earners

We interviewed 50 fee earners and viewed 100 client files. They ranged in experience and work type:

(i) Fee earner by Post Qualification Experience (PQE)

Number of years PQE	Percent	Count
0 to less than 1 year PQE	12.0%	6
1 to less than 3 years PQE	14.0%	7
3 to less than 6 years PQE	14.0%	7
6 to less than 9 years PQE	18.0%	9
9 to less than 12 years PQE	14.0%	7
12 or more years PQE	28.0%	14

(ii) Fee earner by time at firm

Time at firm	Percent	Count
0 to less than 1 year	6.0%	3
1 to less than 3 years	26.0%	13
3 to less than 6 years	38.0%	19
6 to less than 9 years	4.0%	2
9 to less than 12 years	8.0%	4
12 or more years	18.0%	9

(iii) Fee earner by main practice area

Practice area	Percent	Count
Corporate law	16.0%	8
Property - commercial	22.0%	11
Property - residential	50.0%	25
Wills, trusts and tax planning	2.0%	1
Other	10.0%	5

Risk assessment

Anti-money laundering and terrorist financing

2 March 2018

Read our report: Preventing Money Laundering and Financing of Terrorism [[/sra/how-we-work/reports/preventing-money-laundering-financing-terrorism/](#)]

What is the purpose of this document?

This document sets out information on money laundering and terrorist financing risk that we consider relevant to those we supervise.

Money laundering is the means by which criminals make the proceeds of crime appear legitimate. The National Crime Agency (NCA) believes that money laundering costs the UK £24 billion a year¹ [#n1]. Through preventing money laundering, we can take away criminals' incentives to traffic weapons, trade drugs or engage in human trafficking. Money laundering also includes the funding of terrorism, irrespective of the source of funds. So by preventing money laundering we help reduce corruption and create a better, safer society.

The SRA is responsible for the supervision of anti-money laundering (AML), and we take our responsibilities very seriously. We owe a duty to society at large, and to protect the integrity of the legal sector through tackling professional enablers of money laundering. If the UK legal sector is to remain a trusted profession, we must work to identify those who would willingly help money launderers, and inform and educate those who might be unwittingly used by criminals.

This is the first AML sectoral risk assessment published by the SRA, and we will refresh it on a regular basis to keep up-to-date with emerging risks and trends.

The sectoral risk assessment should form the basis for firms' own risk assessments along with the national risk assessment² [#n2] and a comprehensive knowledge of their services, clients and delivery channels.

The risk-based approach is embedded in UK legislation and AML best practice. It means that firms should target their resources to the areas or products that are most likely to be used to launder money. Similarly, the SRA takes a risk-based approach to direct our resources to have the most intense supervision of the firms that are most likely to be used to launder money. We will ask to see firms' written risk assessment as part of our routine monitoring programme, or in response to specific information we have received. Your firm's risk assessment should not be disclosed to customers, or third parties.

Who does it apply to?

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017³ [#n3] ("the money laundering regulations") place obligations on firms offering services that are most likely to be targeted by those wishing to launder money.

These include independent legal professionals⁴ [#n4], and trust or company service providers⁵ [#n5]. All firms that are within scope of the money laundering regulations must take appropriate steps to identify and assess their risk of being used for money laundering or terrorist financing. The firm's risk assessment must be in writing, and when preparing it, you must take into account this risk assessment prepared by the SRA in the role of your AML supervisor.

Risk in the legal sector

The 2017 national risk assessment said:

Legal services remain attractive to criminals due to the credibility and respectability they can convey, helping to distance funds from their illicit source and integrate them into the legitimate economy.

The national risk assessment goes on to say that although there is some deliberate involvement in money laundering within the legal sector, the majority of cases are due to either negligence or wilful ignorance. But professional enablers are crucial to successful money laundering and therefore it is essential that the legal profession and its regulator disrupt and prevent such activity.

As such, the national risk assessment rated the legal sector as high risk of being used for money laundering, although low risk of being used for terrorist financing. In particular, the risk assessment identifies solicitors as being at a high risk of money laundering because of the range of high risk services they may offer.

481 Criminals may use a combination of legal services to add layers of complexity to a transaction. They may also use Chinese Walls (or information barriers) within a law firm, or several legal firms to separate instructions which, taken together, might raise suspicion. The National Risk Assessment also raised instances of lawyers falsely claiming legal professional privilege as posing a risk to the law enforcement response to preventing money laundering. The National Risk Assessment went on to say:

The government recognises that legal professional privilege is a vital part of the UK's legal system and that ensuring that it is applied correctly in all circumstances is important in mitigating money laundering risk

None of the risk factors below are reason alone for the legal sector to withdraw from operating in these ways or offering these services. We expect firms to be aware of the risk, manage it properly and keep themselves and the public safe. Done properly these are all services that help the legal market meet the legitimate needs of society. Firms that design and operate sound risk management systems have little to fear. The SRA will not tolerate firms that are cavalier about preventing money laundering, putting their practices and society at risk.

Risk factors

Risk is the likelihood of money laundering or terrorist financing taking place through your firm. Risk refers to the inherent level of risk before any mitigation – it does not refer to the residual risk that remains after you have put mitigation in place. Risk can exist in isolation, or through a combination of factors that increase or decrease the risk posed by the client or transaction. The different types of risk factors that we consider to be significant for firms we regulate are set out below.

Product and services risk

A large amount of solicitors' money laundering risk depends on the services, or combination of services they offer. The 2017 national risk assessment identifies the following as posing the highest risk of being used for money laundering:

- trust and company formation
- conveyancing
- client account services

Based on our supervisory work and analysis, we agree that these services pose the highest risk.

What	Why
conveyancing	Property is an attractive asset for criminals because of the large amounts of money that can be laundered through a single transaction, and the fact that property will tend to appreciate, or can be used to generate rental income. Approximately half of the suspicious activity reports (SARs) made by the legal sector relate to property transactions, indicating that this is a common way for criminals to seek to launder money.
client accounts	Solicitors are held in a position of trust, and their client account can be viewed as a way of making criminal funds appear to have a genuine source. Criminals target client accounts as a way of moving money from one individual to another through a legitimate third party under the guise of a legal transaction without attracting the attention of law enforcement agencies. You must never allow your client account to be used as a banking facility, or to pass funds through it without a legitimate underlying legal transaction. Firms should be aware of any attempt to pay funds into a client account without a genuine reason, or to get a refund of funds from a client account (particularly to a different account from which the original funds were paid). It is a good idea not to make the details of your client account visible (for example through including them in engagement letters) and to provide them only upon request once client due diligence has been completed.
creating or managing trusts and companies	Trusts or corporate structures which facilitate anonymity can help disguise the source or destination of money or assets. Law enforcement have flagged that many investigations of money laundering lead to opaque corporate structures, used to hide the beneficial owner of assets.

Client risk

Each client is different, and each will have their own particular risk-profile. There are a number of different factors that increase the risk of money laundering presented by clients. Warning signs include clients that appear to want anonymity, clients acting outside their usual pattern of transactions, clients whose identity is difficult to verify or who are evasive about providing ID documents. The risk posed by your client also extends to the risk posed the beneficial owner, if applicable.

What	Why
Politically exposed persons (PEPs)	The 2017 Money Laundering Regulations updated the definition on PEPs so that individuals from the UK are now included, whereas previously the definition was restricted to overseas individuals. Generally speaking, PEPs have access to public funds and the money laundering regulations require PEPs and their close families and associates to be identified and require extra checks to mitigate the risks of corruption. The money laundering regulations require firms to be able to identify PEPs and associates,

482	
What	Why
Customers from cash-intensive/risky sectors or businesses	The nature of the customer's business might increase risk if it is cash-intensive and therefore presents a greater risk of disguising illegal funds within legitimate payments. The customers' sector or area of work is also a significant risk factor, in particular if they are associated with those with a higher risk of corruption or being used for money laundering, for example those from the arms trade or casinos.
Clients seeking anonymity or who cannot prove their identity	Clients who are seeking anonymity on behalf of themselves, a third party or beneficial owner may be seeking to launder money. In some circumstances it might be natural that a client cannot produce identification documents, for example elderly people or illegal immigrants. Clients who are evasive about proving their identity or who produce non-standard documentation might be considered higher risk, if there is no good explanation for this.

Transaction risk

There are a number of factors that might make an individual transaction higher risk. Much of identifying risk is being alert for unusual activity or requests that don't make commercial sense. The use of cash, either as part of a transaction or for payment of fees is inherently higher risk, and it is a good idea to have a policy on what amount of cash you will accept, and in what circumstances.

What	Why
Size and value of the transaction	Money launderers incur a risk with each transaction, and so criminals may seek large or high value transactions to launder as much money as possible in one go. If there is no good explanation for an unusually large transaction, or a client is seeking to make a number of linked transactions this presents a higher risk.
Payment type	Cash and some electronic currencies can facilitate anonymity and enable money laundering. There may be legitimate reasons that a client wants to pay in cash, however this must be considered higher risk because it has not passed through the banking system and is often untraceable.
Transactions that don't fit with your firm or client's normal pattern	Firms will know what their specialisms are and what services they normally provide. In addition, initial client due diligence should include gathering some information on the expected ongoing client relationship. If a new or existing client is requesting transactions or services that you wouldn't normally expect your firm to offer, you might consider this suspicious if there is no obvious reason for the request. Similarly, if a client is requesting services which are not in line with your original customer due diligence or are out of their normal pattern of transactions, without a good reason, you should consider whether this constitutes suspicious behaviour. We would expect firms to have a reasonably good knowledge of the types of services clients will use and to be alert for requests that don't fit the normal pattern.
Transactions or products that facilitate anonymity	Accurate and up-to-date information on beneficial owners is a key factor in preventing financial crime and tracing criminals who try to hide their identity behind corporate structures. Increased transparency reduces the risk of money laundering. Firms should be alert to customers seeking products or transactions that would facilitate anonymity and allow beneficial owners to remain hidden without a reasonable explanation.
New products, delivery mechanisms or technologies	the changing nature of money laundering means that criminals are always seeking new ways to launder funds as old ways become too risky and loopholes are closed. Moving into a new business area or providing a new delivery channel for services means your firm may come across new or previously unidentified risks. In moving into a new area, you will not necessarily have a previous pattern of transactions with which to compare new behaviour that might be suspicious. Criminals might target firms moving into new areas, because of the perception that AML policies and procedures are new and untested. Criminals might seek to target loopholes in new technology before they are identified and closed.
Complex transactions	Criminals can use complexity as a way of obscuring the source of funds or their ownership. Firms should make sure that they fully understand the purpose and nature of a transaction they are being asked to undertake. You should make further enquiries or seek expertise if unsure. Simply proceeding with the transaction as asked without understanding the purpose and details increases the risk of money laundering.

Delivery channel risk

The way in which you deliver your services can increase or reduce risk to the firm. Transparency tends to reduce risk and complexity tends to increase it.

What	Why
Remote clients	Not meeting a client increases the risk of identity fraud and may help facilitate anonymity. Not meeting a client face-to-face may make sense in the context of the transaction, but clients who appear evasive about meeting in person might be cause for concern. The risk posed by remote clients can be somewhat mitigated by the use of safeguards such as electronic signatures.
Combining services	Some services might not be inherently high risk, but when combined with other services or transactions become risky. For example, there might be legitimate reasons for setting up a company, but if that company is used to purchase property and disguise its beneficial owner, this increases the risk of money laundering. Clients may take steps to hide the combination of services they are using, for example through enquiring about, and taking advantage of Chinese walls (or information barriers), through using separate firms, or through allowing a significant amount of time to pass between transactions so they appear unlinked.
Payments to or from third parties	Money launderers can seek to disguise the source of funds by having payments made by associates or third parties or have payments made to third parties. This is a way of disguising assets and you should make sure you always identify the source of funds and source of wealth. A payment to or from a third party is particularly suspicious if it is unexpected, or claimed that it was made in error with a request for the

483	What	money to be refunded. There may be some legitimate reasons for third party payments, for example parents gifting a house deposit to their child. You should ensure you do appropriate due diligence on the source of funds and wealth and the reason behind the payment before accepting funds.
	Why	

Geographical risk

When assessing geographical risk, you should consider the jurisdiction in which services will be delivered, the location of the client, and that of any beneficial owners as well as the source and destination of funds. In some jurisdictions the sources of money laundering are more common, for example the production of drugs, drugs trafficking, terrorism, corruption, people trafficking or illegal arms dealing. Countries with anti-money laundering and counter-terrorist financing regimes which are equivalent to the UK may be considered lower risk.

What	Why
Countries that do not have equivalent AML standards to the UK	The money laundering regulations require firms to put in place enhanced due diligence measures in dealing with countries that have not implemented FATF recommendations, identified by credible sources such as FATF, the International Monetary Fund or World Bank. The Financial Action Taskforce (FATF) maintains the list of high risk jurisdictions [http://www.fatf-gafi.org/countries/#high-risk].
Countries with significant levels of corruption	The money laundering regulations require firms to put in place enhanced due diligence measures in dealing with countries with significant levels of corruption or other criminal activity, such as terrorism. Transparency International also produces the annual corruption index [http://www.transparency.org/country].
Countries with organisations subject to sanctions	The money laundering regulations require firms to put in place enhanced due diligence measures in dealing with countries subject to sanctions, embargos or similar measures. In the UK, the Office of Financial Sanctions Implementation maintains a list of all those subject to financial sanctions [http://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases]. You can also subscribe to an email alerting you to any changes.

Next steps

The SRA will seek to keep this risk assessment up-to-date, taking into account new information from government, law enforcement and our regulatory regime. Firms should have regard to this risk assessment, and any updates, when creating and maintaining their own written risk assessment required in Regulation 18(1) of the money laundering regulations. The SRA may ask to see your firm's risk assessment as a part of routine monitoring visits, or in response to information received.

The SRA publishes more information on preventing money laundering and terrorist financing [[/home/hot-topics/anti-money-laundering/](#)].

Notes

1. National Crime Agency Money Laundering Page
2. National Risk Assessment of Money Laundering and Terrorist Financing 2017
[http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web]
3. The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
[<http://www.legislation.gov.uk/ukSI/2017/692/regulation/11/made>]
4. "independent legal professional" means a firm or sole practitioner who by way of business provides legal or notarial services to other persons, when participating in financial or real property transactions concerning
 - a. the buying and selling of real property or business entities;
 - b. the managing of client money, securities or other assets;
 - c. the opening or management of bank, savings or securities accounts;
 - d. the organisation of contributions necessary for the creation, operation or management of companies; or
 - e. the creation, operation or management of trusts, companies, foundations or similar structures, and, for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.
5. "trust or company service provider" means a firm or sole practitioner who by way of business provides any of the following services to other persons, when that firm or practitioner is providing such services
 - a. forming companies or other legal persons;

- b. acting, or arranging for another person to act
 - i. as a director or secretary of a company;
 - ii. as a partner of a partnership; or
 - iii. in a similar capacity in relation to other legal persons;
- c. providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or legal arrangement;
- d. acting, or arranging for another person to act, as
 - i. a trustee of an express trust or similar legal arrangement; or
 - ii. a nominee shareholder for a person other than a company whose securities are listed on a regulated market

Guidance

The Money Laundering, Terrorist Financing and Transfer of Funds

Updated 25 November 2019 (Date first published: 2 March 2018)

Status

This guidance is to help you understand your obligations and how to comply with them. We may have regard to it when exercising our regulatory functions.

Who is this guidance for?

This guidance is for firms and individuals we regulate that are subject to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) which came into force on 26 June 2017.

Purpose of this guidance

Paragraph 7.1 of the [Code of Conduct for Solicitors, RELs and RFLs](#), and paragraph 3.1 of the [Code of Conduct for Firms](#) require individuals and firms respectively to make sure they keep up to date with, and remain aware of, their responsibilities under any new legislation as and when it is introduced.

This guidance aims to update firms and individuals on the key changes to the MLRs that came into effect on 26 June 2017 and noting that further changes to the regulations are due to take effect in late 2019/early 2020.

Regulation 8 of the MLRs states that the regulations apply to certain categories of persons acting in the course of business carried on in the UK. The main categories likely to be relevant are:

- independent legal professionals participating in certain financial or real property transactions (regulation 12(1))
- trust or company service providers (regulation 12(2))
- auditors, insolvency practitioners, external accountants and tax advisers (regulation 11)
- estate agents (regulation 13)

The category that is most likely to be applicable is "independent legal professionals" as this is likely to include those firms offering conveyancing services or corporate finance work. Many firms may also be acting as a trust or company service provider, and some others may be acting as tax advisers, or estate agents.

General

We are responsible for the supervision of anti-money laundering (AML) and take our responsibilities very seriously. These responsibilities include gathering and holding data on the firms and legal practices we supervise; approving managers, officers and beneficial owners; and undertaking appropriate supervision and regulatory action. We liaise with the National Crime Agency (NCA), Her Majesty's Treasury (HMT), and Her Majesty's Revenue and Customs (HMRC) on a regular basis.

as well as ⁴⁸⁶other regulatory bodies.

You may need to make changes to your firm's or practice's procedures, systems and controls to comply with the requirements in the MLRs.

Key changes you need to be aware of

Risk assessments (Regulation 18)

You must identify and assess the risk of your firm or legal practice being used for money laundering and terrorist financing. You must maintain a written risk assessment, giving consideration to risk factors such as:

- the types of products or services (for example conveyancing services)
- client base
- geographical considerations (high-risk countries | see below)
- industry or business sector of the client
- delivery channel of services (face-to-face, virtual)

You will need to keep an updated written record of what you have done, and we may ask to see your risk assessment from time to time as part of our regulatory activities.

Policies, controls and procedures (Regulation 19)

Having completed a risk assessment (above), you must establish and maintain policies, controls and procedures to mitigate and manage the money laundering risks you have identified. These must be proportionate to the size and nature of your business and be approved by an officer or employee who has enough knowledge of the firm's ML/TF risk exposure and who is of sufficient authority. These policies, controls and procedures must include:

- risk-management practices
- internal controls
- customer due diligence (CDD)
- reliance and record keeping
- monitoring and management of compliance with, and internal communication of, the policies.

You will need to regularly review and update policies and keep a record of your policies, any changes made, and what steps have been taken to communicate those policies to staff.

Internal Controls (Regulation 21)

You should appoint a senior person to be responsible for your firm's compliance with the MLRs. This Money Laundering Compliance Officer (MLCO) should be a member of the board of directors (or your firm's equivalent).

You should also appoint a nominated officer, usually referred to as the Money Laundering Reporting Officer (MLRO), to receive internal reports of suspicious activity, and make Suspicious Activity Reports (SARs) to the National Crime Agency where necessary.

You must notify us of any changes to the identity of the MLCO and MLRO.

You will be required to carry out screening of all relevant staff members and agents, both before appointment and at regular times during it. Screening will need to cover any person whose work is relevant to compliance with MLR 2017, and any other applicable financial crime statutes, such as sanctions lists and the UK Bribery Act 2010.

⁴⁸⁷Enhanced Customer Due Diligence: politically-exposed persons (Regulation 35)

You must identify domestic, as well as foreign, politically-exposed persons (PEPs). Under previous regulations, the definition of PEPs was limited to foreign nationals, however you must now screen all PEPs against national or commercial databases. This requirement also extends to family members or known close associations of PEPs.

Other new requirements

Training (Regulation 24)

You must provide staff with appropriate training on money laundering and terrorist financing, and keep a record of the training staff have undertaken. This now includes an obligation to make staff aware of the law on data protection, insofar as it is relevant to the implementation of the regulations.

We have seen, in some firms and practices, that although training is taking place it is not specifically tailored to the needs of staff. As a result, it does not achieve its goal of helping to identify and prevent money laundering.

Approvals for beneficial owners, officers and managers (Regulation 26)

We must approve all beneficial owners, officers and managers of a firm. Acting as a beneficial owner, officer or manager of a firm without approval after 26 June 2018 is a criminal offence (unless you have applied for approval and it has yet to be determined).

Checks on corporate bodies (Regulation 43)

The new regulations are more prescriptive regarding CDD checks on corporate bodies. You are expected to know your clients, beneficial owners and ultimate beneficial ownership. Where the client is a corporate body, you must obtain and verify:

- its name
- its company number or other registration
- the address of its registered office and, if different, its principal place of business.

In addition, unless the corporate body is a company listed on a regulated market, you must take reasonable measures to determine and verify:

- the law to which it is subject, and its constitution or other governing documents, and
- the names of the board of directors or senior persons responsible for its operations

Timing of CDD (Regulation 30)

You must verify clients as soon as possible after your first contact with them and before establishing a business relationship. The MLRs state that you may undertake CDD while establishing the business relationship if there is a low risk of money laundering and it is necessary not to interrupt the normal conduct of business.

Enhanced due diligence (EDD) (Regulation 33)

Under the regulations, EDD measures must include, as a minimum, examining the background and purpose of the transaction and increasing the monitoring of the business relationship. Regulation 33(1) sets out a list of circumstances in which EDD measures must be applied, which includes:

- any transaction or business relationship involving a person established in a 'high risk third country'
- any transaction or business relationship involving a 'politically-exposed person' (PEP), or a family member or known

488
associate of a PEP

- any other situation that presents a higher risk of money laundering or terrorist financing.

Simplified due diligence (SDD) (Regulation 37)

Simplified due diligence is permitted where a firm determines, after individual risk assessment of the client, that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account their risk assessment. This is a change from the Money Laundering Regulations 2007, under which SDD could be more widely applied.

Reliance (Regulation 39)

Reliance is still possible under the MLR. You may rely on another person (another regulated individual) who is subject to the MLR or equivalent to carry out CDD, but you remain liable for any failings. To rely on a third party, you must enter into a written agreement with the third party under which they agree to provide copies of any identification and verification data on the customer or its beneficial owner within two working days, and to keep records in accordance with MLRs.

Further Guidance

Read out full guidance on the [2017 Money Laundering Regulations](#).

We also provide resources and information about [AML compliance](#)

[Case studies on money laundering](#).

[Warning notices on money laundering and terrorist financing](#).

Further help

If you require further assistance, please contact the [Professional Ethics helpline](#).

For law professionals

SRA Standards and Regulations

Guidance

Investigation and enforcement

Firm-based authorisation

Supervision

Resources

Qualified Lawyers Transfer

For the public

Solicitors Register

Choosing a solicitor

Instructing a solicitor

Problems and complaints

Scam alerts

Who we are

Students

[Academic stage](#)

[Legal Practice Course](#)

[Resources](#)

Trainees

[Period of recognised training](#)

[Professional Skills Course providers](#)

[Admission](#)

[Resources](#)

About us

[Equality and Diversity](#)

[How we work](#)

[Decision making](#)

[Consultation and discussion](#)

[Research and reports](#)

[Complaints about our service](#)

[News and events](#)

[Strategy](#)

[Policy](#)

[Jobs](#)

Legal Sector Affinity Group

Anti-Money Laundering

Guidance for the Legal Sector

March 2018

Contents

Glossary	5
Chapter 1 – Introduction	11
1.1 Who should read this guidance?.....	11
1.2 What is the issue?	12
1.3 Definition of money laundering	12
1.4 Legal framework and other requirements.....	13
1.5 Status of this guidance	18
1.6 Terminology in this guidance	19
Chapter 2 - Risk-based approach	20
2.1 General comments	20
2.2 Requirement to undertake and maintain a practice-wide risk assessment	20
2.3 Assessing your practice's risk profile	21
2.4 Mitigating factors	26
2.5 Assessing individual client and retainer risk.....	28
Chapter 3 – Systems, policies, procedures and controls	30
3.1 General comments	30
3.2 Application and requirements	30
3.3 Group-wide application	31
3.4 Areas to cover	31
3.5 Disclosures.....	37
3.6 Record keeping	37
3.7 Communication and training	40
Chapter 4 – Customer due diligence	42
4.1 General comments	42
4.2 Application.....	42
4.3 CDD in general	42
4.4 Reliance and outsourcing	45
4.5 Timing	48
4.6 Ongoing monitoring.....	50
4.7 New instructions from an existing client	51
4.8 Records.....	51
4.9 CDD on clients.....	52
4.10 CDD on a beneficial owner	68
4.11 Simplified due diligence	73
4.12 Enhanced due diligence	74
4.13 Sanctions and other restrictions.....	79

Chapter 5 – Beneficial ownership information	81
5.1 Overview	81
5.2 Obligations on UK body corporates	81
5.3 Obligations of trustees	82
Chapter 6 – Money laundering offences	87
6.1 General comments	87
6.2 Application.....	87
6.3 Mental elements	87
6.4 Principal money laundering offences	88
6.5 Defences to principal money laundering offences.....	91
6.6 Failure to disclose offences – money laundering	93
6.7 Exceptions to failure to disclose offences	94
6.8 Tipping off.....	96
Chapter 7 – Legal professional privilege	100
7.1 General comments	100
7.2 Application.....	100
7.3 Duty of confidentiality.....	100
7.4 Legal professional privilege	100
7.5 Privileged circumstances	104
7.6 Differences between privileged circumstances and LPP	105
7.7 When do I disclose?	106
Chapter 8 – Terrorist property offences	107
8.1 General comments	107
8.2 Application.....	107
8.3 Principal terrorist property offences	107
8.5 Failure to disclose offences	109
8.6 Defences to failure to disclose	109
8.7 Section 21D tipping off offences: regulated sector	109
8.8 Defences to tipping off.....	110
8.9 Making enquiries of a client	111
8.10 Other terrorist property offences in statutory instruments.....	111
Chapter 9 – Making a disclosure	113
9.1 General comments	113
9.2 Application.....	113
9.3 Suspicious activity reports	113
9.4 Sharing of information within the regulated sector and joint disclosure reports	118
9.5 Feedback on SARs.....	119
Chapter 10 – Enforcement	120
10.1 General comments	120

10.2 Supervision under the Regulations	120
10.3 Disciplinary action against legal professionals	122
10.4 Offences and penalties	122
10.5 Joint liability	127
10.5 Prosecution authorities	127
Chapter 11 – Civil liability	128
11.1 General comments	128
11.2 Constructive trusteeship	128
11.3 Knowing receipt	128
11.4 Knowing assistance	129
11.5 Making a disclosure to the NCA.....	130
11.6 Civil liability in relation to SARs.....	131
Chapter 12 – Money laundering warning signs	132
12.1 General comments	132
12.2 General warning signs during a retainer	132
12.3 Private client work	135
12.4 Property work	137
12.5 Company and commercial work.....	141
Chapter 13 – offences and reporting practical examples	145
13.1 General comments	145
13.2 Principal offences	145
13.3 Should I make a disclosure?	147

Glossary

AIM	Alternative Investment Market
AML / CTF	Anti-money laundering / counter-terrorist
BSB	Bar Standards Board
CDD	Customer due diligence
COLP	Compliance Officer for Legal Practice
DAML	Defence Against Money Laundering
EEA	European Economic Area
FATF	Financial Action Task-force
FCA	Financial Conduct Authority
GRO	General Register Office
HMRC	Her Majesty's Revenue and Customs
IBA	International Bar Association
JMLSG	Joint Money Laundering Steering Group
LLP's	Limited Liability Partnerships
LPP	Legal professional privilege
MLRO	Money Laundering Reporting Officer
PEPs	Politically exposed persons
POCA	Proceeds of Crime Act 2002
Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
SOCPA	Serious Organised Crime and Police Act 2005
SARs	Suspicious activity reports

SRA	Solicitors Regulation Authority
NCA	National Crime Agency
Terrorism Act	Terrorism Act 2000
Third directive	Third European Money Laundering Directive
4th Directive	Fourth European Money Laundering Directive

Definitions

Beneficial owners	See chapter 4 and 5
Business relationship	<p>A business, professional or commercial relationship between a relevant person and a customer, which is:</p> <ul style="list-style-type: none"> • connected to the business of the relevant person and • expected by the relevant person at the time when contact is established to have an element of duration. <p>However, if the relevant person is asked to form a company for its customer, the relationship is a business relationship regardless of whether or not the formation of the company is the only transaction carried out for the customer.</p>
Customer due diligence	See chapter 4.
Criminal conduct	Conduct which constitutes an offence in any part of the UK or would constitute an offence in any part of the UK if it occurred there – see s340(2) of POCA.
Criminal property	Property which is, or represents, a person's benefit from criminal conduct, where the alleged offender knows or suspects that it is such – see also the definition of property.
Disclosure	A report made to the NCA under the POCA – also referred to as a suspicious activity report (SAR).

DAML	DAML stands for Defence Against Money Laundering and is a term used by the NCA to refer to 'appropriate consent' to carrying out an activity that may result in a person committing a principal money laundering or terrorist financing offence as contained in Part 7 of POCA and Part 3 of the Terrorism Act.
Independent legal professional	See chapter 1.4.5.
Insolvency practitioner	Any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986 (as amended) or article 3 of the Insolvency (Northern Ireland) Order 1989 (as amended).
Inter vivos trust	A trust which takes effect while a person is alive.
Legal professional privilege	See chapter 7.4.
Nominated officer	A person nominated within the practice to make disclosures to the NCA under POCA – also referred to as a Money Laundering Reporting Officer (MLRO).
Occasional transaction	A transaction (carried out other than as part of a business relationship) amounting to 15,000 euros or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.
Ongoing monitoring	See chapter 4.6.

Overseas criminal conduct	Conduct which occurs overseas that would be a criminal offence if it occurred in the UK. The definition does not include conduct which occurred overseas where it is known or believed on reasonable grounds that the relevant conduct occurred in a particular country or territory outside the UK, and such conduct was in fact not unlawful under the criminal law then applying in that country or territory. The exemption will not apply to overseas criminal conduct if it would attract a maximum sentence in excess of 12 months' imprisonment were the conduct to have occurred in the UK. Conduct will always be exempt if the overseas conduct is such that it would constitute an offence under the Gaming Act 1968, the Lotteries & Amusements Act 1976 or s23 or s35 of the Financial Services and Markets Act 2000. See s102 of SOCPA.
Politically exposed persons	See chapter 4.12.2.
Practice	An independent legal practitioner's business, whether that business is a law firm or conducted as a sole practitioner. For a barrister the term 'practice' refers to a self-employed professional.
Privileged circumstances	See chapter 6.7.2.
Property	All property whether situated in the UK or abroad, including money, real and personal property, things in action, intangible property and an interest in land or a right in relation to any other property.
Regulated sector	Activities, professions and entities regulated for the purposes of AML/CTF obligations - see chapter 1.

Tax adviser	A practice or sole practitioner who, by way of business, provides advice about the tax affairs of another person, when providing such services.
Terrorist property	Money or other property which is likely to be used for the purposes of terrorism, the proceeds of the commission of acts of terrorism and the proceeds of acts carried out for the purposes of terrorism.
Trust or company service provider	<p>A practice or sole practitioner who by way of business provides any of the following services to other persons -</p> <ul style="list-style-type: none"> • forming companies or other legal persons • acting or arranging for another person to act <ul style="list-style-type: none"> ○ as a director or secretary of a company; ○ as a partner of a partnership; or ○ in a similar position in relation to other legal persons; • providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement; • acting, or arranging for another person to act, as - <ul style="list-style-type: none"> ○ a trustee of an express trust or similar legal arrangement; or ○ a nominee shareholder for another person other than a company listed on a regulated market when providing such services

Chapter 1 – Introduction

1.1 Who should read this guidance?

All independent legal professionals and other staff in a law practice who are involved in anti-money laundering compliance.

As this guidance applies across the entire legal sector the term 'practice' has been used to refer to an independent legal professional's business, whether that business is a law firm or other authorised entity, or is conducted as a sole practitioner, or in a self-employed capacity or operates under another structure. For solicitors, the term 'practice' refers to their firm as a whole and not a practice group within a firm.

1.1.1 Application to barristers and advocates

Barristers and advocates should note that there are areas of this Guidance that will not have application to them, for example where the Guidance refers to undertaking the management of a client's affairs or the handling of client money.

Other sections will apply to some barristers and advocates, but not others. For example, references to the MLRO role and organisational arrangements will not apply to advocates or self-employed barristers who are practising from chambers or as sole practitioners, but will apply to barristers working in private practice in entities, where the MLRO role and the organisational arrangements may be comparable to solicitors' firms.

Where a chapter of the Guidance has only limited or no application to barristers or advocates this is noted at the outset of the relevant chapter.

Barristers in England and Wales should note that BSB Handbook restrictions apply to both barristers and BSB entities; neither are permitted to:

- undertake the management, administration or general conduct of a client's affairs (rS25 for self-employed barristers, rS29 for BSB entities and rS33 for managers and employed barristers of BSB entities);
- receive, control or handle client money apart from that paid by the client to a barrister for their services, save where they are acting as a manager of a body authorised by another approved regulator to undertake reserved legal activities, such as the SRA (rC73 and rS83.5 for BSB entities).

Advocates should note that they are not permitted to receive, control or handle client money when either acting on the instructions of a solicitor or in terms of the Faculty of Advocates' Direct Access Rules.

Barristers in Northern Ireland should note the requirements of their own Code of Conduct including the obligation to remain independent of all intrinsic pressures and personal interests and should note that they; are not permitted to accept a fee directly from a lay client, are not permitted to receive or handle lay clients' money and must not enter into any form of fee sharing arrangement or partnership.

1.2 What is the issue?

Independent legal professionals are key actors in the business and financial world, facilitating vital transactions that underpin the UK economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. Independent legal professionals must act with integrity and uphold the law, and they must not engage in criminal activity.

Money laundering and terrorist financing are serious threats to society, causing a loss of revenue and endangering life, and fueling other criminal activity.

This guidance aims to assist independent legal professionals to meet their obligations under the UK anti-money laundering and counter-terrorist financing (AML/CTF) regime.

1.3 Definition of money laundering

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Under POCA, the definition is broader and more subtle. Money laundering can arise from small profits and savings from relatively minor crimes, such as regulatory breaches, minor tax evasion or benefit fraud. A deliberate attempt to obscure the ownership of illegitimate funds is not necessary.

There are three acknowledged phases to money laundering: placement, layering and integration. However, the broader definition of money laundering offences in POCA includes even passive possession of criminal property as money laundering.

1.3.1 Placement

Cash generated from crime is placed in the financial system. This is the point when proceeds of crime are most apparent and at risk of detection. Because banks and financial institutions have developed AML procedures, criminals look for other ways of placing cash within the financial system. Independent legal professionals can be targeted because they and their practices commonly deal with client money.

1.3.2 Layering

Once the proceeds of crime are in the financial system, layering involves obscuring the origins of the proceeds by passing them through complex transactions. These often involve different entities, for example, companies and trusts and can take place in multiple jurisdictions. An independent legal professional may be targeted at this stage and detection can be difficult.

1.3.3 Integration

Once the origin of the funds has been obscured, the criminal is able to make the funds appear to be legitimate funds or assets. They will invest funds in legitimate businesses or other forms of investment, often, for example, using an independent legal professional to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities. This is the most difficult stage at which to detect money laundering.

1.4 Legal framework and other requirements

1.4.1 Financial Action Task Force (FATF)

This was created in 1989 by the G7 Paris summit, building on UN treaties on trafficking of illicit substances in 1988 and on confiscating the proceeds of crime in 1990. In 1990, FATF released their 40 recommendations for fighting money laundering. Between October 2001 and October 2004 it released nine further special recommendations to prevent terrorist funding. The recommendations were again revised in February 2012. The revised recommendations now fully integrate counter-terrorist financing measures with anti-money laundering controls and, among other things, seek to better address new and emerging threats and clarify and strengthen many of the existing obligations, including the laundering of the proceeds of corruption and tax crimes.

1.4.2 European Union directives

1991 – first money laundering directive

The European Commission issued this directive to comply with the FATF recommendations. It applied to financial institutions, and required member states to make money laundering a criminal offence. It was incorporated into UK law via the Criminal Justice Act 1991, the Drug Trafficking Act 1994 and the Money Laundering Regulations 1993.

2001 – second money laundering directive

This directive incorporated the amendments to the FATF recommendations. It extended anti-money laundering obligations to a defined set of activities provided by a number of service professionals, including independent legal professionals, accountants, auditors, tax advisers and real estate agents. It was incorporated into UK law via POCA and the Money Laundering Regulations 2003.

2005 – third money laundering directive

This directive extended due diligence measures to beneficial owners, recognised that such measures can be applied on a risk-based approach, and required enhanced due diligence to be undertaken in certain circumstances. It was incorporated into UK law by the Money Laundering Regulations 2007, the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (the TACT and POCA Regulations 2007).

2015 - fourth money laundering directive

This directive responded to changes made to the requirements issued by FATF in February 2012 and to a review conducted by the European Commission on the implementation of the third money laundering directive.

There were a number of new developments contained in the 4th Directive. The key ones include the following:

- requirements on regulated entities to have a written risk assessment

- amendments to the way in which simplified due diligence may be applied
- changes to the beneficial ownership provisions
- extension of enhanced due diligence to domestic PEPs
- additional provisions in the legislation focusing on other matters, including changes to the offences that are included for reporting purposes (for example, tax evasion is now included, although many jurisdictions had already incorporated the reporting of tax crimes in their domestic legislation)
- requirements for Member States to maintain registers recording the beneficial owners of companies and trusts which generate tax consequences
- requirements for Member States to take necessary measures to prevent criminals with relevant convictions from holding a management function in, or being the beneficial owner of, an obliged entity

1.4.3 Proceeds of Crime Act 2002 (POCA) Scope

POCA, as amended, establishes a number of money laundering offences including:

- the principal money laundering offences
- the offences of failing to report suspected money laundering
- the offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing a money laundering investigation

The TACT and POCA Regulations 2007 repealed the section 333 POCA tipping off offence. It has been replaced by section 333A which creates two new offences. Section 342(1) has also been amended to reflect these new offences.

See Chapter 6 for further discussion of the principal money laundering offences.

Application

POCA applies to all persons, although certain offences regarding failure to report and tipping off only apply to persons who are engaged in activities in the regulated sector.

The Proceeds of Crime Act 2002 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 amended the POCA, changing the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007. These regulations were in turn replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 on 26 June 2017.

Under Schedule 9 of POCA, key activities which may be relevant to independent legal professionals are the provision of the following services by way of business:

- advice about the tax affairs of another person by a practice or sole practitioner
- legal or notarial services involving the participation in financial or real property transactions concerning the buying and selling of real property or business entities

- the managing of client money, securities or other assets
- the opening or management of bank, savings or securities accounts
- the organisation of contributions necessary for the creation, operation or management of companies
- the creation, operation or management of trusts, companies or similar structures.

Chapters 6, 7 and 9 of this guidance provide more details on the obligations of independent legal professionals under POCA.

1.4.4 Terrorism Act 2000

Scope

The Terrorism Act 2000, as amended, established several offences about engaging in or facilitating terrorism and raising or possessing funds for terrorist purposes. It established a list of proscribed organisations that the Secretary of State believes to be involved in terrorism. The TACT and POCA Regulations 2007 entered into force on 26 December 2007 and introduced tipping off offences and defences to the principal terrorist property offences into the Terrorism Act 2000.

Read about these provisions in Chapter 8.

Application

The provisions of the Terrorism Act generally apply to all persons. There is in addition a failure to disclose offence and tipping off offences for those operating within the regulated sector.

The Terrorism Act 2000 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 amended the Terrorism Act to change the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007. These regulations have since been replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

Chapters 8 and 9 provide more detail on the obligations of independent legal professionals under the Terrorism Act.

1.4.5 The Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)

Scope

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 repeal and replace the Money Laundering Regulations 2007 and implement the 4th Directive. They set out administrative requirements for the anti-money laundering regime within the regulated sector and outline the scope of CDD.

The Regulations aim to limit the use of professional services for money laundering by requiring professionals to know their clients and to monitor the use of their services by clients.

Application

Regulation 8 states that the Regulations apply to persons acting in the course of businesses carried on in the UK in the following areas:

- credit institutions
- financial institutions
- auditors, insolvency practitioners, external accountants and tax advisers
- independent legal professionals
- trust or company service providers
- estate agents
- high value dealers
- casinos

Independent legal professional

An independent legal professional means a firm or a sole practitioner who by way of business provides legal or notarial services to other persons. It does not include legal professionals employed by a public authority or working in-house.

The Regulations only apply to a legal professional's activities where there is a risk of money laundering occurring. As such, they apply when a legal professional participates in financial or real property transactions concerning:

- buying and selling of real property or business entities
- managing of client money, securities or other assets
- opening or management of bank, savings or securities accounts
- organisation of contributions necessary for the creation, operation or management of companies
- creation, operation or management of trusts, companies, foundations or similar structures

A legal professional is considered to be participating in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

The Regulations do not apply to work undertaken by a notary as a public certifying officer where he or she has no substantive role in the underlying transaction. As such, the Regulations do not apply to many aspects of a notary's practice including, for example, the taking of affidavits and declarations, protests, translating, certifying the execution of documents and authentication work in general. Although the Regulations will not apply to work of this nature, notaries are still subject to obligations under the

Notaries Practice Rules 2014 and Code of Practice positively to identify appearing parties and keep records of the means of identification employed.

Activities covered by the Regulations

In terms of the activities covered, you should note that:

- managing client money is more narrowly defined than handling it
- opening or managing a bank account is defined more widely than simply opening a client account. It is likely to cover a legal professional acting as a trustee, attorney or a receiver.

Activities not covered by the Regulations

HM Treasury has confirmed that the following would not generally be viewed as participation in a financial transaction:

- payment on account of costs to a legal professional or payment of a legal professional's bill
- provision of legal advice
- participation in litigation or a form of alternative dispute resolution
- will-writing, although you should consider whether any accompanying taxation advice is covered
- work funded by the Legal Services Commission

If you are uncertain whether the Regulations apply to your work, you should seek legal advice on the individual circumstances of your practice or simply take the broadest possible approach to compliance with the Regulations.

Working elsewhere in the Regulated sector

When deciding whether you are within the regulated sector for the purpose of the Regulations, you also need to consider whether you offer services bringing you within the definitions of a tax adviser, insolvency practitioner, or trust or company service provider.

Under Regulation 11(d) a tax adviser is a firm or sole practitioner who provides advice about tax affairs of other persons, when providing such services.

A trust or company service provider is defined in Regulation 12(2) as firm or sole practitioner who, by way of business provides any of the following services, when providing those services:

- forming companies or other legal persons
- acting, or arranging for another person to act:
 - as a director or secretary of a company;
 - as a partner of a partnership; or
 - in a similar capacity in relation to other legal persons

- providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or legal arrangement
- acting, or arranging for another person to act, as:
 - a trustee of an express trust or similar legal arrangement
 - a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

You must consider the full range of related services, such as tax planning and tax compliance work.

You will also need to consider whether your practice undertakes activities falling within the definition of financial institution, particularly with respect to the list of operations covered by the capital markets directive, as contained in schedule 2 of the Regulations. When considering those operations, you should note that a will is not a designated investment, so storing it is not a safe custody service, and is not covered by the Regulations.

Simply being nominated as a trustee under a will does not amount to being a trust and company service provider, because the trust is not formed until the testator's death.

If you are an independent legal professional within the regulated sector and you also fall within another category, such as work regulated by the Financial Conduct Authority (FCA), this may affect your supervision under these Regulations. You should contact your supervisory authority for advice on any supervisory arrangements that they may have in place with other supervisory authorities.

1.5 Status of this guidance

This draft guidance replaces previous guidance and good practice information on complying with AML/CTF obligations.

Guidance is issued by the Legal Sector Affinity Group, which comprises the AML Supervisors for the legal sector. You are not required to follow this guidance, but doing so will make it easier to account to oversight bodies for your actions.

This guidance is not legal advice, and does not necessarily provide a defence to complaints of misconduct or inadequate professional service.

However, legal sector regulators will take into account whether a legal professional has complied with this guidance when undertaking its role as regulator of professional conduct, and as a supervisory authority for the purposes of the Regulations. You may be asked by your regulatory body to justify a decision to deviate from this guidance.

Some independent legal professionals are authorised and regulated by the FCA because they are involved in mainstream regulated activities, e.g. advising clients directly on investments such as stocks and shares. Those professionals should also consider the Joint Money Laundering Steering Group's guidance.

This guidance has been approved by HM Treasury. In accordance with sections 330(8) and 331(7) of the Proceeds of Crime Act 2002, section 21A(6) of the Terrorism Act 2000, and Regulation 86(2)(b) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, the court is required to consider compliance with this guidance in assessing whether a person committed

an offence or took all reasonable steps and exercised all due diligence to avoid committing the offence.

While care has been taken to ensure that this guidance is accurate, up to date and useful, members of the Legal Sector Affinity Group will not accept any legal liability in relation this guidance.

1.6 Terminology in this guidance

Must

A specific requirement in legislation. You must comply, unless there are specific exemptions or defences provided for in relevant legislation.

Should

Outside of a regulatory context, good practice for most situations in the Legal Sector Affinity Group's view.

These may not be the only means of complying with legislative or regulatory requirements and there may be situations where the suggested route is not the best possible route to meet the needs of your client. However, if you do not follow the suggested route, you should be able to justify to oversight bodies why the alternative approach you have taken is appropriate, either for your practice, or in the particular retainer.

May

A non-exhaustive list of options for meeting your obligations or running your practice. Which option you choose is determined by the profile of the individual practice, client or retainer. You may be required to justify why this was an appropriate option to oversight bodies.

Chapter 2 - Risk-based approach

Note: References to client accounts and management of trusts, companies and charities in sections 2.3.2.2, 2.4.2 and 2.4.5 do not apply to barristers or advocates for the reasons set out in section 1.1.1.

2.1 General comments

The possibility of being used to assist with money laundering and terrorist financing poses many risks for the practice of an independent legal professional, including:

- criminal and disciplinary sanctions for the practice and individuals in the practice
- civil action against the practice as a whole, as well as certain individuals
- damage to reputation leading to a loss of business.

These risks must be appropriately identified, assessed and mitigated, just as you do for all business risks facing your practice. If you know the risks that you face generally and know your client well and understand your instructions thoroughly, you will be better placed to assess risks and spot suspicious activities.

Adopting a risk-based approach to preventing money laundering means that you focus your resources on the areas of greatest risk. The resulting benefits of this approach include:

- more efficient and effective use of resources proportionate to the risks faced,
- minimising compliance costs and burdens on clients. and
- greater flexibility to respond to emerging risks as laundering and terrorist financing methods change.

The risk-based approach does not apply to reporting suspicious activity, because POCA and the Terrorism Act lay down specific legal requirements not to engage in certain activities and to make reports of suspicious activities once a suspicion is held. However, the risk-based approach still applies to ongoing monitoring of clients and retainers and this will enable you to identify suspicions.

Money laundering and terrorist financing risks vary across the legal sector and your practice's particular risk-based processes should be led by an assessment of:

- the activities you undertake,
- the existing professional and ethical rules and regulations to which you are subject, and
- the susceptibility of the activities of your practice to money laundering and terrorist financing in the particular countries in which your practice operates.

2.2 Requirement to undertake and maintain a practice-wide risk assessment

Under Regulation 18(1) an independent legal professional's practice is required to carry out and maintain a documented practice-wide risk assessment to identify and

assess the risk of money laundering and terrorist financing to which the business is subject.

You must:

- take appropriate steps to identify, assess and understand the money laundering and terrorist financing risks your business faces;
- (subject to any specific provisions in the Regulations) apply a risk-based approach to compliance with CDD obligations; and
- have documented policies, controls and procedures that enable your business to manage, monitor and mitigate effectively the different risks that have been identified.

No matter how thorough your risk assessment or how appropriate your controls, some criminals may still succeed in exploiting your practice for criminal purposes. Nevertheless, a comprehensive practice-wide risk assessment combined with appropriate risk-based judgments on individual clients and retainers will enable you to justify your decisions and actions to law enforcement agencies, the courts and your supervisory authority.

2.3 Assessing your practice's risk profile

In carrying out your practice-wide risk assessment you must take into account:

- information on money laundering and terrorist financing risks made available to you by your supervisory authority following their own risk assessment, and
- risk factors relating to:
 - your customers
 - the countries or geographic areas in which your business operates
 - your products or services
 - your transactions, and
 - your delivery channels.

In addition, you should consider the nature of any issues raised in SARs made by your MLRO and consult the key contact in your organisation to understand any risks they may have identified.

Your risk assessment may also include consideration of:

- the UK's National Risk Assessment,
- the EU's Supra-National Risk Assessment,
- the FATF Risk-based Approach Guidance for Legal Professionals ,
- if you provide services in any other jurisdictions, any relevant FATF mutual evaluations, national risk assessments, or publicly available materials in respect of the risks in those jurisdictions; and

- any other material which may be relevant to assess the risk level particular to your practice, for example, press articles highlighting issues that may have arisen in particular jurisdictions.

Having assessed the money laundering and terrorist financing risks your practice faces you should then consider any mitigating factors or reasonable controls that you can implement to manage these risks and reduce their significance to a proportionate and acceptable level.

2.3.1 Customer risk factors

When assessing risk factors relating to your customers you should consider the demographic of your client base. Factors which may affect the level of risk associated with your client base are set out below.

2.3.1.1 High client turnover v stable client base

Although not determinative, you should take into account the length and strength of your typical client relationships.

If you have long-term and strong relationships with your clients you will be in a better position to identify any potential money laundering issues, which may mean your practice is at a lower risk of being subject to money laundering or terrorist financing (although you should always be mindful of clients that put pressure on you citing their long-standing relationship). Conversely, if you tend to have shorter relationships and a higher client turnover, you may conclude that the lack of a long and strong client relationship means your practice faces greater risk.

2.3.1.2 Clients based in high-risk jurisdictions

Country risk factors should feature prominently in your assessment of the money laundering and terrorist financing risks your practice faces. Key issues to consider are whether the jurisdictions in which your clients, or the beneficial owners of your clients, are based or operate their businesses:

- have deficient anti-money laundering legislation, systems and practice
- have high levels of acquisitive crime or higher levels of corruption
- are considered to be 'offshore financial centres' or tax havens
- permit nominee shareholders to appear on the share certificate or register of owners.

Conversely, where your clients or the beneficial owners of your clients are based or operate their business in low risk jurisdictions this should be reflected in your risk assessment.

The European Commission has been empowered under the 4th Directive to publish a list of 'high risk third countries', contained in [Commission Delegated Regulation \(EU\) 2016/1675](#). However, you should note that there may be other jurisdictions that present a high risk of money laundering that are not on the European Commission list of 'high risk third countries'.

FATF provides a source of valuable information on the relative risks associated with particular jurisdictions in its system of mutual evaluations, which provide an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system. It also produces a list of jurisdictions with 'strategic deficiencies' in their money laundering initiatives and a list of jurisdictions with 'low capacity', the latter being characterised as countries which have economic or sociological constraints preventing them from implementing AML/CTF measures effectively.

In addition, information is publicly available on bribery and corruption risks and about countries regarded as secrecy jurisdictions (or jurisdictions that permit the use of nominee shareholders).

Online resources you may consult include:

- FATF and HM Treasury statements on unsatisfactory money laundering controls in overseas jurisdictions.
- [The International Bar Association's summary of money laundering legislation around the world.](#)
- [Transparency International's corruption perception index.](#)

2.3.1.3 Clients in higher risk sectors

Given the wider international focus and extra territorial issues surrounding anti-bribery and corruption laws in some jurisdictions, you should take into consideration the elevated risks attached to certain sectors when carrying out your practice-wide risk assessment.

Certain sectors have been identified by credible sources as giving rise to an increased risk of corruption and, in some countries, are subject to international or UK, UN or EU sanctions.

Sectors that may be higher risk, particularly when coupled with a high-risk jurisdiction include (but are not limited to):

- public work contracts and construction, including post-conflict reconstruction
- real estate and property development
- the oil and gas industry
- the nuclear industry
- mining (including diamond mining and trading)
- arms manufacturing/supply and the defence industry

Clearly not all work in these sectors will be higher risk but it is essential to be aware of the potential for risk so that you can implement proportionate procedures for closer scrutiny on client and matter acceptance.

2.3.1.4 Acting for politically exposed persons (PEPs)

An independent legal professional's exposure to PEPs is also a major consideration in carrying out your practice-wide risk assessment. A PEP may be a client or a beneficial

owner of a client but it is important to consider the type of PEPs that you act for and whether the work to be undertaken will affect your overall risk profile.

PEPs are considered in section 4.12.2.

2.3.1.5 Acting for clients without meeting them

In an increasingly global and technologically advanced environment, it is commonly the case that you will act for clients without meeting them. You should include this as a factor when you carry out your practice-wide risk assessment. In addition, you should consider the systems and procedures that you have implemented to mitigate the risks associated with acting for clients you do not meet.

When you act for clients without meeting them you must be satisfied that it makes sense in all the circumstances that you have not met the client and you must be comfortable that you can mitigate the risks of identity fraud.

2.3.1.6 Clients with high cash turnover businesses

You should consider whether your practice frequently acts for clients who operate or benefit from high cash turnover businesses as these businesses may be appealing to criminals seeking to launder money.

2.3.2 Services and areas of law and geographical location of services provided

In carrying out your practice-wide risk assessment you must consider risks associated with the services you provide, the transactions you participate in and the countries or geographic areas in which you operate.

2.3.2.1 Services and areas of law

Many studies have highlighted that independent legal professionals face the greatest potential risks in the following areas:

- misuse/abuse of client accounts
- sale/purchase of real property
- creation of trusts, companies and charities
- management of trusts and companies
- sham litigation

The involvement of your practice in the sale/purchase of real property, creation of trusts, companies and charities, and management of trusts and companies does not automatically lead to the conclusion that your business is high risk. However, you should consider these areas and consider other risk factors, such as jurisdictional or sector risk, in the context of your business so that you can put in place additional controls where necessary to minimise the risk of money laundering.

Other areas of risk focus more closely on factors which may be more prevalent when considering a particular client or mandate, including unusually complicated transactions. You should consider how you might ensure that your staff can identify the warning signs as part of your risk assessment.

Criminals are constantly developing new techniques, so no list of examples can ever be exhaustive. This section does, however, provide some further guidance on areas of money laundering risk.

2.3.2.2 Client accounts and payments

In carrying out your practice-wide risk assessment you should take into account the risk that criminals may attempt to misuse/abuse your client account. You must ensure that you only use client accounts to hold client money for legitimate transactions where this is incidental to the legal services you supply. Putting the proceeds of crime through your client account can give them the appearance of legitimacy, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into the banking system can be part of the placement stage of money laundering. Therefore, the use of cash may be a warning sign.

Legal professionals should not provide a banking service for their clients.

2.3.2.3 Sale/purchase of real property

Law enforcement authorities believe that the purchase of real estate is a common method for disposing of or converting criminal proceeds.

Real estate is generally an appreciating asset and the subsequent sale of the asset can provide an apparently legitimate reason for the existence of the funds.

2.3.2.4 Creation and management of trusts, companies and charities

Company and trust structures may be exploited by criminals who wish to retain control over criminally derived assets while creating impediments to law enforcement agencies in tracing the origin and ownership of assets. Criminals may ask legal professionals to create companies and trusts and/or to manage companies and trusts, to provide greater respectability and legitimacy to the entities and their activities.

Shell companies are corporate entities that do not have any business activities or recognisable assets. They may be used for legitimate purposes such as serving as transaction vehicles. However, they can also be an easy and inexpensive way to disguise beneficial ownership and the flow of illegitimate funds and so are attractive to criminals engaged in money laundering. You should be suspicious if a client engages your services only in connection with the routine aspects of forming an entity, without seeking legal advice on the appropriateness of the corporate structure and related matters. In jurisdictions where members of the public may register companies themselves with the company register the engagement of a legal professional to register the company may indicate that the client is seeking to add legitimacy to a shell company.

2.3.2.5 Sham litigation

Litigation may constitute sham litigation if the subject of the dispute is fabricated (there is no actual claim and the litigation is a merely a pretext for transferring the proceeds of crime from one entity to another, possibly through a client account) or if the subject of the litigation is a contract relating to criminal activity that a court would not enforce.

2.3.2.6 Geographical location of services

You should carefully consider the jurisdictions in which you are offering your services and whether there are any particular local issues of which you ought to be aware which may impact on your risk assessment. Information on jurisdictional issues is set out above in section 2.3.1.2.

2.4 Mitigating factors

This section sets out mitigating factors that you may wish to incorporate into your policies and procedures in order to address the potential threats/areas of risk identified above.

2.4.1 Client demographic risks

- Conduct thorough due diligence taking a risk-based approach and avoiding tick box processes.
- Understand the risks in the jurisdictions in which your clients are based or have their operations and the sectors in which they operate.
- Introduce a means of identifying potentially higher risk issues and do internet-based research on higher risk clients or beneficial owners.
- Probe source of funds in higher risk cases, including where shareholders have no apparent online presence but the transaction value is substantial.

2.4.2 Client accounts/payments

- Ensure that you comply with the client account rules of your regulator.
- Prohibit the use of your client account without the accompanying legal services and include a process to ensure that information about all payments is cross-checked.
- Conduct thorough CDD before taking money on account, including understanding the transaction.
- Avoid disclosing your client account details as far as possible, discourage clients from passing the details on to third parties, ask them to use the account details only for previously agreed purposes and make it clear that electronic transfer of funds is expected. If you need to provide your account details, ask the client where the funds will be coming from. Will it be an account in their name, from the UK or abroad? Consider whether you are prepared to accept funds from any source that you are concerned about.
- Restrict cash payments. Large payments made in actual cash may also be a sign of money laundering. It is good practice to establish a policy of never accepting cash payments above a certain limit either at your office or into your bank account. Clients may attempt to circumvent such a policy by depositing cash directly into your client account at a bank. You may consider advising clients in such circumstances that they might encounter a delay in completion of the final transaction. If a cash deposit is received, you will need to consider whether you think there is a risk of money laundering taking place and whether it is a circumstance requiring a disclosure to the NCA.

- Accounts staff should monitor whether funds received from clients are from credible sources.
- Ensure appropriate checks are made and the rationale for and size of a transaction and any payments into your accounts by third parties is clearly understood before any third party payments are accepted into the client account. You may not have to make enquiries into every source of funding from other parties. However, you must always be alert to warning signs and in some cases you will need to get more information.
- Where money is accepted into the client account in respect of a transaction or from a client on account and the transaction is aborted, carefully consider the level of risk analysis and CDD conducted at the outset, the legitimacy of the transaction and the parties to it, and the circumstances of the aborted transaction. You should not return funds without considering the need to make a suspicious activity report. Only return funds to the original sender of those funds and not to any other designated person.

2.4.3 Sale/purchase of real property

- Perform thorough CDD checks.
- Keep up-to-date with emerging issues. It may be useful to review resources from law societies or bar associations in other countries to supplement knowledge in this area.
- Provide information and/or training, where appropriate, to staff on these updates so that they are better equipped to spot issues.
- Information overload can be a warning sign. Money launderers may attempt to inundate the legal professional with information to reduce the chances that they spot the issue or to make them convinced of the transaction's legitimacy.

2.4.4 Creation of trusts, companies and charities

- Perform thorough CDD checks. Be aware of higher risk jurisdictions where ownership may be concealed.
- If a prospective client simply requests you to undertake the mechanical aspects of setting up a trust, company or charity, without seeking legal advice on the appropriateness of the company structure and related matters, conduct further investigation.
- Seek to understand all aspects of the transaction.

2.4.5 Management of trusts and companies

- Ask whether there is a legal reason or if it is customary to have a legal professional on the board of an entity in the relevant country.
- Perform checks on the entities concerned to minimise the money laundering risk.
- Provide information and/or training, where appropriate, to staff on possible red flags.

2.4.6 Unusual transactions

- Do further due diligence, particularly on source of funds.
- Seek to understand the commercial rationale/reason for the transaction structure.
- Provide training on possible red-flags. See section 3.7 on training requirements and Chapter 12 on money laundering warning signs.

2.5 Assessing individual client and retainer risk

Under Regulation 28(12)(a)(i) and (ii), the way in which you comply with CDD requirements must reflect both your practice-wide risk assessment and your assessment of the level of risk arising in the particular case.

In assessing the level of risk arising in a particular case you must take into account:

- the purpose of the transaction or business relationship,
- the size of the transactions undertaken by the customer and
- the regularity and duration of the business relationship.

You should also consider whether:

- Your client is within a high-risk category, including whether:
 - they are based or conduct their business in high-risk jurisdictions and/or sectors
 - the retainer involves high-risk jurisdictions, or appears to fall outside of the sector in which the client ordinarily operates.
- Extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.
- In the event you are aware of negative press or information in respect of your client, which gives you cause for concern in relation to money laundering compliance, you may need to consider:
 - the nature and seriousness of any allegations
 - timing of any allegations and whether any steps might have been taken to address previous problems that have arisen and whether any proceeds of crime have been extracted by a fine
 - the level of press coverage and whether the sources of the allegations are reliable or if there is doubt as to their veracity.
- You can be easily satisfied the CDD material for your client is reliable and allows you to identify the client and verify their identity.
- You can be satisfied that you understand their ownership and control structure (particularly if the client or entities in the control structure are based in jurisdictions which permit nominee owners).

- There are concerns about the source of funds or wealth or there are payments to be made by unconnected third parties or payments in cash.
- The retainer involves an area of law or service at higher risk of laundering or terrorist financing.
- Whether the instructions might be considered to be unusual or higher risk, for example:
 - unusually complicated financial or property transactions or transactions where the commercial rationale is unclear
 - instructions on transactional work outside your area of expertise
 - transactions involving various potentially connected private individuals (as clients or as beneficial owners) in higher risk jurisdictions
 - transactions with an unexplained cross-border element

This assessment will help you to consider whether you are comfortable acting in the particular circumstances and, if so, to adjust your internal controls to the appropriate level of risk presented by the individual client or the particular retainer. Different aspects of your CDD controls will meet the different risks posed:

- If you are satisfied that you have verified the client's identity, but the retainer is high risk, you may require fee earners to monitor the transaction more closely, rather than seek further verification of identity.
- If you have concerns about verifying a client's identity, but the retainer is low risk, you may expend greater resources on verification and monitor the transaction in the normal way.

Risk assessment is an ongoing process both for the practice generally and for each client, business relationship and retainer. It is the overall information held by the legal professional gathered while acting for the client that will inform the risk assessment process, rather than sophisticated computer data analysis systems. The better you know your client and understand your instructions, the better placed you will be to assess risks and spot suspicious activities.

Chapter 3 – Systems, policies, procedures and controls

3.1 General comments

Develop and document systems to meet your obligations and risk profile in a risk-based and proportionate manner. Policies and procedures supporting these systems enable staff to apply the systems consistently and demonstrate to supervisors that processes facilitating compliance are in place.

3.2 Application and requirements

Regulation 19 requires the regulated sector to have written policies, controls and procedures (PCPs) in place to mitigate and manage the AML and CTF risks identified in the practice's risk assessment.

These PCPs need to be proportionate to the size and nature of your practice. They must include:

1. PCPs which provide for the identification and scrutiny of matters where:
 - a transaction is complex and unusual and has no apparent economic or legal purpose
 - there is an unusual pattern of transactions and they have no apparent economic or legal purpose
 - there appears to be no apparent economic or legal purpose, or where the commercial rationale is unclear, and a high risk of money laundering is present.

Legal professionals must carefully consider whether it is appropriate for them to proceed on a matter in the absence of a clear understanding of the nature and purpose of the transaction.

2. Consideration of additional measures to prevent the misuse of products and transactions which favour anonymity.

It is important that you are able to distinguish between those legal services that you provide and/or transactions in which you act which provide or allow the client a legitimate level of anonymity and those where no good reason for that anonymity has been established and understood.

Additional measures could include ensuring a better understanding of the background of the transaction and your role in the matter and/or any wider transaction.

3. Consideration of the AML/CTF risk posed to the practice by new technology/legal service delivery methods adopted by the practice.

Effective management of AML and CTF risks are the responsibility of senior management. As such, all PCPs must be approved by senior management.

Those operating in the regulated sector must ensure their PCPs are documented and available to all relevant staff.

You must regularly review and update your PCPs and maintain a written record of any changes you make to them following such a review. You must also maintain a written record of the steps that you have taken to communicate your PCPs, and any changes to your PCPs, to your staff.

It is vital that, where staff make decisions in line with the PCPs identified by the practice, they record their decisions and, where appropriate, the decision-making process either on the client record or matter file.

3.3 Group-wide application

Practices must consider the application of the Regulations to their wider group. Where a practice is a parent undertaking, it must ensure that its PCPs apply to:

1. All subsidiary undertakings, including those located outside the UK, and
2. All branches established outside the UK, which carry out activities that would fall in the regulated sector in the UK.

Subsidiaries/branches in the EEA: Where the subsidiaries or branches are in an EEA state, the PCPs need to reflect the requirement that these subsidiaries and branches must follow the law of that EEA state transposing the fourth money laundering directive. The parent undertaking will be held responsible for the conduct of its subsidiaries and branches.

Subsidiaries/branches outside of the EEA: If any of the subsidiary undertakings or branches of a parent undertaking are established in a country outside of the EEA which does not impose requirements to counter money laundering and terrorist financing as strict as those of the United Kingdom, the relevant parent undertaking must ensure that those subsidiary undertakings and branches apply measures equivalent to those required by the UK's implementation of the Regulations, as far as permitted under the law of that country.

In the unlikely event that the law of a country does not permit the application of such equivalent measures by the branch or subsidiary undertaking established in that country, the relevant parent undertaking must:

- a) inform its supervisory authority accordingly; and
- b) take additional measures to handle the risk of money laundering and terrorist financing effectively, which should be clearly documented.

As with your practice-wide PCPs, you must regularly review and update your group-wide PCPs and maintain a written record of any changes that you make to them following such a review. You must also maintain a written record of the steps that you have taken to communicate your group wide PCPs, and any changes to them, to your staff.

3.4 Areas to cover

Practices must ensure they have PCPs which address:

1. Risk management practices.
2. Internal controls.
3. CDD controls.

4. Reliance and record keeping.
5. Disclosures to the NCA (and decisions not to make disclosures to the NCA).
6. The monitoring and management of compliance with the PCPs.

3.4.1 Risk management practices

Practices must ensure that they have documented their understanding of the key AML/CTF risks that they face.

They should keep a record of the sources used in completing their AML/CTF risk assessment.

It is important that decisions taken in relation to the application of the PCPs are documented. For example, if a decision is taken to adopt extra controls in relation to a client or matter, you should record the reason for the additional controls and the nature of the controls.

In relation to your risk management practices you may also wish to consider:

- the level of personnel permitted to exercise discretion on the risk-based application of the Regulations, and the circumstances under which that discretion may be exercised
- the CDD requirements to be met for simplified, standard and enhanced due diligence
- when outsourcing of CDD obligations or reliance will be permitted, and on what conditions
- how you will restrict work being conducted on a file where CDD has not been completed
- the circumstances in which delayed CDD is permitted
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- the manner in which disclosures are to be made to the nominated officer.

3.4.2 Internal controls

Regulation 21(1) sets out three internal controls which practices are required to adopt where it is appropriate 'with regard to the size and nature of its business'. Factors you may consider when determining whether it is appropriate to apply those controls include:

- The number of staff members your practice has
- The number of offices your practice has and where they are located (including whether your practice has overseas offices)
- Your client demographic
- The nature and complexity of work your practice undertakes

- The level of visibility and control that senior management has over client matters

You should consider each of the controls set out in Regulation 21(1) separately and need only apply those which are appropriate having regard to the size and nature of your practice.

The controls referred to in Regulation 21(1) are:

1. Appointing an individual as the officer responsible for the practice's compliance with the Regulations.

The individual must be either a member of the board of directors (or equivalent management body) or senior management.

A member of senior management means an officer or employee with sufficient knowledge of your practice's money laundering and terrorist financing risk exposure and sufficient authority to take decisions affecting that risk exposure.

The requirement to appoint an officer responsible for compliance with the Regulations is additional to the requirement to appoint an MLRO. However, your practice's officer responsible for compliance with the Regulations may also be your MLRO or, if applicable, your Compliance Officer for Legal Practice, provided they are of sufficient seniority.

2. Screening relevant employees prior to and during the course of their employment in relation to their skills and knowledge and their conduct and integrity.

Screening could mean having regard to:

- a person's qualifications
- any regulatory, professional and/or ethical obligations to which the person is subject
- checking a person's references.

A 'relevant employee' is someone whose work is relevant to your practice's compliance with the Regulations or who is otherwise capable of contributing to:

- the identification or mitigation of money laundering and terrorist financing risks to which your practice is subject, or
- the prevention and detection of money laundering and terrorist financing in relation to your practice.

3. Establishing an independent audit function to examine, evaluate and make recommendations regarding the adequacy and effectiveness of the practice's PCPs.

You will need to consider the following factors:

- The size of your practice. Smaller practices are unlikely to need such a function, assuming that the individuals within the practice feel that they have a good understanding of the clients and matters undertaken.

- The volume of work. Does your practice manage a high volume of work undertaken by relatively junior staff?
- Complexity of the practice and the work undertaken.
- The extent of the PCPs in place to manage the risks identified in your practice's risk assessment.

An independent audit function does not have to be external to the practice but must be independent of the specific function being reviewed. The independent auditor should have the authority to:

- Access all relevant material to be able to evaluate the adequacy and effectiveness of the PCPs.
- Make recommendations in relation to those PCPs.
- Monitor the practice's compliance with its recommendations.

You should take a risk-based approach to determining how frequently an independent audit should take place. An independent audit will not necessarily need to be carried out annually, but should occur following material changes to your practice's risk assessment.

3.4.3 Nominated officers

Regulation 21(3) requires that all practices within the regulated sector must have a nominated officer to receive disclosures under Part 7 of POCA and the Terrorism Act, and to make disclosures to the NCA.

Regulation 21(6) provides that there is no requirement to have a nominated officer in the regulated sector if you are an individual who provides regulated services but do not employ any people or act in association with anyone else.

Practices who do not provide services within the regulated sector should consider appointing a nominated officer, even though it is not required under the Regulations, because POCA and the Terrorism Act still apply. You may also be subject to regulatory requirements to have business management systems facilitating compliance with legal obligations.

You will need to inform your supervisor of the identity of your MLRO and officer responsible for compliance with the Regulations within 14 days of appointment. You will also need to inform your supervisor of any subsequent appointments to either of those positions within 14 days.

Who should be a nominated officer?

Your nominated officer should be of sufficient seniority to make decisions on reporting which can impact your practice's business relations with your clients and your exposure to criminal, civil, regulatory and disciplinary sanctions. They should also be in a position of sufficient responsibility to enable them to have access to all of your practice's client files and business information, when necessary, to enable them to make the required decisions on the basis of all information held by the practice.

Practices authorised by the FCA will need to obtain the FCA's approval for the appointment of the nominated officer as this is a controlled function under section 59 of the Financial Services and Markets Act 2000.

Role of the nominated officer

Your nominated officer is responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the relevant authority. The decision to report, or not to report, must not be subject to the consent of anyone else. Your nominated officer will also liaise with the NCA or law enforcement on the issue of whether to proceed with a transaction or what information may be disclosed to clients or third parties.

A range of factors, including the type of practice, its size and structure, may lead to the nominated officer delegating certain duties regarding the practice's AML/CTF obligations. In some large practices, one or more permanent deputies of suitable seniority may be appointed. All practices will need to consider arrangements for temporary cover when the nominated officer is absent.

Responding to enquiries from law enforcement agencies

In accordance with Regulation 21(8), practices must establish and maintain systems which enable it to respond fully and rapidly to enquiries from law enforcement agencies as to—

- (a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- (b) the nature of that relationship.

Responses must factor in legal professional privilege, which is not overridden by such requests. Legal professional privilege is covered in more detail in Chapter 7.

3.4.4 Customer due diligence

You are required to have a system outlining the CDD measures to be applied to specific clients. Your risk assessment should record your practice's risk tolerances so that you are able to demonstrate to your supervisor that your CDD measures are appropriate and proportionate.

Your CDD system may include:

1. When CDD is to be undertaken.
2. Information to be recorded on client identity.
3. Information to be obtained to verify identity, either specifically or providing a range of options with a clear statement of who can exercise their discretion on the level of verification to be undertaken in any particular case.
4. When simplified due diligence may occur.
5. What steps need to be taken for enhanced due diligence.
6. What steps need to be taken to ascertain whether your client is a high-risk or low-risk PEP and subsequent controls that will be put in place.
7. When CDD needs to occur and under what circumstances delayed CDD is permitted.

8. How to conduct CDD on existing clients and how often CDD information will be reviewed to ensure that it is up to date.
9. What ongoing monitoring is required.

For further information on conducting CDD see Chapter 4.

3.4.5 Reliance and Record Keeping

Reliance

Your PCPs must cover reliance, which is discussed further in section 4.4. You should consider including in your PCPs:

- the circumstances in which you consider it appropriate to rely on another regulated person, and
- the steps you will take when relying on another regulated person to satisfy yourself that they have complied fully with the requirements of the Regulations.

Record keeping

Your PCPs should set out how your business complies with the record keeping obligations contained in the Regulations, which are discussed further in section 4.8.

3.4.5 Monitoring Compliance with PCPs

Practices must ensure that they regularly review their risk assessment and PCPs, even if they have determined that the size and nature of the practice is such that an independent audit function is not required.

Monitoring compliance will assist you to assess whether the PCPs that you have implemented are effective in identifying and preventing money laundering and terrorist financing opportunities within your practice. Issues which may be covered in such a review may include:

1. Procedures to be undertaken to monitor compliance, which may involve:
 - random file audits
 - file checklists to be completed before opening or closing a file
 - a nominated officer's log of situations brought to their attention, queries from staff and reports made.
2. Reports to be provided to senior management on compliance.
3. How to rectify lack of compliance, when identified.
4. How lessons learnt will be communicated back to staff and fed back into the risk profile of the practice.

3.5 Disclosures

Practices (except sole practitioners) must have a system clearly setting out the requirements for making a disclosure under POCA and the Terrorism Act. These may include:

- the circumstances in which a disclosure is likely to be required
- how and when information is to be provided to the nominated officer or their deputies
- resources which can be used to resolve difficult issues around making a disclosure
- how and when a disclosure is to be made to the NCA
- how to manage a client when a disclosure is made while waiting for consent/DAML
- the need to be alert to tipping off issues

For details on when a disclosure needs to be made see Chapters 6, 7 and 8. For details on how to make a disclosure see Chapter 9.

3.6 Record keeping

Various records must be kept to comply with the Regulations and defend any allegations against the practice in relation to money laundering and failure to report offences. Your records system must outline what records are to be kept, the form in which they should be kept and for how long they should be kept.

Regulation 40 requires that you keep records of CDD material and supporting evidence and records in respect of the relevant business relationship or occasional transaction. Adapt your standard archiving procedures for these requirements.

3.6.1 CDD material

You may keep either a copy of CDD material, or references to it. Keep it for five years after the business relationship ends or the occasional transaction is completed. At the end of the five year period you must delete any personal data in the record unless:

- you are required to retain records containing personal data under any enactment or rule made by your regulator, or
- you are required to retain records containing personal data for the purposes of any court proceedings, or
- you have the consent of the person whose data it is.

Consider holding CDD material separately from the client file for each retainer, as it may be needed by different groups in your practice.

Depending on the size and sophistication of your practice's record storage procedures, you may wish to:

- scan the CDD material and hold it electronically

- take photocopies of CDD material and hold it in hard copy with a statement that the original has been seen
- accept certified copies of CDD material and hold them in hard copy
- keep electronic copies or hard copies of the results of any electronic verification checks
- record reference details of the CDD material sighted.

The option of merely recording reference details may be particularly useful when taking instructions from clients at their home or other locations away from your office. The types of details it would be useful to record include:

- any reference numbers on documents or letters
- any relevant dates, such as issue, expiry or writing
- details of the issuer or writer
- all identity details recorded on the document.

Where you are relied upon by another person under Regulation 39 for the completion of CDD measures, you must keep the relevant documents for five years from the date on which you were relied upon.

3.6.2 Risk assessment notes

Under the Regulation 28(12)(a)(i) and (ii), the way in which you comply with CDD requirements must reflect both your practice-wide risk assessment and your assessment of the level of risk arising in the particular case.

You should consider keeping records of decisions on risk assessment processes of what CDD was undertaken. This does not need to be in significant detail, but merely a note on the CDD file stating the risk level you attributed to a file and why you considered you had sufficient CDD information. For example:

'This is a low risk client with no beneficial owners providing medium risk instructions. Standard CDD material was obtained and medium level ongoing monitoring is to occur.'

Such an approach may assist practices to demonstrate they have applied a risk-based approach in a reasonable and proportionate manner. Notes taken at the time are better than justifications provided later.

3.6.3 Supporting evidence and records

You must keep all original documents or copies admissible in court proceedings.

Records of a particular transaction, either as an occasional transaction or within a business relationship, must be kept for five years after the date on which the transaction is completed.

All other documents supporting records must be kept for five years after the completion of the business relationship.

3.6.4 Suspicions and disclosures

You should keep comprehensive records of suspicions and disclosures because disclosure of a suspicious activity is a defence to criminal proceedings. Such records may include notes of:

- ongoing monitoring undertaken and concerns raised by fee earners and staff
- discussions with the nominated officer regarding concerns
- advice sought and received regarding concerns
- why the concerns did not amount to a suspicion and a disclosure was not made
- copies of any disclosures made
- conversations with the NCA, law enforcement agencies, insurers and supervisory authorities regarding disclosures made
- decisions not to make a report to the NCA which may be important for the nominated officer to justify his or her position to law enforcement agencies.

You should ensure that records are not inappropriately disclosed to the client or third parties to avoid offences of tipping off and prejudicing an investigation, and to maintain a good relationship with your clients. This may be achieved by maintaining a separate file, either for the client or for the practice area.

3.6.5 Data protection

The Data Protection Act 1998 applies to you and the NCA. It allows clients or others to make subject access requests for data held by you. Such requests could cover any disclosures made.

Section 29 of the Data Protection Act 1998 states that you need not provide personal data where disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

[HM Treasury and the Information Commissioner have issued guidance](#) which essentially provides that the section 29 exception would apply where granting access would amount to tipping off. This may extend to suspicions only reported internally within the practice.

If you decide that the section 29 exception applies, document steps taken to assess this, to respond to any enquiries by the Information Commissioner.

Under Regulation 41(3) you cannot use personal information which you obtain for the purposes of complying with the Regulations for any other purpose unless you are authorised to do so under another enactment or you have the person's consent. In addition, you are required to provide new clients with the information specified in paragraph 2(3) in Part 2 of Schedule 1 to the Data Protection Act 1998 (interpretation of data protection principles) and a statement that any personal data received from the client will only be processed for the purposes of preventing money laundering or terrorist financing and any other purposes to which they have consented.

3.7 Communication and training

Your staff members are the most effective defence against launderers and terrorist financiers who would seek to abuse the services provided by your practice.

Regulation 24 requires that you ensure relevant employees:

- Are made aware of the law relating to money laundering, terrorist financing and the requirements of data protection which are relevant to the implementation of the Regulations, and
- Are regularly provided with training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

Professional regulatory requirements may also oblige you to train your staff to a level appropriate to their work and level of responsibility. You may consider providing relevant employees with appropriate training and equipment to help identify forged documents.

3.7.1 Criminal sanctions and defences

Receiving insufficient training is a defence for individual staff members who fail to report a suspicion of money laundering, provided they did not know or suspect money laundering. However, it is not a defence to terrorist funding charges, and leaves your practice vulnerable to sanctions under the Regulations for failing to properly train your staff.

3.7.2 Who should be trained?

When setting up a training and communication system you should consider:

- which staff require training
- what form the training will take
- how often training should take place
- how staff will be kept up-to-date with emerging risk factors for the practice

Assessments of who should receive training should include who deals with clients in areas of practice within the regulated sector, handles funds or otherwise assists with compliance. Consider fee earners, reception staff, administration staff and finance staff, because they will each be differently involved in compliance and so have different training requirements.

Training can take many forms and may include:

- face-to-face training seminars
- completion of online training sessions
- attendance at AML/CTF conferences
- participation in dedicated AML/CTF forums
- review of publications on current AML/CTF issues

- practice or practice group meetings for discussion of AML/CTF issues and risk factors.

Providing an AML/CTF policy manual is useful to raise staff awareness and can be a continual reference source between training sessions.

3.7.3 How often?

You must give your employees relevant training at regular and appropriate intervals. In determining whether your training programme meets this requirement, you should have regard to the practice's risk profile and the level of involvement certain staff have in ensuring compliance.

You should consider retaining evidence of your assessment of training needs and steps taken to meet such needs.

You should also consider:

- criminal sanctions and reputational risks of non-compliance
- developments in the common law
- changing criminal methodologies.

You should take a risk-based approach to determining how often training should take place. Some type of training every two years is preferable.

3.7.4 Communicating with your clients

While not specifically required by the Regulations, we consider it useful for you to tell your client about your AML/CTF obligations. Clients are then generally more willing to provide required information when they see it as a standard requirement.

You may wish to advise your client of the following issues:

- the requirement to conduct CDD to comply with the Regulations
- whether any electronic verification is to be undertaken during the CDD process
- the requirement to report suspicious transactions.

Consider the manner and timing of your communications, for example whether the information will be provided in the standard client care letter or otherwise.

Chapter 4 – Customer due diligence

Note: Section 4.12.2.4 (Senior management approval) of this Chapter may not apply to self-employed barristers or advocates who are practising from chambers or as sole practitioners.

4.1 General comments

CDD is required by the Regulations; you are in a better position to identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you.

4.2 Application

You must apply CDD on those clients who retain you for services regulated under the Regulations. See section 1.4.5 for further guidance on the scope of the regulated sector.

4.3 CDD in general

4.3.1 When is CDD required?

Regulation 27 requires that you apply CDD when:

- establishing a business relationship
- carrying out an occasional transaction that amounts to 15,000 Euros or more, whether it is executed in a single operation or in several operations which appear to be linked
- you suspect money laundering or terrorist financing
- you doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

The distinction between occasional transactions and long-lasting business relationships is relevant to the timing of CDD and the time period for record keeping.

Where an occasional transaction is likely to increase in value or develop into a business relationship, consider conducting CDD early in the retainer to avoid delays later. As relationships change, practices must ensure they are compliant with the relevant standard.

There is no obligation to conduct CDD in accordance with the Regulations for retainers involving non-regulated activities. However, many practices do conduct CDD on all new clients, regardless of the nature of the matter. This enables you to know your client from the outset and clients can be 'passport-ed' easily between a practice's non-regulated and regulated departments.

4.3.2 What is CDD?

Regulation 28 requires that you:

- Identify the client and verify their identity on the basis of documents or information obtained from a reliable source which is independent of the client, unless the identity of the client is already known to you and has been verified by you.
- Identify where there is a beneficial owner who is not the client and take reasonable measures to verify the identity so that you are satisfied that you know who the beneficial owner is. This includes taking reasonable measures to understand the ownership and control structure of a legal person, trust, company, foundation or similar legal arrangement.
- Assess and where appropriate obtain information on the purpose and intended nature of the business relationship or occasional transaction.

Identification and verification

Identification of a client or a beneficial owner is simply being told or coming to know a client's identifying details, such as their name and address.

Verification is obtaining some evidence which supports this claim of identity.

A risk-based approach

Regulation 28(12) provides that when complying with the requirement to take CDD measures, which may differ from case to case, you must reflect:

- the practice's risk assessment required under Regulation 18, and
- your assessment of the level of risk arising in any particular case.

Regulation 28(13) provides that in assessing the risk you must take account of factors including:

- the purpose of a transaction or business relationship
- the size of the assets or of the transactions undertaken
- the regularity and duration of the business relationship.

You cannot avoid conducting CDD, but you can use a risk-based approach to determine the extent and quality of information required and the steps to be taken to meet the requirements.

4.3.3 General Information - methods of verification

Verification should be completed on the basis of documents or information which come from a reliable source, independent of the customer. This means that there are a number of ways in which you can verify a client's identity including:

- obtaining or viewing original documents
- conducting electronic verification
- obtaining information from other regulated persons
- obtaining information from other reliable publicly available sources

Independent source

You need a reliable source to verify your client's identity, which is independent of the client. This can include materials provided by the client, such as a passport.

Consider the cumulative weight of information you have on the client and the risk levels associated with both the client and the retainer.

You are permitted to use a wider range of sources when verifying the identity of the beneficial owner and understanding the ownership and control structure of the client. Sometimes only the client or their representatives can provide you with such information. Apply the requirements in a risk-based manner to a level at which you are satisfied that you know who the beneficial owner is.

Regulation 28(9) confirms that the register of people with significant control, or confirmation statement, which is published on the Companies House website, may not be solely relied upon for the purpose of identifying the beneficial owner of a company or LLP client. So, in addition, it will be necessary to obtain further verification, for example confirmation from the client that the information is up to date or other documentation confirming the beneficial ownership of the client.

Documents

You should not ignore obvious forgeries, but you are not required to be an expert in forged documents. You may consider providing relevant employees with appropriate training and equipment to help identify forged documents.

Electronic verification

You should consider whether any electronic verification system you use properly establishes the customer's identity, rather than just establishing that the identity exists. You should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that your client is not the person they say they are. You may mitigate risk by corroborating electronic verification with some other CDD material.

When choosing an electronic verification service provider, you should look for a provider who:

- has proof of registration with the Information Commissioner's Office to store personal data
- can link an applicant to both current and previous circumstances using a range of positive information sources
- accesses negative information sources, such as databases on identity fraud and deceased persons
- accesses a wide range of 'alert' data sources
- has transparent processes enabling you to know what checks are carried out, the results of the checks, and how much certainty they give on the identity of the subject
- allows you to capture and store the information used to verify an identity.

When using electronic verification, you are not required to obtain consent from your client, but they must be informed that this check will take place.

While electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate.

4.4 Reliance and outsourcing

Reliance has a specific meaning within the Regulations and relates to the process under Regulation 39 where, in certain circumstances, you may rely on another person to conduct CDD for you, subject to their agreement.

Reliance is an important feature of the Regulations as in certain circumstances it may allow relevant persons to avoid unnecessary duplication in complying with their CDD obligations. As well as reducing the regulatory burden on relevant persons, reliance may be in the interests of your client as it can facilitate swift and convenient access to services. For example, if you instruct another legal professional (or other regulated person) on behalf of your client, then allowing that person to rely on the CDD checks you have already undertaken may enable your client to access those services sooner than they otherwise would have.

It is important to note that reliance, as set out in Regulation 39, is not:

- accepting information from others to verify a client's identity when meeting your own CDD obligations, or
- electronic verification, which is outsourcing.

4.4.1 Relying on a third party

In order to rely on another regulated person to apply CDD measures you must:

- Immediately obtain from the other person all the information needed to satisfy the requirement to apply CDD measures in accordance with Regulations 28(2) to (6) and (10)
- Enter into arrangements with the other person, which
 - enable you to obtain from the other person immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the customer or its beneficial owner; and
 - require the third party to retain copies of the data and documents in accordance with Regulation 40.
- Obtain evidence to establish that the person relied upon falls into the category of persons who may be relied upon (per Regulation 40(3)).

You should note that you remain liable for any non-compliance with CDD requirements when you rely on another person. For this reason you should ask what CDD enquiries the other person has undertaken to ensure that they actually comply with the Regulations and the risk-based approach. This is particularly important when relying on a person outside the UK. Before relying on a person outside the UK you should be satisfied that the CDD has been conducted to a standard compatible with

the 4th Directive, taking into account the ability to use different sources of verification and jurisdictional specific factors.

You should ensure that the CDD information provided to you is not out of date, and be aware that the risk assessment of the person you are relying on may not match your own. It may not always be appropriate to rely on another person and you should consider reliance as a risk in itself.

4.4.2 Granting reliance

Another relevant person may seek to rely on the CDD checks you have completed, and this will often be the case where you instruct such a person on behalf of your client. In such a situation you should consider whether you wish to enter into an arrangement to allow the relevant person to rely on your CDD checks, noting that it may be beneficial for your client.

Before agreeing to enter into such an arrangement, you should ensure that:

- You can make CDD information available immediately on request, and
- You have appropriate consent from your client to disclose the CDD information to the other party.

You may be concerned that, by granting reliance, there is a risk you may at some point become liable to the party who relies if they suffer a loss as a result of their reliance. However, to address this concern you may wish to consider adopting an exclusion of liability clause as part of the arrangement allowing reliance between you and the other party.

Before granting reliance you should also consider whether, by doing so, you would be breaching a contract with another party, such as an electronic verification service provider. If you would be breaching such a contract by granting reliance then you should still confirm to the other party that you have in fact completed CDD checks on the client (although this will not constitute granting reliance).

4.4.3 Reliance in the UK

You can only rely on the following persons in the UK:

- a credit or financial institution as defined in Regulation 10
- auditors, insolvency practitioners, external accountants and tax advisers as defined in Regulation 11
- independent legal professionals as defined in Regulation 12
- trust or company service providers as defined in Regulation 12(2)
- estate agents as defined in Regulation 13
- high value dealers as defined in Regulation 14(1)
- casinos as defined in Regulation 14(2)

4.4.4 Reliance in an EEA state

You can only rely on a person in an EEA state if they are:

- subject to requirements in national legislation implementing the fourth money laundering directive; and
- supervised for compliance with the requirements laid down in the 4th Directive in accordance with section 2 of Chapter VI of that directive

4.4.5 Reliance in other countries

You can rely on a person who carries on business in a third country, other than a 'high-risk third country', only if they are:

- subject to requirements in relation to CDD and record keeping equivalent to those laid down in the 4th Directive; and
- supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter VI of the 4th Directive

4.4.6 High Risk Third Countries

You cannot rely on a third person established in a country that has been designated by the European Commission as high risk third country, unless:

- the third person is a branch or majority owned subsidiary of a person established in an EEA state who is subject to the fourth money laundering directive; and
- the branch or subsidiary complies fully with the procedures and policies established for the group under Article 45 of the 4th Directive

The list of countries designated as high risk third countries by the European Commission is contained in [Commission Delegated Regulation \(EU\) 2016/1675](#).

4.4.7 Passporting clients between jurisdictions

Many practices have branches or affiliated offices ('international offices') in other jurisdictions and will have clients who utilise the services of a number of international offices. It is not considered proportionate for a client to have to provide original identification material to each international office.

Some practices may have a central international database of CDD material on clients to which they can refer. Where this is the case you should review the CDD material to be satisfied that CDD has been completed in accordance with the implementation of the 4th Directive in that jurisdiction. If further information is required, you should ensure that it is obtained and added to the central database. Alternatively, you could ensure that the CDD approval controls for the database are sufficient to ensure that all CDD is compliant.

Other practices may wish to rely on their international office simply to provide a letter of confirmation that CDD requirements have been undertaken with respect to the client. This is acceptable provided that:

- the international office is a member of the same group;

- that group applies CDD measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with the Regulations, the 4th Directive, or rules having the equivalent effect; and
- the effective implementation of those requirements is supervised at group level by an authority of an EEA state with responsibility for the implementation of the 4th Directive or by an equivalent authority of a third country.

Finally, practices without a central database may wish to undertake their own CDD measures with respect to the client, but ask their international office to supply copies of the verification material, rather than the client themselves. This will not be reliance, but outsourcing. Outsourcing is permitted under Regulation 39(7), on the condition that the arrangements with the outsourcing provider provide that you remain liable for any failure to apply CDD measures.

It is important to note that you will need to have in place a process for checking whether a person passported into your office is a PEP and, if so, undertake appropriate enhanced due diligence measures.

UK-based fee earners will have to undertake their own ongoing monitoring of the retainer, even if the international office is also required to do so.

4.5 Timing

4.5.1 When must CDD be undertaken?

Regulation 30 requires you to verify your client's identity, the identity of any person purporting to act on their behalf and that of any beneficial owner, before you establish a business relationship or carry out transaction which amounts to 15,000 Euros or more.

Regulation 31 provides that if you are unable to complete CDD in time, you cannot:

- carry out a transaction with or for the client through a bank account
- establish a business relationship or carry out a transaction otherwise than through a bank account.

You must also:

- terminate any existing business relationship
- consider making a disclosure to the NCA.

You cannot seek consent from the NCA to proceed with a transaction where you have been unable to complete CDD measures as required by Regulation 28.

Although you must consider making a disclosure to the NCA where you have been unable to complete CDD this does not mean you are automatically required to submit a SAR. You should only make a disclosure to the NCA if you have a reportable suspicion or knowledge of money laundering or terrorist financing and the information is not covered by legal professional privilege. Further information on making a disclosure is contained in Chapter 9 and practical examples are contained in Chapter 13.

Regulation 31(2) confirms that you are not prevented from repaying money deposited in the client account, provided that, if a disclosure to NCA is required, because you have the necessary suspicion, you obtain consent/DAML from NCA for the transaction.

4.5.2 Exceptions to the timing requirement

There are several exceptions to the timing requirement and the prohibition on acting for the client.

However, you should consider why there is a delay in completing CDD, and whether this of itself gives rise to a suspicion which should be disclosed to the NCA.

Normal conduct of business

Regulation 30(3) provides that verification of the client and the beneficial owner may be completed as soon as practicable after contact is first established, during the establishment of the business relationship if:

- it is necessary not to interrupt the normal conduct of business, and
- there is little risk of money laundering or terrorist financing.

This exception does not apply if your matter is an occasional transaction.

Consider your risk profile when assessing which work can be undertaken on a retainer prior to verification being completed. When applying CDD to a trust, or other legal arrangement or entity which is not a company, involving a class of beneficiaries, you must always verify the identity of the beneficiary or beneficiaries before any payment is made to them or they exercise their vested rights in the trust (see Regulation 30 (7)).

Do not undertake substantive work, permit funds to be deposited in your practice's client account, property to be transferred or final agreements to be signed before completion of full verification.

If you are unable to conduct full verification of the client and beneficial owners, then the prohibition in Regulation 31 will apply.

Ascertaining legal position

Regulation 31(3) provides that the prohibition in 31(1) does not apply where:

'An independent legal professional or other professional adviser is in the course of ascertaining the legal position for their client or performing the task of defending or representing that client in, or concerning, legal proceedings, including giving advice on the institution or avoidance of proceedings.'

The requirement to cease acting and consider making a report to the NCA when you cannot complete CDD does not apply when you are providing legal advice or preparing for or engaging in litigation or alternative dispute resolution.

This exception does not apply to transactional work, so take a cautious approach to the distinction between advice and litigation work, and transactional work.

4.6 Ongoing monitoring

Regulation 28(11) requires that you conduct ongoing monitoring of a business relationship. Ongoing monitoring is defined as:

- scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with your knowledge of the client, their business and the risk profile
- undertaking reviews of existing records and keeping the documents, or information obtained for the purpose of applying CDD, up-to-date.

You must also be aware of obligations to keep clients' personal data updated under the Data Protection Act 1998 and the General Data Protection Regulation, which will apply in the UK from 25 May 2018.

You are not required to:

- conduct the whole CDD process again every few years
- suspend or terminate a business relationship until you have updated information or documents, as long as you are still satisfied you know who your client is, and keep under review any request you have made for up to date information or documents
- use sophisticated computer analysis packages to review each new retainer for anomalies.

Many practices operate a system of regular review and renewal of CDD as good practice.

Ongoing monitoring will normally be conducted by legal professionals handling the retainer, and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material. A high degree of professionalism and scrutiny is expected from legal professionals – see *R v Griffiths & Pattison* (2007) CA which confirmed that legal professionals are expected to fulfill these obligations 'up to the hilt'.

For example, you may have acted for a client in preparing a will and purchasing a modest family home. They may then instruct you in the purchase of a holiday home, the value of which appears to be outside the means of the client's financial situation as you had previously been advised in earlier retainers. While you may be satisfied that you still know the identity of your client, as a part of your ongoing monitoring obligations it would be appropriate in such a case to ask about the source of the funds for this purchase. Depending on your client's willingness to provide you with such information and the answer they provide, you will need to consider whether you are satisfied with that response, want further proof of the source of the funds, or need to discuss making a disclosure to the NCA with your nominated officer.

In circumstances where no subsequent action was taken/change effected as a result of the obligation to conduct ongoing monitoring through the lifecycle of a transaction, it is suggested that practices record:

- that they considered this issue,
- that they took no action, and

- the reasons for that decision.

A brief note to this effect should be recorded.

4.7 New instructions from an existing client

In accordance with Regulation 27(9) you must apply CDD to existing clients on a risk-sensitive basis and when you become aware that the circumstances of the existing client have changed.

In determining this, you must take into account:

- any indication that the identity of the client, or beneficial owner has changed
- any transactions which are not reasonably consistent with your knowledge of the client
- any change in the purpose or nature of the relationship
- any other matter which may affect your assessment of the money laundering or terrorist financing risk in relation to the client

It is good practice to refresh the CDD if there has been a gap of over three years between instructions. You must update the CDD when you become aware of any changes to the client's identification information. This will include change of name, address or business.

You are not required to undertake a renewal of CDD if there has been no change in the risk profile of the client, the type of work you are undertaking or their personal details.

4.8 Records

Regulation 40 requires you to keep records of your CDD documents and information and sufficient supporting records in respect of a transaction (whether or not an occasional transaction) which is the subject of CDD or ongoing monitoring to enable the transaction to be reconstructed.

This includes information and documentation obtained in connection with source of funds checks and the process of the transaction itself.

You must retain the records for a period of five years beginning on the date on which you knew or had reasonable grounds to believe that the occasional transaction was complete or the business relationship had come to end.

On expiry of this period, you must delete any personal data, unless:

- you are required to retain it by another enactment
- you are retaining the data for the purposes of any court proceedings
- the client has given consent to the retention
- you have reasonable grounds for believing that the records containing personal data need to be retained for the purposes of legal proceedings.

You are not required to retain the records relating to a transaction which occurred as part of a business relationship for more than 10 years.

Many practices will wish to retain the complete file of papers, including CDD records, for a period exceeding that which is specified in Regulation 40(3). For example, your practice's retention policy may specify longer retention times to take account of the expiry of limitation periods for potential negligence actions against the practice. If there any variation on the period prescribed in Regulation 40(3), the client's consent must be obtained. This consent clause can be contained in your engagement letter or terms of business and should be signed or acknowledged by the client.

4.9 CDD on clients

Your practice will need to make its own assessment as to what evidence is appropriate to verify the identity of your clients. We outline a number of sources which may help you make that assessment.

4.9.1 Natural persons

A natural person's identity comprises a number of aspects, including their name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances. Their identity must be verified in accordance with Regulation 28, on the basis of documents or information obtained from a reliable source which is independent of the client. You should use information or documents from a reliable source.

Evidence of identity can include:

- identity documents such as passports and photocard driving licences
- other forms of confirmation, including assurances from persons within the regulated sector or those in your practice who have dealt with the person for some time.

In most cases of face to face verification, producing a valid passport or photocard identification should enable most clients to meet the AML/CTF identification requirements.

It is good practice to have either:

- one government document which verifies either name and address or name and date of birth
- a government document which verifies the client's full name and another supporting document which verifies their name and either their address or date of birth.

Where it is not possible to obtain such documents, consider the reliability of other sources and the risks associated with the client and the retainer. Electronic verification may be sufficient verification on its own as long as the service provider uses multiple sources of data in the verification process.

Where you are reasonably satisfied that an individual is nationally or internationally known, for example, because they are a public figure or a well-known celebrity, a

record of identification may include a file note of your satisfaction about identity, usually including an address.

UK residents

The following sources may be useful for verification of UK-based clients:

- current signed passport
- birth certificate
- marriage certificate
- current photocard driver's licence
- current EEA member state identity card
- current identity card issued by the Electoral Office for Northern Ireland
- residence permit issued by the Home Office
- firearms certificate or shotgun licence
- photographic registration cards for self-employed individuals and partnerships in the construction industry
- benefit book or original notification letter confirming the right to benefits
- council tax bill
- utility bill or statement, or a certificate from a utilities supplier confirming an arrangement to pay services on pre-payment terms
- a cheque or electronic transfer drawn on an account in the name of the client with a credit or financial institution regulated for the purposes of money laundering
- bank, building society or credit union statement or passbook containing current address
- entry in a local or national telephone directory confirming name and address
- confirmation from an electoral register that a person of that name lives at that address
- a recent original mortgage statement from a recognised lender
- legal professional's letter confirming recent house purchase or land registry confirmation of address
- local council or housing association rent card or tenancy agreement
- HMRC self-assessment statement or tax demand
- house or motor insurance certificate
- record of any home visit made
- statement from a member of the practice or other person in the regulated sector who has known the client for a number of years attesting to their

identity. Bear in mind you may be unable to contact this person to give an assurance supporting that statement at a later date.

Adopting a risk based approach you may consider confirming these sources as valid by checking with the issuing authority. If the issuing authority is not able to confirm the validity of the source this does not necessarily mean it is invalid. For example, the issuing authority may decline to tell you whether it is valid because to do so would reveal someone's personal data.

Persons not resident in the UK

Where you meet the client you are likely to be able to see the person's passport or national identity card. If you have concerns that the identity document might not be genuine, contact the relevant embassy or consulate.

The client's address may be obtained from:

- an official overseas source
- a reputable directory
- a person regulated for money laundering purposes in the country where the person is resident who confirms that the client is known to them and lives or works at the overseas address given.

If documents are in a foreign language you must take appropriate steps to be reasonably satisfied that the documents in fact provide evidence of the client's identity.

When you do not meet the client, you should consider the reason for this and whether this represents an additional risk which should be taken into account in your risk assessment of the client and the extent of the CDD measures you apply.

Clients unable to produce standard documentation

Sometimes clients are unable to provide standard verification documents. The purpose of the Regulations is not to deny people access to legal services for legitimate transactions, but to mitigate the risk of legal services being used for the purposes of money laundering. You should consider whether the inability to provide you with standard verification is consistent with the client's profile and circumstances or whether it might make you suspicious that money laundering or terrorist financing is occurring.

If you decide that a client has a good reason for not meeting the standard verification requirements, you may accept a letter from an appropriate person who knows the individual and can verify the client's identity.

For example:

- Clients in care homes might be able to provide a letter from the manager.
- Clients without a permanent residence might be able to provide a letter from a householder named on a current council tax bill or a hostel manager, confirming temporary residence.

- A refugee might be able to provide a letter from the Home Office confirming refugee status and granting permission to work, or a Home Office travel document for refugees.
- An asylum seeker might be able to provide their registration card and any other identity documentation they hold, or a letter of assurance as to identity from a community member such as a priest, GP, or local councillor who has knowledge of the client.
- A student or minor might be able to provide a birth certificate and confirmation of their parent's address or confirmation of address from the register of the school or higher education institution.
- A person with mental health problems or mental incapacity might know medical workers, hostel staff, social workers, deputies or guardians appointed by the court who can locate identification documents or confirm the client's identity.

Professionals

Where other professionals use your services in their capacity as a professional rather than a private individual, you may consult their professional directory to confirm the person's name and business address. It will not be necessary to then confirm the person's home address. You may consult directories for foreign professionals, if you are satisfied it is a valid directory, e.g. one produced and maintained by their professional body, and if necessary, you can translate the information unless you already have a sufficient understanding of what it says.

Persons acting on behalf of the client

In accordance with Regulation 28(10) where a person (the representative) purports to act on behalf of your client, you must:

- verify that the representative is authorised to act on your client's behalf
- identify the representative
- verify the identity of the representative on the basis of documents and information from a reliable source which is independent of both the representative and the client.

4.9.2 Partnerships, limited partnerships, Scottish limited partnerships and UK LLPs

A partnership, other than in Scotland, is not a separate legal entity, so you must obtain information on the constituent individuals.

Where partnerships or unincorporated businesses are:

- well-known, reputable organisations
- with long histories in their industries, and
- with substantial public information about them, their principals, and controllers.

The following information should be sufficient:

- name
- registered address, if any
- trading address
- nature of business.

Other partnerships and unincorporated businesses which are small and have few partners should be treated as private individuals. Where the numbers are larger, they should be treated as private companies.

Where a partnership is made up of regulated professionals, it will be sufficient to confirm the practice's existence and the trading address from a reputable professional directory or search facility with the relevant professional body. Otherwise you should obtain evidence on the identity of at least the partner instructing you and one other partner, and evidence of the practice's trading address.

For a UK LLP, you should obtain information in accordance with the requirements for companies as outlined below.

4.9.3 Companies

A company is a legal entity in its own right, but conducts its business through representatives. You must identify and verify the existence of the company.

A company's identity comprises its constitution, its business and its legal ownership structure.

Where a company is a well-known household name, you may consider that the level of money laundering and terrorist financing risks are low and apply CDD measures in a manner which is proportionate to that risk.

Where you commence acting for a subsidiary of an existing client, you may have reference to the CDD file for your existing client for verification of details for the subsidiary, provided that the existing client has been identified to the standards of the Regulations.

You will also need to consider the identity of beneficial owners where you cannot apply simplified due diligence.

Public companies listed in the UK

Regulation 28(3) requires that, in all cases, if a client is a corporate body you must obtain and verify:

- its name
- the company number or other registration number, and
- the address of the registered office and, if different, principal place of business.

Unless the body corporate is a company listed on a regulated market, you must also take reasonable measures to determine and verify:

- the law to which it is subject and its constitution
- the full names of the board of directors (or equivalent management body) and senior persons responsible for its operations.

In accordance with Regulation 28(5), if the company is listed on a regulated market it is not necessary to:

- obtain information about the beneficial owners of the company, or
- take reasonable measures to determine and verify the law to which it is subject or the names of its directors and senior persons.

The fact that a company's securities are listed on a regulated market is also one of the factors specified in Regulation 37(3) which you must take into account when deciding whether the risk is low and whether to apply simplified due diligence to a particular client. Simplified due diligence can also be applied to a majority-owned subsidiary of such a company.

Following an assessment that the client is low risk it will be sufficient, for a listed company, to obtain confirmation of the company's listing on the regulated market. Such evidence may be:

- a copy of the dated page of the website of the relevant stock exchange showing the listing
- a photocopy of the listing in a reputable daily newspaper
- information from a reputable electronic verification service provider or online registry.

For a subsidiary of a listed company you will also require evidence of the parent/subsidiary relationship. Such evidence may be:

- the subsidiary's last filed annual return
- a note in the parent's or subsidiary's last audited accounts
- information from a reputable electronic verification service provider or online registry
- information from the parent company's published reports, for example, from their website.

The regulated market in the UK is the London Stock Exchange. AIM is not considered a regulated market within the UK, but under the risk-based approach you may feel that the due diligence process for listing on AIM gives you equivalent comfort as to the identity of the company under consideration.

Where further CDD is required for a listed company (i.e. when it is not on a regulated market) obtain relevant particulars of the company's identity.

Verification sources may include:

- a search of the relevant company registry (such as [Companies House](#))
- a copy of the company's certificate of incorporation
- information from a reputable electronic verification service provider

You are still required to conduct ongoing monitoring of the business relationship with a publicly-listed company to enable you to spot suspicious activity. See section 4.6 for further guidance on ongoing monitoring.

Private and unlisted companies in the UK

Private companies are generally subject to a lower level of public disclosure than public companies. In general however, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

You must obtain and verify:

- the name
- the company number or other registration number
- the address of the registered office and principal place of business

You must take reasonable measures to determine and verify:

- the law to which it is subject and its constitution
- the full names of the board of directors(or equivalent management body) and senior persons responsible for its operations.

Sources for verifying corporate identification may include:

- certificate of incorporation
- details from the relevant company registry, confirming details of the company and of the director/s and their address
- filed audited accounts
- information from a reputable electronic verification service provider.

In lower risk cases you may be able to satisfy the requirement to take reasonable steps to determine and verify the law to which the company is subject and its constitution by ensuring that you understand the type of business and transactions the company can engage in.

Regulation 43 requires UK companies not listed on a regulated market to provide information about their identity on request, including their articles of association or other governing documents and information about beneficial owners.

Public overseas companies

You must obtain and verify the:

- company name
- company number or other registration number
- address of the registered office and, if different, principal place of business

You must take reasonable measures to determine and verify the:

- law to which it is subject and its constitution

- full names of the board of directors (or equivalent management body) and senior persons responsible for its operations.

In accordance with Regulation 28(5), if the company is listed on a regulated market it is not necessary to:

- obtain information about the beneficial owners of the company, or
- take reasonable measures to determine and verify the law to which it is subject or the names of its directors and senior persons.

This may also be applied to a majority-owned subsidiary of such a company.

“Regulated market” is defined as follows:

- (a) Within the EEA, the meaning given by Article 4.1 (14) of the Markets in Financial Instruments Directive
- (b) Outside the EEA, a regulated financial market which subjects companies whose securities are admitted to trading to disclosure obligations which are equivalent to the specified disclosure obligations.
- (c) Specified disclosure obligations are disclosure requirements consistent with specified articles of:
 - The Prospectus Directive [2003/71/EC]
 - The Transparency Obligations Directive [2004/109/EC]
 - The Market Abuse Regulation [No 596/2014]

If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. Under a risk-based approach you may wish to simply record the steps taken to ascertain the status of the market.

Consider a similar approach for non-EEA markets that subject companies to disclosure obligations which are contained in international standards equivalent to specified disclosure obligations in the EU.

Consult the register on the [European Securities and Markets Authority website](#).

Evidence of the company's listed status should be obtained in a manner similar to that for UK public companies. Companies whose listing does not fall within the above requirements should be identified in accordance with the provisions for private companies.

Private and unlisted overseas companies

Obtaining CDD material for these companies can be difficult, particularly regarding beneficial ownership.

You should apply the risk-based approach, looking at the risk of the client generally, the risk of the retainer and the risks presented as a result of the country in which the client is incorporated. Money laundering risks are likely to be lower where the company is incorporated or operating in an EEA state or a country which is a member of FATF.

The company's identity is established in the same way as for UK private and unlisted companies.

Where you are not obtaining original documentation, you may want to consider on a risk-sensitive basis having the documents certified by a person in the regulated sector or another professional whose identity can be checked by reference to a professional directory.

4.9.4 Other arrangements or bodies

Trusts

Who is the client?

Trusts, including express trusts, do not have legal personality. As such, you cannot take on a trust as your client. When advising in relation to a trust your client may be the either:

- the settlor
- the trustee(s)
- the protector(s) or
- one or more of the beneficiaries.

Determining which of the settlor, the trustee(s), the protector(s) or one or more of the beneficiaries is/are your client(s) will involve an analysis of the person to whom you owe your duty of care and who will receive the benefit of your advice.

Where an express trust has yet to be established and you are providing tax or transactional advice to a prospective settlor in anticipation of creating a trust your client will usually be the settlor. If your client is represented by an intermediary, ensure that you comply with Regulation 28(10) and identify and verify the intermediary's identity and authority to act on behalf of your underlying client.

Your CDD will also involve identifying and verifying the identity of your settlor client and, if applicable, understanding the settlor's net wealth and the nature and extent of the assets that will be settled on the trust. The information and documents you obtain will depend on whether your client is a natural person or an entity. If the settlor is an entity you will also need to understand its beneficial owner.

When should a trust's beneficial owners be considered?

If you go on to advise a settlor on trust affairs once the trust has been established, and whenever you are instructed by someone involved with an existing trust to advise in relation to it, you will need to extend your CDD to the trust's beneficial owners.

Regulation 28(4)(a) requires a relevant person to identify the beneficial owner 'of a customer' which is beneficially owned by another person. Regulation 6(1) defines 'the beneficial owners in relation to a trust' as the settlor, the trustees, the beneficiaries (or class of beneficiaries) and any individual who has control over the trust. Although your client will not actually be the trust (because a trust does not have legal personality), if

you advise any client in relation to a trust, the Regulations require you to understand who the trust's other beneficial owners are, as defined in Regulation 6(1).

Does enhanced CDD apply?

UK common law trusts are used extensively in everyday situations and often pose a limited risk of money laundering or terrorist financing. However, trusts are vehicles for holding (often personal) assets because they exist to separate legal and beneficial ownership. Under Regulation 33(6)(a)(iii) you must take into account whether 'the customer is a legal person or legal arrangement that is a vehicle for holding personal assets' as a 'customer risk factor' when you are assessing whether there is a high risk of money laundering or terrorist financing in a particular situation which may oblige you to apply EDD measures.

While you must take this factor into account when deciding whether there is a high risk of money laundering and terrorist financing, you should consider the situation as a whole. Factors that may increase the risk of money laundering or terrorist financing when advising a client in relation to a trust are:

- if the client requests a trust to be used when there seems to be little reason to do so,
- the trust is established in a jurisdiction with limited AML/CTF regulation, or
- there are concerns about the client's net wealth or source of funds which will be contributed to the trust, for example, there are public domain allegations that they may potentially harbour the proceeds of crime.

When assessing whether a situation poses a higher risk of money laundering and terrorist financing you must take into account the risk factors set out in Regulation 33(6). However, as Regulation 33(7) makes clear, the presence of one of these risk factors does not in and of itself mean that a particular situation is high risk. If, having considered the risk factors in Regulation 33(6) and any other relevant warning signs, you determine that a higher risk of money laundering or terrorist financing is present, then you must apply EDD measures.

EDD may also apply because your client or one of the trust's other beneficial owners is established in a high risk third country or a PEP. See section 4.12.2.

Applying EDD measures will involve you understanding:

- your client's net wealth and, where they have a funding role, their source of funds,
- the amount and nature of the trust assets and
- the background to the trust and purpose for which the trust was set up.

EDD will also involve your applying increased monitoring.

Specific CDD requirements where you are instructed in relation to an existing trust

Bearing the above in mind, where you are instructed in relation to an existing trust, when applying CDD, you may need:

- to obtain and verify the identity of your client (which as above may be the settlor, trustee(s), protector(s) or beneficiary(ies));
- where you act for more than two trustees (or protectors), only to obtain and verify the identity of two trustees (or protectors);
- where you act for several beneficiaries (subject to conflicts issues), to obtain and verify the identity of each of them, unless you are acting for them as a class (in which case you should identify the class by its name);
- if your client (whether the settlor, trustee(s), protector(s) or beneficiary(ies)) is an entity, in each case to identify its beneficial owner;
- where your client has had a trust funding role, to understand your client's net wealth and the source of funds which were contributed (or which were used to acquire assets which were contributed) to the trust;
- to understand the nature and extent of the assets settled on the trust; and
- to understand and record the identity of the (non-client) settlor, trustee(s), protector(s), and/or beneficiary(ies) and any person who otherwise has control of the trust, as trust beneficial owners.

If the trust is a relevant trust you should also identify potential beneficiaries.

Should further CDD be sought if the identified beneficial owner is an entity?

If the identified beneficial owner is an entity, you will need to understand who its ultimate beneficial owners are, depending on the entity's status (e.g. whether it is a company or a charity).

The extent of the reasonable measures you take to identify the ultimate beneficial owner of one of the trust's defined 'beneficial owners' will depend on its role in relation to the trust. The ultimate beneficial owner of a settlor, protector or sole beneficiary entity should be fully investigated. As a trustee has no beneficial interest in the trust assets, you need not, in the absence of any suspicions, identify the ultimate beneficial owner of a professional trustee entity. It may not be necessary to identify the ultimate beneficial owner of an entity beneficiary where it is one of many discretionary beneficiaries.

Who is a 'beneficiary' for the purposes of CDD where you act in relation to trusts?

Regulation 6(1) implies that individual beneficiaries need not be identified in CDD unless it has been determined that they will benefit from the trust. That is, unless and until they have a vested interest in the capital of the trust.

However, as CDD is a 'snapshot' process, undertaken at commencement of the relevant business relationship, you may wish to note the names of all discretionary beneficiaries (including those who have yet to acquire determined interests) named in the trust deed and any document from the settlor relating to the trust, such as a letter of wishes. This is because their interests may vest (or otherwise be determined) while you are acting in relation to the trust, thus bringing them within the group of individuals who need to be noted in CDD as beneficiaries, as defined in Regulation 6(1)(c).

In any event, if you decide not to note individual beneficiaries named in the trust deed or any associated document on the basis that you have assured yourself that their benefit from the trust has not yet been determined, you should identify any named class of beneficiaries, by its description. For example:

- grandchildren of [X]
- charity [Y].

When considering the identity of those in whose main interest a trust is set up or operates and there are several classes of beneficiary, consider which class is most likely to receive most of the trust property. For example:

- where a trust is for the issue of [X], then the class is the issue of [X] as there is only one class
- where a trust is for the children of [X], if they all die, for the grandchildren of [X] and if they all die for charity [Y], then the class is likely to be the children of [X] as it is unlikely that they will all die before the funds are disbursed
- where a discretionary trust allows for payments to the widow, the children, their spouses and civil partners, the grandchildren and their spouses and civil partners then all interests are equal and all classes will need to be identified.

When in doubt about which class has the main interest, you should identify all classes.

However, where you act in relation to a discretionary trust, if you decide against noting in your CDD the names of individual beneficiaries who are named in the trust deed or any associated document on the basis that their benefitting from the trust has not yet been determined, you will need to seek regular updates from your client, on when and whether beneficiaries' interests in the trust will be or have been determined.

The wider approach, involving noting all beneficiaries and potential beneficiaries named in the trust deed and any associated document at CDD outset, may therefore be preferable.

What does 'an individual who has control over the trust' mean?

Regulation 6(1)(e) brings any individual who has control over the trust within the definition of the beneficial owners of a trust and they will therefore need to be identified when you act in relation to a trust.

Regulation 6(2) defines control as a power, whether exercisable alone, jointly or with the consent of another, under the trust instrument or by law to:

- dispose of, advance, lend, invest, pay or apply trust property;
- vary or terminate the trust;
- add or remove a person as a beneficiary or to or from a class of beneficiaries;
- appoint or remove trustees or give another individual control over the trust;
- direct, withhold consent to or veto the exercise of one of the above powers.

Regulation 6(4)(b) specifically excludes from the definition of an individual who has control over a trust an individual ('P') who has control solely as a result of:

- P's consent being required in accordance with section 32(1)(c)(power of advancement) of the Trustee Act 1925
- any discretion delegated to P under section 34 (power of investment and delegation) of the Pensions Act 1995
- the power to give a direction conferred on P by section 19(2) (appointment and retirement of trustee at instance of beneficiaries) of the Trusts of Land and Appointment of Trustees Act 1996, or
- the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are of full age and capacity and (taken together) absolutely entitled to the property subject to the trust (or, in Scotland, have a full and unqualified right to the fee).

CDD implications arising from the register of beneficial owners of taxable relevant trusts

If you or your practice on occasions acts as (as opposed to for) a trustee of a taxable relevant trust, pursuant to Regulation 44 of the Regulations you will need to maintain accurate and up to date records of all beneficial owners and potential beneficiaries of the trust. Even if your practice is also acting for the trustee(s) and has applied CDD, this may involve you in more extensive and onerous investigations.

A taxable relevant trust is:

- a UK express trust, meaning that either all the trustees are resident in the UK or at least one trustee is UK resident and the settlor was UK resident and domiciled when the trust was set up or when the settlor added funds to it; or
- any other (non UK) express trust which, in any tax year, becomes liable to pay one or more of UK income tax, capital gains tax, inheritance tax, stamp duty land tax, land and buildings transaction tax or stamp duty reserve tax in relation to UK income or assets.

If you form a business relationship in your role as trustee with a relevant person, which could be an advisory relationship with your practice (if it is subject to the Regulations), you will need to inform the relevant person that you are acting as a trustee and on request provide the relevant person with information identifying the trust's beneficial owners and potential beneficiaries.

That obligation lies on (external) trustees of relevant trusts who enter into transactions in relation to which you or your practice are required to apply CDD or who form a business relationship with you or your practice (if you are subject to the Regulations). This should assist you in your compliance with your CDD obligations and is another reason why it makes sense to extend your CDD in relation to a relevant trust's beneficial owners also to cover potential beneficiaries.

Otherwise, from a reputational risk and advisory perspective, as law enforcement authorities may gain access to information not only about the trust's beneficial owners as defined in Regulation 6(1) but also the names of those individuals who are referred to in any document from the settlor, such as a letter of wishes, relating to the trust, it is likely to be prudent to note such wider information in your CDD records where you act for any client in relation to a relevant trust, and, indeed where you act in relation to any trust.

The information which needs to go on the register in relation to each identified individual is extensive and set out in Chapter 5.

Practical considerations

Applying CDD where you act in relation to an existing trust will usually involve your having sight of the trust deed and, as above, any document which relates to it.

Alternatively, you may be able to rely on assurances from the client or another regulated person who has had an involvement with setting up or managing the trust. However, before doing so, you should note and be assured that the reason for your not being provided with the trust deed and any document which relates to it makes sense in all of the circumstances and is not in itself indicative of a high risk of money laundering.

You will also need to assure yourself that in identifying the trust's beneficial owners, the client or other regulated person, as appropriate, had proper regard to whether they included any individual (other than the settlor, the trustees and the beneficiaries) who has control over the trust, and potential beneficiaries.

Foundations

Foundations may or may not have legal personality. You should investigate whether this is the case (e.g. is the relevant structure incorporated?) and thus whether it is appropriate to take on the foundation as your client or whether, as in the case of a trust, your client should be the board of trustees or another party involved with the foundation.

If the foundation lacks legal personality, you should approach CDD, where you act in relation to it, as you would where you act for a client in relation to a trust. Regulation 6(5) provides that 'beneficial owner' in relation to a foundation or other legal arrangement similar to a trust, mean those individuals who hold equivalent or similar positions to the (defined) beneficial owners of trusts.

Charities

Charities may take a number of forms. In the UK, you may come across five types of charities:

- small
- registered
- unregistered
- excepted, such as churches
- exempt, such as museums and universities

For registered charities, you should take a record of their full name, registration number and place of business. Details of registered charities can be obtained from:

- the [Charity Commission of England and Wales](#).
- the [Office of the Scottish Charity Regulator](#).

- the [Charity Commission for Northern Ireland](#).

Other countries may also have charity regulators which maintain a list of registered charities. You may consider it appropriate to refer to these when verifying the identity of an overseas charity.

For all other types of charities you should consider the business structure of the charity and apply the relevant CDD measures for that business structure. You can also generally get confirmation of their charitable status from HMRC. Further, in applying the risk-based approach to charities it is worth considering whether it is a well-known entity or not. The more obscure the charity, the more likely you are to want to view the constitutional documents of the charity.

Due to the increased interest in some charities and not-for-profit organisations from terrorist organisations you may want to also consult [HM Treasury's consolidated list](#) of persons designated as being subject to financial restrictions to ensure the charity is not a designated person.

Deceased persons' estates

When acting for the executor(s) or administrators of an estate, you should establish their identity using the procedures for natural persons or companies set out above. When acting for more than one executor or administrator, it is preferable to verify the identity of at least two of them. You should consider getting copies of the death certificate, grant of probate or letters of administration.

If a will trust is created, and the trustees are different from the executors, the procedures in relation to trusts will need to be followed when the will trust comes into operation.

Churches and places of worship

Places of worship may either register as a charity or can apply for registration as a certified building of worship from the General Register Office (GRO) which will issue a certificate. Further, their charitable tax status will be registered with HMRC. As such, identification details with respect to the church or place of worship may be verified:

- as for a charity
- through the headquarters or regional organisation of the denomination or religion

For UK charities, identification details may be verified:

- with reference to the GRO certificate
- through an enquiry to HMRC

Schools and colleges

Schools and colleges may be a registered charity, a private company, an unincorporated association or a government entity and should be verified in accordance with the relevant category.

The Department of Education maintains [lists of approved educational establishments](#) which may assist in verifying the existence of the school or college.

Clubs and associations

Many of these bear a low money laundering risk, but this depends on the scope of their purposes, activities and geographical spread.

The following information may be relevant to the identity of the club or association:

- full name
- legal status
- purpose
- any registered address
- names of all office holders

Documents which may verify the existence of the club or association include:

- any articles of association or constitution
- statement from a bank, building society or credit union
- recent audited accounts
- financial statements presented to the annual general meeting
- listing in a local or national telephone directory

Pension funds

Regulation 37 provides that simplified due diligence is permitted where there is a low risk of money laundering or terrorist financing, taking account of the risk assessment for that client/matter and the risk factors referred to in Regulation 37(3).

The risk factors include product and service factors including where the product is a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

So you will need evidence that the product is such a scheme and so qualifies for simplified due diligence. Such evidence may include:

- a copy of a page showing the name of the scheme from the most recent definitive deed
- a consolidating deed for the scheme, plus any amending deed subsequent to that date, from which you can assess how contributions are made and member's interest assignment rights.

Pension funds or superannuation schemes outside the above definition should be subject to CDD according to their specific business structure.

For information on how to conduct CDD on other funds please see the JMLSG's Guidance.

Government agencies and councils

The money laundering and terrorist financing risks associated with public authorities vary significantly depending on the nature of the retainer and the home jurisdiction of the public authority. It may be simple to establish that the entity exists, but where there is a heightened risk of corruption or misappropriation of government monies, greater monitoring of retainers should be considered.

The following information may be relevant when establishing a public sector entity's identity:

- full name of the entity
- nature and status of the entity
- address of the entity
- name of the home state authority
- name of the directors or equivalent
- name of the individual instructing you and confirmation of their authority to do so
- extract from official government website

Under Regulation 37(3) the fact that the client is a public administration or publicly owned enterprise is one of the factors to take into account when deciding whether it is low risk and whether to apply simplified due diligence. It will usually be appropriate to apply simplified due diligence to UK public authorities and to some non-UK public authorities, particularly those in the EEA.

4.10 CDD on a beneficial owner

4.10.1 General comments

When conducting CDD on a client, you will need to identify any beneficial owners within the meaning of Regulation 5. Note that the definition of a beneficial owner is broad.

To identify the beneficial owner, obtain at least their name and record any other identifying details which are readily available. You may decide to use records that are publicly available, ask your client for the relevant information or use other sources.

To assess which verification measures are needed, consider the client's risk profile, any business structures involved and the proposed transaction.

The key is to understand the ownership and control structure of the client. A prudent approach is best, monitoring changes in instructions, or transactions which suggest that someone is trying to undertake or manipulate a retainer for criminal ends. Simply ticking boxes will not satisfy the risk-based approach. You must take reasonable

measures to verify the identity of the beneficial owner so you are satisfied that you know who they are.

Appropriate verification measures may include:

- a certificate from your client confirming the identity of the beneficial owner
- a copy of the trust deed, partnership agreement or other such document
- shareholder details from an online registry
- the passport of, or electronic verification on, the individual
- other reliable, publicly available information

It is not enough to rely only on the information contained in a company's register of persons with significant control.

4.10.2 Assessing the risk

An effective risk-based assessment of a particular case may include:

- how well you know your client
- whether your client is a regulated person
- the type of business structure involved in the transaction
- where the business structure is based
- the AML/CTF requirements in the jurisdiction where it is based
- why this business structure is being used in this transaction
- how soon property or funds will be provided to the beneficial owner
- whether/why your client is acting on behalf of someone else

When conducting CDD on beneficial owners within a corporate entity or arrangement, you must:

- understand the ownership and control structure of the client as required by Regulation 5
- identify the specific individuals listed in Regulation 6

The level of understanding required depends on the complexity of the structure and the risks associated with the transaction. For example, it may be sufficient to review the trust deed or partnership arrangement and discuss the issue with your client. In the case of a company, you may obtain a company structure chart from your client directly, their website or their annual reports.

It is vital to understand in what capacity your client is instructing you to ensure that you are identifying the correct beneficial owners.

If for example you are acting for Bank A, which is a corporate entity, to purchase new premises for Bank A, then it would be the shareholders and controllers of Bank A who are the beneficial owners. However, if Bank A is a trustee for XYZ Trust and they have instructed you to sell trust property, then Bank A is instructing you on behalf of the arrangement which is XYZ Trust in their capacity as trustee. The beneficial

owners in that transaction will be those with specified interests in and/or control of the XYZ Trust.

4.10.3 Agency

Regulation 6(9) says a beneficial owner generally means any individual who ultimately owns or controls the client or on whose behalf a transaction is being conducted.

In these cases, it is presumed that the client is himself the beneficial owner, unless the features of the transaction indicate that they are acting on someone else's behalf. So you do not have to proactively search for beneficial owners, but to make enquiries when it appears the client is not the beneficial owner.

Situations where a natural person may be acting on behalf of someone else include:

- exercising a power of attorney. The document granting power of attorney may be sufficient to verify the beneficial owner's identity.
- acting as the deputy, administrator or insolvency practitioner. Appointment documents may be sufficient to verify the beneficial owner's identity.
- acting as an appointed broker or other agent to conduct a transaction. A signed letter of appointment may be sufficient to verify the beneficial owner's identity.

You should be alert to the possibility that purported agency relationships are actually being utilised to facilitate a fraud. Understanding the reason for the agency, rather than simply accepting documentary evidence of such at face value, will assist to mitigate this risk. Where a client or retainer is higher risk, you may want to obtain further verification of the beneficial owner's identity in line with the suggested CDD methods to be applied to natural persons.

4.10.4 Companies

Regulation 5(1) defines the beneficial owner of a body corporate, other than a listed company, as meaning:

any individual who:

- exercises ultimate control over the management of the body corporate
- ultimately owns or controls, directly or indirectly, including through bearer share holdings or other means, more than 25% of the shares or voting rights in the body corporate, or
- otherwise controls the body:
 - by satisfying one or more of the conditions set out in Part 1 of Schedule 1A to the Companies Act 2006 (persons with significant control) or
 - if the individual was an undertaking the body corporate would be a subsidiary undertaking of the individual under section 1162 of the Companies Act 2006 read with Part 7 of that Act.

This Regulation does not apply to a company listed on a regulated market. It does apply to UK limited liability partnerships.

Shareholdings

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant as determined by your risk analysis, verify their identity. These may include:

- getting assurances from the client on the existence and identity of relevant beneficial owners
- getting assurances from other regulated persons more closely involved with the client, particularly in other jurisdictions, on the existence and identity of relevant beneficial owners
- conducting searches on the relevant online registry
- obtaining information from a reputable electronic verification service

You cannot rely solely on the information contained in the company's register of persons with significant control. Where the holder of the requisite level of shareholding of a company is another company, apply the risk-based approach when deciding whether further enquiries should be undertaken.

A proportionate approach

It would be disproportionate to conduct independent searches across multiple entities at multiple layers of a corporate chain to see whether, by accumulating very small interests in different entities, a person finally achieves more than a 25 per cent interest in the client corporate entity. You must simply be satisfied that you have an overall understanding of the ownership and control structure of the client company.

Voting rights are those which are currently exercisable and attributed to the company's issued equity share capital.

Companies with capital in the form of bearer shares

These pose a higher risk of money laundering as it is often difficult to identify beneficial owners and such companies are often incorporated in jurisdictions with lower AML/CTF regulations. You should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and ensure you are notified whenever there is a change of holder and/or beneficial owner. This may be achieved by:

- requiring that the shares be held by a regulated person
- getting an assurance that either such a regulated person or the holder of the shares will notify you of any change of records relating to the shares.

Control

A corporate entity can also be subject to control by persons other than shareholders. Such control may rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms.

You should remain alert to anyone with such powers while you are obtaining a general understanding of the ownership and control structure of the corporate entity. Further enquiries are not likely to be necessary. Monitor situations within the retainer where control structures appear to be bypassed and make further enquiries at that time.

4.10.5 Partnerships

Regulation 5(3) provides that in the case of a partnership (but not a limited liability partnership) the following individuals are beneficial owners:

- any individual ultimately entitled to or who controls, (whether directly or indirectly), more than 25 per cent of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership, or
- any individual who otherwise exercises control over the management of the partnership

Relevant points to consider when applying Regulation 5(3):

- the property of the entity includes its capital and its profits
- control involves the ability to manage the use of funds or transactions outside of the normal management structure and control mechanisms

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant, verify their identity in a risk-based manner.

Enquiries and verification may be undertaken by:

- receiving assurances from the client on the existence and identity of relevant beneficial owners
- receiving assurance from other regulated persons more closely involved with the client, particularly in other jurisdictions, on the existence and identity of relevant beneficial owners
- reviewing the documentation setting up the partnership such as the partnership agreement or any other profit-sharing agreements

4.10.6 Trusts

See section 4.9.4 above.

4.10.7 Other arrangements and legal entities

Regulation 6(7) provides that where you are dealing with a client who is not a natural person, nor a corporate entity or a trust, then the following individuals are beneficial owners:

- any individual who benefits from the property of the entity or arrangement
- where the individuals who benefit from the entity or arrangement have yet to be determined, the class or persons in whose main interest the entity or arrangement is set up or operates

- any individual who exercises control over the property of the entity or arrangement

Unincorporated associations and foundations are examples of entities and arrangements likely to fall within this Regulation.

When applying this Regulation relevant points to consider are:

- the property of the entity includes its capital and its profits
- determined benefits are those to which an individual is currently entitled
- contingent benefits or situations where no determination has been made should be dealt with as a class as benefit has yet to be determined
- a class of persons need only be identified by way of description
- an entity or arrangement is set up for, or operates in, the main interest of the persons who are likely to get most of the property
- control involves the ability to manage the use of funds or transactions outside the normal management structure and control mechanisms
- where you find a body corporate with the requisite interest outlined above, you will need to make further proportionate enquiries as to the beneficial owner of the body corporate

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant, verify their identity in a risk-based manner.

Enquires and verification may be undertaken by:

- asking the client and receiving assurances as to the existence and identity of beneficial owners
- asking other regulated persons more closely involved with the client (particularly in other jurisdictions) and receiving assurances as to the existence and identity of beneficial owners
- reviewing the documentation setting up the entity or arrangement such as its constitution or rules

4.11 Simplified due diligence

Regulation 37 permits simplified due diligence to be undertaken where you determine that the business relationship or transaction presents a low risk of money laundering or terrorist financing taking into account your risk assessment.

4.11.1 What is simplified due diligence?

You have to obtain evidence that the transaction and client or products provided are eligible for simplified due diligence. You will not necessarily need to obtain information on the beneficial owners. You will need to conduct CDD and ongoing monitoring where you suspect money laundering.

4.11.2 Who qualifies for simplified due diligence?

When assessing whether there is a lower risk of money laundering or terrorist financing such that SDD can be applied you must take into account:

- whether the customer is:
 - a public administrator or a publicly owned enterprise
 - an individual resident in a geographical area of lower risk
 - a credit or financial institution which is subject to requirements in national legislation implementing the 4th Directive and supervised for compliance with those requirements in accordance with the 4th Directive
 - a company listed on a regulated market and the location of the regulated market
- product, service, transaction or delivery channel risk factors, including whether the product or service is one of the insurance policies, pensions or electronic money products specified in Regulation 37(3)(b)
- geographical risk factors based on where the client is established and where it does business, for example, an EEA state or third country with effective systems to counter money laundering or terrorist financing or with documented low levels of corruption or other criminal activity.

Financial services firms are not required to apply CDD to the third party beneficial owners of pooled accounts held by legal professionals, provided the information on the identity of the beneficial owners is available upon request and the financial services firm's business relationship with the holder of the pooled account presents a low degree of risk.

For further details on the requirements for qualification for simplified due diligence, see Regulation 37.

4.12 Enhanced due diligence

Regulation 33 provides that you will need to apply enhanced due diligence in addition to the CDD measures required in Regulation 28, on a risk-sensitive basis where:

- the case has been identified as one where there is a high risk of money laundering or terrorist financing in your risk assessment or in the information made available to you by your supervisor under Regulations 17(9) and 47
- the client is a politically exposed person (PEP), or a family member or known close associate of a PEP
- the client or transaction is in a high-risk third country
- the client has provided false or stolen identification documentation or information on establishing the relationship and you have decided to continue dealing with the client
- wherever the transaction:

- is complex and unusually large or there is an unusual pattern of transactions, and
- the transaction or transactions have no apparent economic or legal purpose
- there is any other situation which can present a higher risk of money laundering or terrorist financing

The Regulations specify that you must take measures to examine the background and purpose of the transaction and to increase the monitoring of the business relationship where enhanced due diligence is required.

In applying the risk-based approach to the situation you should consider whether it is appropriate to:

- seek further verification of the client or beneficial owner's identity from independent reliable sources
- obtain more detail on the ownership and control structure and financial situation of the client
- request further information on the purpose of the retainer or the source of the funds, and/or
- conduct enhanced ongoing monitoring

4.12.1 Non face-to-face clients

Where a client is a natural person and they are not physically present for identification purposes, you must take this into account when assessing whether there is a high risk of money laundering or terrorist financing and the extent of any EDD measures you should take.

A client who is not a natural person can never be physically present for identification purposes and will only ever be represented by an agent. Although the fact that you do not have face-to-face meetings with the agents of an entity or arrangement is specified as a risk factor under the Regulations, this does not automatically mean that enhanced due diligence must be undertaken. You should consider your risk analysis, the risks associated with the retainer and the client, assess how well standard CDD measures are meeting those risks and decide whether further CDD measures are required.

Ensuring that the first payment in the retainer is through an account opened in the client's name with a credit institution will further help to verify your client's identity.

If such information is not included on the electronic fund transfer, discuss this with the relevant financial or credit institution. Consider taking up the matter with the FCA if the institution refuses to give you written confirmation of the details. Take other steps to verify your client's identity.

4.12.2 Politically exposed persons

PEPs have been a focus of the FATF as there is concern amongst OECD member states that PEPs have used their political position to corruptly enrich themselves.

You should take a risk-based and proportionate approach to identifying PEPs and then applying EDD measure and treat business with PEPs on a case by case basis. When there is a PEP relationship (which, for the purposes of compliance with the Regulations, also includes where a PEP is a beneficial owner of a client and where a client or its beneficial owner is a family member or known close associate of a PEP), the Regulations specify that you must take the following steps to deal with the heightened risk:

- have senior management approval for establishing a business relationship with a PEP or an entity beneficially owned by a PEP
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction
- conduct closer ongoing monitoring of the business relationship

You are not required to actively investigate whether beneficial owners of a client are PEPs. However, where you have a beneficial owner who you know to be a PEP, you should consider on a risk-based approach what extra measures, if any, you need to take when dealing with that client.

A useful source of further information is the FCA's guidance on [the treatment of politically exposed persons for anti-money laundering purposes](#). The guidance is aimed at firms supervised by the FCA, but you may take it into account in accordance with Regulation 34(4)(b)(i).

4.12.2.1 Who is a PEP?

A person who has been entrusted within the last year (or for a longer period if you consider it appropriate to address the risks in relation to that person) with one of the following prominent public functions by a community institution, an international body, or a state, including the UK:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or similar legislative bodies
- members of governing bodies of political parties
- members of supreme courts, of constitutional courts, or any judicial body whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charges d'affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board of equivalent function of an international organisation

Middle ranking and junior officials are not PEPs. In the UK, only those who hold truly prominent positions should be treated as PEPs and the definition should not be applied to local government, more junior members of the civil service or military officials other than those holding the most senior ranks. Section 2.16 of the FCA

guidance referred to above sets out the FCA's view of what categories of person should be treated as PEPs in the UK.

In addition to the primary PEPs listed above, a PEP also includes:

- family members of a PEP – spouse, civil partner, children, their spouses or partners, and parents
- known close associates of a PEP – persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the primary PEP.

4.12.2.2 How to identify PEPs

You are not required to conduct extensive investigations to establish whether a person is a PEP. Have regard to information that is in your possession or publicly known. Many practices use subscriber services that can run checks against the PEPs databases which they maintain. If your practice regularly encounters PEPs, you should consider a subscription as otherwise it is easy to 'miss' PEPs in your client database including at ultimate beneficial ownership level.

To assess your PEP risk profile, you must take into account your risk assessment carried out under Regulation 18(1), the level of risk of money laundering or terrorist financing inherent in your business and the extent to which that risk would be increased by a business relationship with a PEP.

If the risk of you acquiring a PEP as a client is low, you may simply wish to ask clients whether they fall within any of the PEP categories. Where they say no, you may reasonably assume the individual is not a PEP unless anything else within the retainer, or that you otherwise become aware of, makes you suspect they may be a PEP.

Where you have a higher risk of having PEPs as clients or you have reason to suspect that a person may actually be a PEP contrary to earlier information, you should consider conducting some form of electronic verification. You may find that a web-based search engine will be sufficient for these purposes, or you may decide that it is more appropriate to conduct electronic checks through a reputable international electronic verification provider.

Note: The range of PEPs is wide and constantly changing, so electronic verification will not give you 100 per cent certainty. You should remain alert to situations suggesting the client is a PEP. Such situations include:

- receiving funds in the retainer from a government account
- correspondence on official letterhead from the client or a related person
- general conversation with the client or person related to the retainer linking the person to a PEP
- news reports which come to your attention suggesting your client is actually a PEP or linked to one

Where you suspect a client is a PEP but cannot establish that for certain, you should consider what steps you could take in order to resolve this uncertainty. If you are not able to resolve the issue to your satisfaction, you may consider on a risk-sensitive

basis applying aspects of enhanced due diligence procedures (as a lack of clarity as to whether a person is a PEP could, in and of itself, be indicative of a heightened risk of money laundering).

4.12.2.4 Senior management approval

Regulation 3(1) defines 'senior management' as:

An officer or employee of the relevant person with sufficient knowledge of the relevant person's money laundering and terrorist financing risk exposure, and of sufficient authority to take decisions affecting its risk exposure.

The FCA guidance referred to above sets out their view as to who, for the purposes of the Regulations, should be treated as coming within the definition of senior management.

For independent legal professionals, senior management may be:

- the head of a practice group
- another partner who is not involved with the particular file
- the partner supervising the particular file
- the nominated officer or, if different, the officer responsible for compliance with the Regulations
- the managing partner.

In any case, it is recommended that you advise those responsible for monitoring risk assessment that a business relationship with a PEP has begun, to help their overall monitoring of the practice's risk profile and compliance.

4.12.2.5 Establishing source of wealth and funds

Generally, this simply involves asking questions of the client about their source of wealth and the source of the funds to be used with each retainer. When you know a person is a PEP, their salary and source of wealth is often publicly available on a register of their interests. This may be relevant for higher risk retainers.

The question of evidencing source of wealth should be addressed on a risk sensitive basis. There is no one size fits all answer to this question; certain evidence may be sufficient in some circumstances, though insufficient in others. In cases identified as lower-risk, you should minimise the amount of information relating to source of wealth that you seek to collect directly from clients and make use of information which is readily available. When assessing what evidence will be sufficient to address this issue, those who operate under the 2017 Regulations need to take a global view of the risk factors relevant to the situation and *consideration* of the client's source of wealth should be central to this assessment. Whatever actions are taken or not taken, those actions and the reasons for them should be clearly recorded.

In addition, please note that source of funds is different from source of wealth. Source of funds relates to from where the client's funds are received – a UK bank account for example. Source of wealth relates to how the client came to have the funds in question – via inheritance, house sale, or investment windfall for example. Source of wealth is fundamental to money laundering risk assessment. If you are clear about the

legitimacy of a client's source of wealth, the risk of money laundering is significantly reduced.

4.12.2.6 Enhanced monitoring

You should ensure that funds paid into your client account by your client come from the account nominated and are for an amount commensurate with the client's known wealth. Ask further questions if they are not.

4.12.3 High risk third countries

You must apply EDD measures in any transaction or business relationship with a person established in a 'high risk third country'. However, this requirement does not apply if:

- the customer is a branch or majority owned subsidiary of an entity which is established in an EEA state and subject to the 4th Directive,
- it complies with the group wide policies established by the entity under Article 45 of the 4th Directive, and
- you do not consider EDD measures to be necessary taking a risk-based approach.

Note that not all countries where there may be a higher risk of money laundering are 'high risk third countries'. Under the Regulations a high risk third country is defined as a country which has been identified by the European Commission under Article 9.2 of the 4th Directive. The current list of high risk third countries is contained in [Commission Delegated Regulation \(EU\) 2016/1675](#).

4.12.4 Other situations of higher risk of money laundering or terrorist financing

Enhanced due diligence is also required where there is a higher risk of money laundering or terrorist financing. In determining whether there is a higher risk of money laundering or terrorist financing in a given case you must take into account the risk factors set out in Regulation 33(6). While you must take these risk factors into account, you should consider the situation as a whole. The presence of one or more risk factors does not in and of itself mean that the situation presents a higher risk of money laundering or terrorist financing.

See Chapters 2 and 12 for factors and warning signs you should consider in determining whether a high risk of money laundering is present in a given case.

4.13 Sanctions and other restrictions

Your CDD measures should, following a risk-based approach, be able to ascertain whether your client is subject to the restrictions or directions listed below.

You should also be able to ascertain whether key beneficial owners or the intended recipient of funds from a transaction you are undertaking are subject to the restrictions or directions listed below, where there is a higher risk of money laundering or terrorist financing.

You should assess each case on its merits. However, examples of higher risk situations may include transactions with:

- complex corporate entities in jurisdictions where there is a high risk of terrorist funding
- persons from jurisdictions which are subject to sanctions

The Office of Financial Sanctions Implementation (OFSI) maintains a consolidated list of asset-freeze financial restrictions in force in the UK. One can access this list, register for updates and obtain further information on financial restrictions.

See paragraph 8.10.2 for further information on obtaining a licence from HM Treasury to carry out transactions with persons or entities subject to financial restrictions.

4.13.1 Financial restrictions – general

The UK government imposes financial restrictions on persons and entities following their designation by the United Nations and/or European Union. The UK also operates a domestic counter-terrorism regime, where the government decides to impose financial restrictions on certain persons and entities.

Statutory Instruments are issued for each financial sanctions regime (e.g. DPRK, ISIL/Daesh). An order can be made freezing the assets of a person or entity, where a financial restriction is imposed. It is unlawful to make payments to or allow payments to be made to that designated person or entity.

These persons and entities will be on [HM Treasury's consolidated list](#).

Other financial sanctions provisions, such as investment bans, can be imposed. These provisions are always contained in clauses in the regime-specific Statutory Instruments.

OFSI will always aim to update guidance as soon as possible following a change to the financial sanctions provisions for a regime. Regime specific guidance can be found on <https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>

4.13.2 Restrictions against Al-Qaida and terrorism

The Al Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2009¹ create specific offences for providing funds or economic resources to terrorists.

Persons or entities designated under these orders will be on HM Treasury's consolidated list.

Chapter 5 – Beneficial ownership information

Note: This Chapter may not apply to barristers, BSB entities or advocates who are prohibited from undertaking the management, administration or general conduct of a client's affairs as set out in section 1.1.1.

5.1 Overview

You will need to comply with Part 5 of the Regulations if:

- your practice is a UK body corporate, or
- you (as an individual or an organisation) accept an engagement as a trustee (i.e. as opposed to acting for a trustee) of a relevant trust.

5.2 Obligations on UK body corporates

Under Regulation 42(2)(a) a UK body corporate is defined as 'a body corporate which is incorporated or formed under the laws of the UK or a part of the UK'. This includes but is not limited to:

- listed and unlisted companies
- limited liability partnerships
- Scottish limited partnerships

Under Regulation 43(1), if your practice is a body corporate and it enters into a relevant transaction or forms a business relationship with another person to whom the Regulations apply then you will need to provide that person with the following information on request:

- your name, registered number, registered office and principal place of business;
- your board of directors, or members of your equivalent management body;
- the senior persons responsible for your operations;
- the law to which you are subject;
- your legal owners;
- your beneficial owners; and
- your articles of association or other governing documents.

The obligation to provide this information also applies to your clients who are UK body corporates when they enter relevant transactions or form a business relationship with your firm, which should assist you in your conduct of CDD.

If the identity of individuals or the above information changes during the course of the business relationship then you must notify the other person within 14 days of the date on which you or the relevant body corporate became aware of the change.

5.3 Obligations of trustees

The Regulations impose obligations on trustees of 'relevant trusts' to maintain accurate and up to date written records relating to the trust's beneficial owners and potential beneficiaries and provide certain information about those beneficial owners and potential beneficiaries to relevant persons and law enforcement authorities on request. The trustees must also provide this information to HMRC through the Trust Registration Service (TRS) each tax year in which the trustees incur a liability to UK tax in relation to trust income or assets. The information on the Trust Register will be available to law enforcement agencies in the UK and EEA member states.

A **relevant trust** is a UK express trust or a non-UK express trust which has UK source income or UK assets. A **taxable relevant trust** arises when the trustees of a relevant trust have incurred a liability to UK tax in relation to trust income or assets in a given tax year. The definition of relevant trust is further outlined below.

Where you act (including occasionally) as a trustee of a taxable relevant trust you will need to maintain written records and provide to HMRC annually and to relevant persons with whom you enter into relevant transactions or business relationships and law enforcement authorities on request, the information specified in the Regulations.

5.3.1 Which trusts are caught?

A trust is a UK express trust if all the trustees are resident in the UK or if one or more of the trustees is UK resident and the settlor was resident and domiciled in the UK when the trust was set up or (at any time) when the settlor added funds. A trust is a non-UK express trust if it is not a UK trust and it receives UK source income or has UK assets on which it is liable to pay a UK tax.

A trustee or settlor is resident in the UK if it is a UK body corporate or, if the trustee is an individual, he or she is resident in the UK for the purposes of one or more of the above-mentioned UK taxes.

A taxable relevant trust is a UK express trust or a non-UK express trust which has UK source income or UK assets which the trustees are liable, even if only occasionally, to one or more of the following UK taxes in relation to trust income or assets: Income Tax, Capital Gains Tax, Inheritance Tax, Stamp Duty Land Tax, Land and Buildings Transaction Tax or Stamp Duty Reserve Tax. Bare trusts (a trust in which the beneficiary has an absolute right to the capital and assets within the trust and income thereby generated) and implied trusts (a trust which arises by operation of law, so a resulting trust or a constructive trust) are not relevant trusts and are therefore not subject to Part 5 of the Regulations.

5.3.2 Which beneficial owners do the trustees need to note and record?

The trustees of a relevant trust are obliged to maintain accurate and up to date written records of all the trust's beneficial owners, who will include its:

- settlor;
- trustees;
- actual or potential beneficiaries;

- any other individual who has control over the trust which may include a protector or protectors; and
- any other potential individual (note, not entity) beneficiaries referred to in a document from the settlor, such as a letter of wishes, relating to the trust.

The concept of individuals who have 'control' over the trust is defined in Regulation 6(2) and encompasses individuals who have a power (exercisable alone or jointly) under the trust instrument or by law to:

- dispose of, advance, lend, invest, pay or apply trust property;
- vary or terminate the trust;
- add or remove a person as a beneficiary or to or from a class of beneficiaries;
- appoint or remove trustees or give another individual control over the trust; or
- direct, withhold consent to or veto the exercise of a power mentioned in subparagraph 5.3.1 to 5.3.7 above.

5.3.3 What information must the trustees maintain in relation to each beneficial owner, potential beneficiary and the trust itself?

Where the beneficial owner or potential beneficiary is an individual (but note, not where a class), the trustees need to note and record:

- the individual's full name;
- the individual's national insurance number or unique taxpayer reference, if any
- if the individual does not have a national insurance number or unique taxpayer reference, the individual's usual residential address, and if that address is not in the UK, the individual's passport number or identification card number, with the country of issue and the expiry date of the passport or identification card; or if the individual does not have a passport or identification card, the number, country of issue and expiry date of any equivalent form of identification;
- the individual's date of birth; and
- the nature of the individual's role in relation to the trust.

Where the beneficial owner is a corporate body, the trustees need to note and record:

- the legal entity's corporate or firm name;
- the legal entity's unique taxpayer reference, if any;
- the registered or principal office of the legal entity;
- the legal form of the legal entity and the law by which it is governed;
- if applicable, the register of companies in which the legal entity is entered (including details of the EEA state or third country in which it is registered), and its registration number in that register; and
- the nature of the entity's role in relation to the trust.

The trustees are also obliged to note and record the following information in relation to the trust:

- the name of the trust;
- the date on which the trust was set up;
- a statement of accounts for the trust, describing the trust assets and identifying the value of each category of the trust assets at the date on which the information is first provided to HMRC (including the address of any property held by the trust);
- the country where the trust is considered to be resident for tax purposes;
- the place where the trust is administered;
- a contact address for the trust; and
- the name of any advisers who are being paid to provide legal, financial, tax or other advice to the trustees in relation to the register requirements.

The details of trust assets have to be based on market value at the date on which the asset(s) was placed in the trust by the settlor, when the settlement was first created. To keep administrative burdens on trustees to a minimum HMRC are not expecting any formal valuation but as was done with the previous 41G form, HMRC would expect trustees to provide a good estimate of the market value of the assets. If trustees are registering a trust where the value of assets were notified to HMRC previously through either a 41G form or SA900 tax returns then trustees should just complete the "Other Asset" field using the term – "Already notified", leaving all other asset fields marked as "£1". The details of trust assets have to be provided only once at the first point of registration.

5.3.4 When does the information need to be obtained and updated?

The obligation on trustees to maintain the written records outlined above came into effect when the Regulations came into force (26 June 2017).

The information must be provided to HMRC on or before 31 January 2018 or the next 31 January which falls after the end of the tax year in which the trustees were first liable to pay any of the above specified UK taxes. If they provide information prior to 31 January and they become aware it has changed (save if going to value of the trust assets) they must notify HMRC of the change and the date on which it occurred prior to 31 January after the end of the tax year in which the trustees are liable to pay any of the specified UK taxes.

Information provided in relation to beneficial owners should be current at the date the register is updated and not as at the tax year which triggered the registration. There are certain obligations on trustees in the Regulations to provide third parties with the records, and update third parties of a change to the records, which they hold on beneficial owners and potential beneficial owners, within 14 days.

5.3.5 Associated obligation on the trustees to provide information to a relevant person

Where a trustee of a relevant trust is acting as a trustee and enters into a transaction or forms a business relationship with a relevant person to whom the Regulations

apply they must inform that relevant person they are acting as trustee. They must also provide that relevant person with information identifying the beneficial owners of the trust and any other person named in a letter of wishes on request.

Regulation 44(3) imposes an obligation on the trustees to notify the relevant person of any change in the identity of the beneficial owners and potential beneficiaries (including persons named in letters of wishes, which may be revised informally and frequently) within 14 days of the date on which any one of the trustees became aware of the relevant change.

5.3.6 Obligation on trustees to provide records to any law enforcement authority

Aside from the obligation to provide HMRC with information on the 31 January following the end of each tax year, the trustees of a relevant trust are also obliged by Regulation 44(5) to provide information about the beneficial owners and potential beneficiaries of the trust which they have recorded, directly and 'on request' to any law enforcement authority in compliance with the deadline set by the law enforcement authority (listed in Regulation 44(10)). The trustees of a relevant trust could be approached by law enforcement at any point after the Regulations have come into effect (from 26 June 2017)

5.3.7 How long do the records need to be maintained?

Where the trustees are professional trustees (i.e. being paid to act as trustees), which is likely to be the case if you or your practice is acting as a trustee, they must retain the records referred to above for a period of five years after the date on which the final distribution is made under the trust.

They must then delete them unless 'the person to whom information in a record relates', so each named beneficial owner and potential beneficiary in the relevant records, consents to longer retention or where longer retention is required by an enactment or for the purposes of court proceedings.

This may result in your practice having one retention period for its CDD records, including where it acts in relation to a trust for trustees, and a different retention period for records which it is required to hold when it acts as a trustee.

5.3.8 What information do trustees need to provide to HMRC for the register and when?

The trustees of a taxable relevant trust need to provide all the information which they are obliged to record on the trust and its beneficial owners and potential beneficiaries as set out above to HMRC.

We understand that HMRC are expecting trustees of a taxable relevant trust (or an agent acting on behalf of the trustees) to submit the first set of information on or before 31 January 2018. However, as above, trustees could find themselves on the receiving end of a request for information from a relevant person or UK law enforcement authority at any time after commencement of the Regulations (from 26 June 2017) meaning that it would be prudent for trustees to attend to collation of relevant written records promptly.

Trustees should note that the register reporting obligation only arises if the trustees incurred a liability to pay any of the specified UK taxes in relation to trust income or assets in the preceding tax year. So, a trustee of a non-UK trust which only generates a UK tax liability in the form of a ten-yearly inheritance tax charge need only report to HMRC on or before the 31 January which falls after the tax year in which the inheritance tax charge falls due (in each case).

Trustees that submit the trust tax return will be asked to confirm in Q20 of the return whether they have registered or updated the details of their trust on the TRS.

5.3.9 How will relevant information be provided to HMRC?

The TRS will be an online register and therefore trustees will need to submit information about their taxable relevant trust online. For further information on how to register a trust on the TRS trustees should visit www.gov.uk.

Trustees will also be obliged to make a 'no change' declaration to HMRC annually on or before the 31 January which falls after any tax year in which the trustees are liable to pay any of the above mentioned UK taxes if there has been no change to the information provided to HMRC.

5.3.10 With whom can HMRC share the information on the register?

HMRC is obliged to share the trust data with any UK law enforcement authority. The following organisations are listed as UK law enforcement authorities in the Regulations:

- Financial Conduct Authority (FCA);
- National Crime Agency (NCA);
- the police forces maintained under section 2 of the Police Act 1996(a);
- the Police of the Metropolis and for the City of London;
- the Police Services of Scotland and Northern Ireland; and
- the Serious Fraud Office (SFO).

It is also obliged to ensure the NCA can use information on the register to respond promptly to a request made by a similar authority or financial intelligence unit in another EEA state.

Chapter 6 – Money laundering offences

6.1 General comments

The Proceeds of Crime Act 2002 (POCA) created a single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. It also creates a disclosure regime, which makes it an offence not to disclose knowledge or suspicion of money laundering, but also permits persons to be given consent in certain circumstances to carry out activities which would otherwise constitute money laundering.

6.2 Application

POCA applies to all legal professionals, although some offences apply only to persons within the regulated sector, or nominated officers.

6.3 Mental elements

The mental elements which are relevant to offences under Part 7 of POCA are:

- knowledge
- suspicion
- reasonable grounds for suspicion

These are the three mental elements in the actual offences, although the third one only applies to offences relating to the regulated sector. There is also the element of belief on reasonable grounds in the foreign conduct defence to the money laundering offences. A person will have a defence to a principal offence if they know or believe on reasonable grounds that the criminal conduct involved was exempt overseas criminal conduct.

For the principal offences of money laundering the prosecution must prove that the property involved is criminal property. This means that the prosecution must prove that the property was obtained through criminal conduct and that, at the time of the alleged offence, you knew or suspected that it was.

For the failure to disclose offences, where you are acting in the regulated sector, you must disclose if you have knowledge, suspicion or reasonable grounds for suspicion; while if you are not in the regulated sector you will only need to consider making a disclosure if you have actual, subjective knowledge or suspicion.

These terms for the mental elements in the offences are not terms of art; they are not defined within POCA and should be given their everyday meaning. However, case law has provided some guidance on how they should be interpreted.

6.3.1 Knowledge

Knowledge means actual knowledge. There is some suggestion that willfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice.

6.3.2 Suspicion

The term 'suspects' is one which the court has historically avoided defining; however, because of its importance in English criminal law, some general guidance has been given. In the case of *R v Da Silva [2007] 1 WLR 303*, which was prosecuted under previous money laundering legislation, Longmore LJ stated:

'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'

There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

The test for whether you hold a suspicion is a subjective one.

If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion.

Chapter 12 of this guidance contains a number of standard warning signs which may give you a cause for concern; however, whether you have a suspicion is a matter for your own judgment. To help form that judgment, consider talking through the issues with colleagues or contacting your supervisor. Listing causes for concern can also help focus your mind.

If you have not yet formed a suspicion but simply have cause for concern, you may choose to ask the client or others more questions. This choice depends on what you already know, and how easy it is to make enquiries.

If you think your own client is innocent but suspect that another party to a transaction is engaged in money laundering, you may still have to consider referring your client for specialist advice regarding the risk that they may be a party to one of the principal offences.

6.3.3 Reasonable grounds to suspect

The issues here for the legal professional conducting regulated activities are the same as for the mental element of suspicion, except that it is an objective test. Were there factual circumstances from which an honest and reasonable person, engaged in a business in the regulated sector should have inferred knowledge or formed the suspicion that another was engaged in money laundering?

6.4 Principal money laundering offences

6.4.1 General comments

Money laundering offences assume that a criminal offence has occurred in order to generate the criminal property which is now being laundered. This is often known as a

predicate offence. No conviction for the predicate offence is necessary for a person to be prosecuted for a money laundering offence.

The principal money laundering offences apply to money laundering activity which occurred on or after 24 February 2003 as a result of the Proceeds of Crime Act 2002 (Commencement No. 4, Transitional Provisions & Savings) Order 2003.

If the money laundering occurred or started before 24 February 2003, the former legislation will apply.

However, if the money laundering took place after 24 February 2003, the conduct giving rise to the criminal property can occur before that date.

When considering the principal money laundering offences, be aware that it is also an offence to conspire or attempt to launder the proceeds of crime, or to counsel, aid, abet or procure money laundering.

6.4.2 Section 327 – concealing

A person commits an offence if he or she conceals, disguises, converts, or transfers criminal property, or removes criminal property from England and Wales, Scotland or Northern Ireland.

Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it.

6.4.3 Section 328 - arrangements

A person commits an offence if he or she enters into, or becomes concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

What is an arrangement?

Arrangement is not defined in Part 7 of POCA. The arrangement must exist and have practical effects relating to the acquisition, retention, use or control of property.

An agreement to make an arrangement will not always be an arrangement. The test is whether the arrangement does in fact, in the present and not the future, have the effect of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.

What is not an arrangement?

Bowman v Fels [2005] EWCA Civ 226 held that section 328 does not cover or affect the ordinary conduct of litigation by legal professionals, including any step taken in litigation from the issue of proceedings and the securing of injunctive relief or a freezing order up to its final disposal by judgment.

Our view, supported by Counsel's opinion, is that dividing assets in accordance with the judgment, including the handling of the assets which are criminal property, is not an arrangement. Further, settlements, negotiations, out of court settlements, alternative dispute resolution and tribunal representation are not arrangements.

However, the property will generally still remain criminal property and you may need to consider referring your client for specialist advice regarding possible offences they may commit once they come into possession of the property after completion of the settlement.

The recovery of property by a victim of an acquisitive offence will not be committing an offence under either section 328 or section 329 of the Act.

Sham litigation

Sham litigation created for the purposes of money laundering remains within the ambit of section 328. Our view is that shams arise where an acquisitive criminal offence is committed and settlement negotiations or litigation are intentionally fabricated to launder the proceeds of that separate crime.

A sham can also arise if a whole claim or category of loss is fabricated to launder the criminal property. In this case, money laundering for the purposes of POCA cannot occur until after execution of the judgment or completion of the settlement.

Entering into or becoming concerned in an arrangement

To enter into an arrangement is to become a party to it.

To become concerned in an arrangement suggests a wider practical involvement such as taking steps to put the arrangement into effect.

Both entering into, and becoming concerned in, describe an act that is the starting point of an involvement in an existing arrangement.

Although the Court did not directly consider the conduct of transactional work, its approach to what constitutes an arrangement under section 328 provides some assistance in interpreting how that section applies in those circumstances.

Our view is that *Bowman v Fels* supports a restricted understanding of the concept of entering into or becoming concerned in an arrangement, with respect to transactional work. In particular:

- entering into or becoming concerned in an arrangement involves an act done at a particular time
- an offence is only committed once the arrangement is actually made, and
- preparatory or intermediate steps in transactional work which does not itself involve the acquisition, retention, use or control of property will not constitute the making of an arrangement under section 328

If you are doing transactional work and become suspicious, you have to consider:

- whether an arrangement exists and, if so, whether you have entered into or become concerned in it or may do so in the future
- if no arrangement exists, whether one may come into existence in the future which you may become concerned in.

6.4.4 Section 329 - acquisition, use or possession

A person commits an offence if he or she acquires, uses or has possession of criminal property.

6.5 Defences to principal money laundering offences

You will have a defence to a principal money laundering offence if:

- you make an authorised disclosure prior to the offence being committed and you gain appropriate consent/DAML (the consent defence)
- you intended to make an authorised disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence)

In relation to section 329 you will also have a defence if you received adequate consideration for the criminal property (the adequate consideration defence).

6.5.1 Authorised disclosures

Section 338 authorises you to make a disclosure regarding suspicion of money laundering as a defence to the principal money laundering offences.

It specifically provides that you can make an authorised disclosure either

- before money laundering has occurred
- while it is occurring but as soon as you suspect
- after it has occurred, if you had good reason for not disclosing earlier and make the disclosure as soon as practicable

If a disclosure is authorised, it does not breach any rule which would otherwise restrict it, including professional regulatory requirements relating to confidentiality.

Where your practice has a nominated officer, you should make your disclosure to the nominated officer. The nominated officer will consider your disclosure and decide whether to make an external disclosure to the NCA. If your practice does not have a nominated officer, you should make your disclosure directly to the NCA.

Appropriate consent/DAML

If you have a suspicion that a retainer you are acting in will involve dealing with criminal property, you can make an authorised disclosure to the NCA via your nominated officer and seek consent/DAML to undertake the further steps in the retainer which would constitute a money laundering offence.

For further information on how to make an authorised disclosure to the NCA and the process by which consent/DAML is gained, see Chapter 9 of this guidance.

Reasonable excuse defence

This defence applies where a person intended to make an authorised disclosure before doing a prohibited act, but had a reasonable excuse for not disclosing.

Reasonable excuse has not been defined by the courts, but the scope of the reasonable excuse defence is important for legal professional privilege.

You will have a defence against a principal money laundering offence if you make an authorised disclosure.

However, you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception. It is the Legal Sector Affinity Group's view that you will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

There may be other circumstances which would provide a reasonable excuse. For example:

- if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already aware of the suspected criminal conduct or money laundering and the reporter does not have any additional information which might assist the regulator or enforcement authority, or
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 330 is information entirely within the public domain, or
- if all the suspected predicate offending occurs outside the UK and all the suspected money laundering occurs outside the UK and there is otherwise no UK nexus to the suspected criminality.

This is not intended to be an exhaustive list. Moreover, reporters should be aware that it will ultimately be for a court to decide if a reporters' excuse for not making an authorised disclosure report under section 330 was a reasonable excuse. Reporters should clearly document their reasons for concluding that they have a reasonable excuse in any given case and, if in doubt, may wish to seek independent legal advice.

Where you suspect part way through

It is not unusual for a transactional matter to seem legitimate early in the retainer, but to develop in such a way as to arouse suspicion later on. It may be that certain steps have already taken place which you now suspect facilitated money laundering; while further steps are yet to be taken which you also suspect will facilitate further money laundering.

Section 338(2A) provides that you may make an authorised disclosure in these circumstances if:

- at the time the initial steps were taken they were not a money laundering offence because you did not have good reason to know or suspect that the property was criminal property; and
- you make a disclosure of your own initiative as soon as practicable after you first know or suspect that criminal property is involved in the retainer.

In such a case you would make a disclosure seeking consent/DAML for the rest of the transaction to proceed, while fully documenting the reasons why you came to know or suspect that criminal property was involved and why you did not suspect this to be the case previously.

6.5.2 Adequate consideration defence

This defence applies if there was adequate consideration for acquiring, using and possessing the criminal property, unless you know or suspect that those goods or services may help another to carry out criminal conduct.

The Crown Prosecution Service guidance for prosecutors says the defence applies where professional advisors, such as legal professionals or accountants, receive money for or on account of costs, whether from the client or from another person on the client's behalf. Disbursements are also covered. The fees charged must be reasonable, and the defence is not available if the value of the work is significantly less than the money received.

The transfer of funds from client to office account, or vice versa, is covered by the defence.

Returning the balance of an account to a client may be a money laundering offence if you know or suspect the money is criminal property. In that case, you must make an authorised disclosure and obtain consent/DAML to deal with the money before you transfer it.

Reaching a matrimonial settlement or an agreement on a retiring partner's interest in a business does not constitute adequate consideration for receipt of criminal property, as in both cases the parties would only be entitled to a share of the legitimately acquired assets of the marriage or the business. This is particularly important where your client would be receiving the property as part of a settlement which would be exempted from section 328 due to the case of *Bowman v Fels*.

The defence is more likely to cover situations where:

- a third party seeks to enforce an arm's length debt and, unknown to them, is given criminal property in payment for that debt;
- a person provides goods or services as part of a legitimate arm's length transaction but unknown to them is paid from a bank account which contains the proceeds of crime.

6.6 Failure to disclose offences – money laundering

6.6.1 General comments

The failure to disclose provisions in sections 330, 331 and 332 apply where the information on which the knowledge or suspicion is based came to a person on or after 24 February 2003, or where a person in the regulated sector has reasonable grounds for knowledge or suspicion on or after that date.

If the information came to a person before 24 February 2003, the old law applies.

In all three sections, the phrase 'knows or suspects' refers to actual knowledge or suspicion - a subjective test. However, legal professionals and nominated officers in the regulated sector will also commit an offence if they fail to report when they have reasonable grounds for knowledge or suspicion - an objective test. On this basis, they may be guilty of the offence under sections 330 or 331 if they should have known or suspected money laundering.

For all failure to disclose offences you must either:

- know the identity of the money launderer or the whereabouts of the laundered property, or
- believe the information on which your suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property

6.6.2 Section 330 – failure to disclose: regulated sector

A person commits an offence if

- he or she knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, and
- the information on which his suspicion is based comes in the course of business in the regulated sector, and
- he or she fails to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a nominated officer or the NCA.

Making a required notification or being party to a joint disclosure report will both be treated as satisfying any requirement to disclose once section 339ZD is in force.

Our view is that delays in disclosure arising from taking legal advice or seeking help may be acceptable provided you act promptly to seek advice.

6.6.3 Section 331 – failure to disclose: nominated officer in the regulated sector

A nominated officer in the regulated sector commits a separate offence if, as a result of an internal disclosure under section 330, he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering and he fails to disclose as soon as practicable to the NCA.

6.6.4 Section 332 – failure to disclose: nominated officer in the non-regulated sector

An organisation which does not carry out relevant activities and so is not in the regulated sector, may decide on a risk-based approach to set up internal disclosure systems and appoint a person as nominated officer to receive internal disclosures.

A nominated officer in the non-regulated sector commits an offence if, as a result of a disclosure, he knows or suspects that another person is engaged in money laundering and fails to make a disclosure as soon as practicable to the NCA.

For this offence, the test is a subjective one: did you know or suspect in fact?

6.7 Exceptions to failure to disclose offences

There are three situations in which you have not committed an offence for failing to disclose:

- you have a reasonable excuse;
- you are a professional legal adviser or a relevant professional adviser and the information came to you in privileged circumstances;

- you did not receive appropriate training from your employer.

The first defence is the only one which applies to all three failure to disclose offences; the other two defences are only specifically provided for persons in the regulated sector who are not nominated officers.

All of the failure to disclose sections also reiterate that the offence will not be committed if the property involved in the suspected money laundering is derived from exempted overseas criminal conduct.

6.7.1 Reasonable excuse

No offence is committed if there is a reasonable excuse for not making a disclosure, but there is no judicial guidance on what might constitute a reasonable excuse.

However, you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception. It is the Legal Sector Affinity Group's view that you will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

There may be other circumstances which would provide a reasonable excuse. For example:

- if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already aware of the suspected criminal conduct or money laundering and the reporter does not have any additional information which might assist the regulator or enforcement authority, or
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 330 is information entirely within the public domain, or
- if all the suspected predicate offending occurs outside the UK and all the suspected money laundering occurs outside the UK and there is otherwise no UK nexus to the suspected criminality.

This is not intended to be an exhaustive list. Moreover, reporters should be aware that it will ultimately be for a court to decide if a reporter's excuse for not making an authorised disclosure report under section 330 was a reasonable excuse. Reporters should clearly document their reasons for concluding that they have a reasonable excuse in any given case and, if in doubt, may wish to seek independent legal advice.

6.7.2 Privileged circumstances

No offence is committed if the information or other matter giving rise to suspicion comes to a professional legal adviser or relevant professional advisor in privileged circumstances.

You should note that receipt of information in privileged circumstances is not the same as legal professional privilege. It is a creation of POCA designed to comply with the exemptions from reporting set out in the European directives.

Privileged circumstances means information communicated:

- by a client, or a representative of a client, in connection with the giving of legal advice to the client, or
- by a client, or by a representative of a client, seeking legal advice from you; or
- by a person in connection with legal proceedings or contemplated legal proceedings.

The exemption will not apply if information is communicated or given to the legal professional with the intention of furthering a criminal purpose.

[The Crown Prosecution Service guidance](#) for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances exemption applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence.

For a further discussion of privileged circumstances see Chapter 7.

6.7.3 Lack of training

Employees within the regulated sector who have no knowledge or suspicion of money laundering, even though there were reasonable grounds for suspicion, have a defence if they have not received training from their employers. Employers may be prosecuted for a breach of the Regulations if they fail to train staff.

6.8 Tipping off

The offences of tipping off for money laundering are contained in POCA as amended by the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (TACT and POCA Regulations 2007).

There are also tipping off offences for terrorist property in the Terrorism Act, as amended by the TACT and POCA Regulations 2007.

6.8.1 Offences

6.8.1.1 Tipping off – in the regulated sector

There are two tipping off offences in section 333A of POCA. They apply only to business in the regulated sector.

Section 333A(1) – disclosing a suspicious activity report (SAR)

It is an offence to disclose to a third person that a SAR has been made by any person to the police, HM Revenue and Customs, the NCA or a nominated officer, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR. This offence can only be committed:

- *after* a disclosure to the NCA
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR

- the information upon which the disclosure is based came to you in the course of business in the regulated sector.

Section 333A(3) – disclosing an investigation

It is an offence to disclose the fact that an investigation into a money laundering offence is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector. The key point is that you can commit this offence, even when you are unaware that a SAR was submitted.

6.8.1.2 Prejudicing an investigation

Section 342(1) contains an offence to prejudice a confiscation, civil recovery or money laundering investigation, if the person making the disclosure knows or suspects that an investigation is being, or is about to be conducted. Section 342(1) was amended by paragraph 8 of the TACT and POCA Regulations 2007. It applies to those outside the regulated sector as well as those within the regulated sector.

You only commit this offence if you knew or suspected that the disclosure would, or would be likely to, prejudice any investigation.

6.8.2 Defences

6.8.2.1 Tipping off

The following disclosures are permitted:

- Section 333B - disclosures within an undertaking or group, including disclosures to a professional legal adviser or relevant professional adviser;
- Section 333C - disclosures between institutions, including disclosures from a professional legal adviser to another professional legal adviser;
- Section 333D - disclosures to your supervisory authority;
- Section 333D(2) - disclosures made by professional legal advisers to their clients for the purpose of dissuading them from engaging in criminal conduct.

A person does not commit the main tipping off offence if he does not know or suspect that a disclosure is likely to prejudice an investigation.

Section 333B – disclosures within an undertaking or group etc

It is not an offence if an employee, officer or partner of a practice discloses that a SAR has been made if it is to an employee, officer or partner of the same undertaking.

A legal professional will not commit a tipping off offence if:

- the disclosure is to a professional legal adviser or a relevant professional adviser,

- both the person making the disclosure and the person to whom it is made carry on business in an EEA state or in a country or territory imposing equivalent money laundering requirements, and
- those persons perform their professional activities within different undertakings that share common ownership, management or control.

Section 333C – disclosures between institutions etc

A legal professional will not commit a tipping off offence if *all* the following criteria are met:

- The disclosure is made to another legal professional in an EEA state, or one with an equivalent AML regime;
- The disclosure relates to a client or former client of both parties, or a transaction involving them both, or the provision of a service involving them both;
- The disclosure is made for the purpose of preventing a money laundering offence; and
- Both parties have equivalent professional duties of confidentiality and protection of personal data.

Section 333D(2) – limited exception for professional legal advisers

A legal professional will not commit a tipping off offence if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence. This exception and the tipping off offence in section 333A apply to those carrying on activities in the regulated sector.

6.8.2.2 Prejudicing an investigation

Section 342(4) – professional legal adviser exemption

It is a defence to a section 342(1) offence that a disclosure is made by a legal adviser to a client, or a client's representative, in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.

Such a disclosure will not be exempt if it is made with the intention of furthering a criminal purpose (section 342(5)).

6.8.3 Making enquiries of a client

You should make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

There is nothing in POCA which prevents you making normal enquiries about your client's instructions, and the proposed retainer, in order to remove any concerns and enable the practice to decide whether to take on or continue the retainer.

These enquiries will only be tipping off if you disclose that a SAR has been made or that a money laundering investigation is being carried out or contemplated. The offence of tipping off only applies to the regulated sector.

It is not tipping-off to include a paragraph about your obligations under the money laundering legislation in your practice's standard client care letter.

Chapter 7 – Legal professional privilege

7.1 General comments

Legal professionals are under a duty to keep the affairs of their clients confidential, and the circumstances in which they are able to disclose client communications are strictly limited.

However, sections 327 - 329, 330 and 332 of POCA contain provisions for disclosure of information to be made to the NCA. Sections 339ZB-G [not yet in force] contain further provisions for disclosure of confidential information to both the NCA and to other persons carrying on business in the regulated sector.

Legal professionals also have a duty of full disclosure to their clients. However, sections 333A and 342 of POCA prohibit disclosure of information in circumstances where a SAR has been made and/or where it would prejudice an existing or proposed investigation.

This chapter examines the tension between a legal professional's duties and these provisions of POCA. Similar tensions also arise with respect to the Terrorism Act.

This chapter should be read in conjunction with Chapter 6 of this guidance and if you are still in doubt as to your position, you should seek independent legal advice.

7.2 Application

This chapter is relevant to any legal professional considering whether to make a disclosure under POCA.

7.3 Duty of confidentiality

A legal professional is professionally and legally obliged to keep the affairs of clients confidential and to ensure that his staff do likewise. The obligations extend to all matters revealed to a legal professional, from whatever source, by a client, or someone acting on the client's behalf.

In exceptional circumstances this general obligation of confidence may be overridden. However, certain communications can never be disclosed unless statute permits this either expressly or by necessary implication. Such communications are those protected by legal professional privilege (LPP).

7.4 Legal professional privilege

7.4.1 General overview

LPP is a privilege against disclosure, ensuring clients know that certain documents and information provided to legal professionals cannot be disclosed at all. It recognises the client's fundamental human right to be candid with his legal adviser, without fear of later disclosure to his prejudice. It is an absolute right and cannot be overridden by any other interest.

LPP does not extend to everything that legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

The extent to which LPP attaches to a notary's records has not been the subject of a legal decision in England and Wales and is an evolving area of law. Notaries should therefore consider seeking specific legal advice based on the particular circumstances of a given situation if it appears LPP may apply.

7.4.2 Advice privilege

Principle

Communications between a legal professional, acting in his capacity as a legal professional, and a client, are privileged if they are both:

- confidential; and
- for the purpose of seeking legal advice from a legal professional or providing it to a client.

Scope

Communications are not privileged merely because a client is speaking or writing to you. The protection applies only to those communications which directly seek or provide advice or which are given in a legal context, that involve the legal professional using his legal skills and which are directly related to the performance of the legal professional's professional duties [*Passmore on Privilege 2nd edition 2006*].

Case law helps define what advice privilege covers.

Communications subject to advice privilege:

- a solicitor's bill of costs and statement of account [*Chant v Brown (1852) 9 Hare 790*]
- information imparted by prospective clients in advance of a retainer if the communications were made for the purpose of indicating the advice required [*Minster v Priest [1930] AC 558 per Lord Atkin at 584*].

Communications not subject to advice privilege:

- notes of open court proceedings [*Parry v News Group Newspapers (1990) 140 New Law Journal 1719*], as the content of the communication is not confidential;
- conversations, correspondence or meetings with opposing legal professionals [*Parry v News Group Newspapers (1990) 140 New Law Journal 1719*], as the content of the communication is not confidential;
- a client account ledger maintained in relation to the client's money [*Nationwide Building Society v Various Solicitors [1999]P.N.L.R. 53*];
- an appointments diary or time record on an attendance note, time sheet or fee record relating to a client [*R v Manchester Crown Court, ex p. Rogers [1999] 1 W.L.R. 832*];

- conveyancing documents, as they are not communications [*R v Inner London Crown Court ex p. Baines & Baines* [1988] QB 579].

Advice within a transaction

All communications between a legal professional and his or her client relating to a transaction in which the legal professional has been instructed for the purpose of obtaining legal advice are covered by advice privilege, notwithstanding that they do not contain advice on matters of law and construction, provided that they are directly related to the performance by the legal professional of his professional duty as legal adviser of his or her client. [*Three Rivers District Council and others v the Bank of England* [2004] UKHL 48 at 111]

This will mean that where you are providing legal advice in a transactional matter (such as a conveyance) the advice privilege will cover all:

- communications with,
- instructions from, and
- advice given to

the client, including any working papers and drafts prepared, as long as they are directly related to your performance of your professional duties as a legal adviser.

7.4.3 Litigation privilege

Principle

This privilege, which is wider than advice privilege, protects confidential communications made after litigation has started, or is reasonably in prospect, between any of the following:

- a legal professional and a client;
- a legal professional and an agent, whether or not that agent is a legal professional; or
- a legal professional and a third party.

These communications must be for the sole or dominant purpose of litigation, for any of the following:

- for seeking or giving advice in relation to it;
- for obtaining evidence to be used in it; or
- for obtaining information leading to obtaining such evidence

7.4.4 Important points to consider

An original document not brought into existence for these privileged purposes and so not already privileged, does not become privileged merely by being given to a legal professional for advice or other privileged purpose.

Further, where you have a corporate client, communication between you and the employees of a corporate client may not be protected by LPP if the employee cannot be considered to be 'the client' for the purposes of the retainer. As such, some employees will be clients, while others will not. [*Three Rivers District Council v the Governor and Company of the Bank of England (no 5)* [2003] QB 1556]

It is not a breach of LPP to discuss a matter with your nominated officer for the purposes of receiving advice on whether to make a disclosure.

7.4.5 Crime/fraud exception

LPP protects advice you give to a client on avoiding committing a crime [*Bullivant v Att-Gen of Victoria* [1901]AC 196] or warning them that proposed actions could attract prosecution [*Butler v Board of Trade* [1971] Ch 680]. LPP does not extend to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence [*R v Cox & Railton* (1884) 14 QBD 153]. It is irrelevant whether or not you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia* [1986] 1 Lloyd's Rep 336].

Intention of furthering a criminal purpose

It is not just your client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the legal professional/client communication to be made with that purpose (e.g. where the innocent client is being used by a third party) [*R v Central Criminal Court ex p Francis & Francis* [1989] 1 AC 346].

Knowing a transaction constitutes an offence

If you know the transaction you're working on is a principal offence, you risk committing an offence yourself. In these circumstances, communications relating to such a transaction are not privileged and should be disclosed.

Suspecting a transaction constitutes an offence

If you merely suspect a transaction might constitute a money laundering offence, the position is more complex. If the suspicions are correct, communications with the client are not privileged. If the suspicions are unfounded, the communications should remain privileged and are therefore non-disclosable.

Prima facie evidence

If you suspect you are unwittingly being involved by your client in a fraud, the courts require prima facie evidence before LPP can be displaced [*O'Rourke v Darbishire* [1920] AC 581]. The sufficiency of that evidence depends on the circumstances: it is easier to infer a prima facie case where there is substantial material available to support an inference of fraud. While you may decide yourself if prima facie evidence exists, you may also ask the court for directions [*Finers v Miro* [1991] 1 W.L.R. 35].

The Crown Prosecution Service guidance for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances

exemption (see 7.5 below) applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence. It is likely that a similar approach would be taken with respect to a genuine, but mistaken, belief that LPP applies.

We believe you should not make a disclosure unless you know of prima facie evidence that you are being used in the furtherance of a crime.

7.5 Privileged circumstances

Quite separately from LPP, POCA recognises another type of communication, one which is received in 'privileged circumstances'. This is not the same as LPP, it is merely an exemption from certain provisions of POCA, although in many cases the communication will also be covered by LPP.

The privileged circumstances exemptions are found in the following places:

- POCA – section 330 (6)(b), (10) and (11)
- POCA – section 342 (4)
- Terrorism Act – section 19 (5) and (6)
- Terrorism Act – section 21A (8)

Although the wording is not exactly the same in all these sections, the essential elements of the exemption are:

- you are a professional legal adviser;
- the information or material is communicated to you:
 - by your client or their representative in connection with you giving legal advice;
 - by the client or their representative in connection with them seeking legal advice from you; or
 - by any person for the purpose of/in connection with actual or contemplated legal proceedings; and
- the information or material cannot be communicated or given to you with a view to furthering a criminal purpose.

The defence covers 'legal professional advisers' and their employees. For the position regarding notaries, see section 7.4.1 above.

Consider the crime/fraud exception when determining what constitutes the furthering of a criminal purpose.

Finally, section 330(9A) protects the privilege attaching to any disclosure made to a nominated officer for the purposes of obtaining advice about whether or not a disclosure should be made.

7.6 Differences between privileged circumstances and LPP

7.6.1 Protection of advice

When advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances communications between you and third parties will not be protected under the advice arm of LPP.

Privileged circumstances, however, exempt communications regarding information communicated by representatives of a client, where it is in connection with your giving legal advice to the client, or the client seeking legal advice from you. This may include communications with:

- a junior employee of a client (if it is reasonable in the circumstances to consider them to be a representative of the client); or
- other professionals who are providing information to you on behalf of the client as part of the transaction.

You should consider the facts of each case when deciding whether or not a person is a representative for the purposes of privileged circumstances.

7.6.2 Losing protection by dissemination

There may be circumstances in which a legal adviser has communicated to him information which is subject to legal professional privilege, but which does not fall within the definition of privileged circumstances.

For example, a legal professional representing client A may hold or have had communicated to him information which is privileged as between client B and his own legal professional, in circumstances where client A and client B are parties to a transaction, or have some other shared interest.

The sharing of this information may not result in client B's privilege being lost, if it is stipulated that privilege is not waived (*Gotha City v Sotheby's (no1)* [1998] 1 WLR 114).

Privileged circumstances will not apply because the information was not communicated to client A's legal professional by a client of his in connection with the giving by him of legal advice to that client. However, if it was given to him by any person in connection with legal proceedings or contemplated legal proceedings, privileged circumstances would apply.

In such circumstances, the legal professional representing client A would not be able to rely on privileged circumstances, but the information might still be subject to LPP, unless the crime/fraud exemption applied.

7.6.3 Vulnerability to seizure

It is important to correctly identify whether communications are protected by LPP or if they are merely covered by the privileged circumstances exemption. This is because the privileged circumstances exemption exempts you from certain POCA provisions. It does not provide any of the other LPP protections to those communications. Therefore a communication which is only covered by privileged circumstances, not

LPP, will still remain vulnerable to seizure or production under a court order or other such notice from law enforcement agencies.

7.7 When do I disclose?

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.

If the communication was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of POCA, which include making a disclosure to the NCA.

If neither of these situations applies, the communication will still be confidential. However, the material is disclosable under POCA and can be disclosed, whether as an authorised disclosure, or to avoid breaching section 330. Sections 337 [in force] and 339ZF [not yet in force] of POCA permit you to make such a disclosure and provides that you will not be in breach of your professional duty of confidentiality when you do so.

Chapter 8 – Terrorist property offences

8.1 General comments

Terrorist organisations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The Terrorism Act 2000 (as amended) criminalises not only the participation in terrorist activities but also the provision of monetary support for terrorist purposes.

8.2 Application

All persons are required to comply with the Terrorism Act. The principal terrorist property offences in sections 15 – 18 apply to all persons and therefore to all legal professionals. However, the specific offence of failure to disclose and the two tipping off offences apply only to persons in the regulated sector.

The definition of business in the regulated sector was amended by the Terrorism Act 2000 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 to reflect changes brought about by the third money laundering directive. There are similar changes to the definition of business in the regulated sector in POCA.

8.3 Principal terrorist property offences

8.3.1 Section 15 – fundraising

It is an offence to be involved in fundraising if you have knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes. You can commit the offence by:

- inviting others to make contributions;
- receiving contributions; or
- making contributions towards terrorist funding, including making gifts and loans.

It is no defence that the money or other property is a payment for goods and services.

8.3.2 Section 16 – use or possession

It is an offence to use or possess money or other property for terrorist purposes, including when you have reasonable cause to suspect they may be used for these purposes.

8.3.3 Section 17 – arrangements

It is an offence to become involved in an arrangement which makes money or other property available to another if you know, or have reasonable cause to suspect it may be used for terrorist purposes.

8.3.4 Section 18 – money laundering

It is an offence to enter into or become concerned in an arrangement facilitating the retention or control of terrorist property by, or on behalf of, another person including, but not limited to the following ways:

- by concealment
- by removal from the jurisdiction
- by transfer to nominees

It is a defence if you did not know, and had no reasonable cause to suspect, that the arrangement related to terrorist property.

Read about arrangements under POCA in Chapter 6.

8.4 Defences to principal terrorist property offences

The TACT and POCA Regulations 2007 of 26 December 2007 introduced three new defences to the main offences in sections 15 – 18. These defences are contained in sections 21ZA – 21ZC, and are as follows:

- **prior consent/DAML defence** – you make a disclosure to an authorised person before becoming involved in a transaction or an arrangement, and the person acts with the consent of an authorised officer;
- **consent/DAML defence** – you are already involved in a transaction or arrangement and make a disclosure, so long as there is a reasonable excuse for failure to make a disclosure in advance;
- **reasonable excuse defence** – you intended to make a disclosure but have a reasonable excuse for failing to do so. See section 6.7.1 on reasonable excuse.

Read Chapter 9 for more information on how to make a disclosure and gaining consent.

There are further defences relating to co-operation with the police in section 21. You do not commit an offence under sections 15-18 in the following further circumstances:

- you are acting with the express consent of a constable, including civilian staff at the NCA;
- you disclose your suspicion or belief to a constable or the NCA after you become involved in an arrangement or transaction that concerns money or terrorist property, and you provide the information on which your suspicion or belief is based. You must make this disclosure on your own initiative and as soon as reasonably practicable.

The defence of disclosure to a constable or the NCA is also available to an employee who makes a disclosure about terrorist property offences in accordance with the internal reporting procedures laid down by the practice.

8.5 Failure to disclose offences

8.5.1 Non-regulated sector

Section 19 provides that anyone, whether they are a nominated officer or not, must disclose as soon as reasonably practicable to a constable, or the NCA, if they know or suspect that another person has committed a terrorist financing offence based on information which came to them in the course of a trade, profession or employment. The test is subjective.

8.5.2 Regulated sector

Section 21A, inserted by the Anti-Terrorism Crime and Security Act 2001, creates a criminal offence for those in the regulated sector who fail to make a disclosure to either a constable or the practice's nominated officer where they know, suspect, or there are reasonable grounds for suspecting that another person has committed an offence. This was further expanded by the TACT and POCA Regulations 2007 to cover failure to disclose an attempted offence under sections 15 -18.

8.6 Defences to failure to disclose

The following are defences to failure to disclose offences under both section 19 and section 21A. Either:

- you had a reasonable excuse for not making the disclosure; or
- you received the information on which the belief or suspicion is based in privileged circumstances, without an intention of furthering a criminal purpose.

The TACT and POCA Regulations 2007 introduced an additional defence for those in the regulated sector. A person has a defence where they are employed or are in partnership with a 'professional legal adviser' to provide assistance and support and they receive information giving rise to the relevant knowledge or suspicion in privileged circumstances.

Read about privileged circumstances in 6.7.2.

It is also a defence under section 19 if you made an internal report in accordance with your employer's reporting procedures.

8.7 Section 21D tipping off offences: regulated sector

Section 21D(1) – disclosing a suspicious activity report (SAR).

It is an offence to disclose to a third person that a SAR has been made by any person to the police, HM Revenue and Customs, the NCA or a nominated officer, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR. This offence can only be committed:

- *after* a disclosure to the NCA
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR

- the information upon which the disclosure is based came to you in the course of business in the regulated sector

Section 21D(3) – disclosing an investigation.

It is an offence to disclose that an investigation into allegations relating to terrorist property offences is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector. The key point is that you can commit this offence, even where you are unaware that a SAR was submitted.

8.8 Defences to tipping off

8.8.1 Section 21E – disclosures within an undertaking or group etc

It is not an offence if an employee, officer or partner of a practice discloses that a SAR has been made if the disclosure is to an employee, officer or partner of the same undertaking.

A legal professional will also not commit a tipping off offence if a disclosure is made to another legal professional in a different undertaking, provided that the undertakings the parties work in:

- share common ownership, management or control, and
- carry on business in either an EEA state or a country or territory that imposes equivalent money laundering requirements equivalent to the EU.

8.8.2 Section 21F – other permitted disclosures

A legal professional will not commit a tipping off offence if all the following criteria are met:

- the disclosure is made to another legal professional in an EEA state, or one having an equivalent AML regime;
- the disclosure relates to a client or former client of both parties, or a transaction involving them both, or the provision of a service involving them both;
- the disclosure is made for the purpose of preventing a money laundering offence; and
- both parties have equivalent professional duties of confidentiality and protection of personal data.

8.8.3 Section 21G – limited exception for professional legal advisers

A legal professional will not commit a tipping off offence if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence. This exception and the tipping off offence in section 21D only apply to the regulated sector.

8.9 Making enquiries of a client

You will often make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

These enquiries will only amount to tipping off if you disclose that a suspicious activity report has been made, or that an investigation into allegations relating to terrorist property offences is being carried out or contemplated.

8.10 Other terrorist property offences in statutory instruments

8.10.1 The offences

Under The Al Qaida and Taliban (United Nations Measures) Order 2006 you must not:

- deal with the funds or economic resources of designated persons; or
- make funds and economic resources available, directly or indirectly for the benefit of designated persons.

Under the Terrorism (United Nations Measures) Order 2009, you must not:

- deal with the funds or economic resources of a designated person;
- make funds, financial services or economic resources available, directly or indirectly to a designated person; or
- make financial services or economic resources available to any person for the significant benefit of a designated person.

Finally, you must not knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions, enable, or facilitate the commission of any of the above offences.

It is a defence if you did not know nor had any reason to suspect that you were undertaking a prohibited act with respect to a designated person.

In relation to funds, 'deal with' is defined by the legislation as:

- using, altering, moving, allowing access to or transferring;
- dealing with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or
- making any other change that would enable use, including portfolio management.

In relation to economic resources, 'deal with' is defined as:

- using to obtain funds, goods, or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.

Financial services are defined broadly and include advisory services such as providing advice on:

- acquisitions; and

- corporate restructuring and strategy.

8.10.2 Obtaining a licence from the Office of Financial Sanctions Implementation (OFSI)

You must not proceed with a transaction without a licence from the OFSI Asset Freezing Unit where a client or the intended recipient of funds from the transaction is identified as a designated person.

You must do all of the following:

- suspend the transaction pending advice from the Asset Freezing Unit;
- contact the Asset Freezing Unit to seek a licence to deal with the funds; and
- consider whether you have a suspicion of money laundering or terrorist financing which requires a report to the NCA

You must not return funds to the designated person without the approval of the Asset Freezing Unit

The Asset Freezing Unit has the power to grant licences exempting certain transactions from the financial restrictions. Requests are considered on a case-by-case basis, to ensure that there is no risk of funds being diverted to terrorism.

Contact the Asset Freezing Unit to request a licence or obtain advice regarding financial restrictions at:

Asset Freezing Unit

Fax 020 7451 7677

Email ofsi@hmtreasury.gsi.gov.uk

Address Office of Financial Sanctions Implementation
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Chapter 9 – Making a disclosure

9.1 General comments

The disclosure regime for money laundering and terrorist financing is run by the financial intelligence unit within the National Crime Agency (the NCA). The NCA was launched on 7 October 2013 under provisions granted by the Crime and Courts Act 2013. It is a law enforcement body devoted to dealing with organised crime within the UK and networking with other law enforcement agencies to combat global organised crime.

For full details on the NCA and its activities view its website at:

<http://www.nationalcrimeagency.gov.uk/>

9.2 Application

All persons within the regulated sector and nominated officers have obligations under POCA and the Terrorism Act 2000 as amended, to make disclosures of suspicions of money laundering, terrorist financing and terrorist property offences.

In addition, any person may need to make an authorised disclosure about criminal and terrorist property.

All persons are required to make disclosures to the NCA of suspected terrorist financing.

9.3 Suspicious activity reports

9.3.1 What is a SAR?

A suspicious activity report (SAR) is the name given to the making of a disclosure to the NCA under either POCA or the Terrorism Act.

9.3.2 Who discloses?

Where a practice has a nominated officer, either they or their deputy will make the SAR to the NCA.

9.3.3 When?

You must make a SAR as soon as practicable after you have formed a reportable suspicion or know of terrorist financing or money laundering (subject to privilege considerations). Swiftly made SARs avoid delays in fulfilling your client's instructions.

Where a joint disclosure report [not yet in force] is made as a result of a disclosure request, it must be made either within the period specified by the requesting NCA officer, or within 28 days of complying with a request for voluntary disclosure of information from another person in the regulated sector.

9.3.4 How to disclose

Forms

The NCA has issued preferred forms to be completed when making a SAR. We encourage you to use the preferred form to enhance the NCA's ability to assess your SAR quickly.

SARs online

You should use SARs online where you have computer access. This securely encrypted system provided by the NCA allows you to:

- register your practice and relevant contact persons;
- submit a SAR at any time of day; and
- receive e-mail confirmations of each SAR submitted.

You can register with the NCA at

[https://www.ukciu.gov.uk/\(e50jai55ui0x2quvierajr45\)/Registration/NewUserRegistrationInfo.aspx](https://www.ukciu.gov.uk/(e50jai55ui0x2quvierajr45)/Registration/NewUserRegistrationInfo.aspx)

Post or fax

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. You will not receive acknowledgement of any SARs sent this way. Where you require consent/DAML you should send by fax, not by post.

Hard copy SARs should be sent to:

Fax: 020 7238 8256

Post: UK FIU

PO Box 8000

London SE11 5EN

9.3.5 Information to include

The NCA has provided information on completing the preferred SARs form.

To speed up consideration of your SAR, it is recommended that you use the NCA's glossary of codes for each reason for suspicion section of the report.

Contact your supervisory authority to find out your regulatory number.

9.3.6 Getting consent/DAML from the NCA to proceed

You will often be asking the NCA for consent/DAML to undertake acts which would be prohibited as a principal money laundering offence or a terrorist property offence.

While the NCA has [produced information on obtaining consent/DAML](#), here are a number of key points to remember:

- You only receive consent/DAML to the extent to which you asked for it. So it is vital that you clearly outline all the remaining steps in the transaction that could be a prohibited act. For example:

We seek consent/DAML to finalise an agreement for sale of property X and to then transfer property X into the name of (purchaser) and, following payment of disbursements, pay the proceeds of the sale of the property to (seller).

- The initial notice period is seven working days after the SAR is made, and if consent/DAML is refused, the initial moratorium period is a further 31 calendar days from the date of refusal. If you need consent/DAML sooner, you should clearly state the reasons for the urgency in the initial report and perhaps contact the NCA to discuss the situation. The NCA can sometimes give consent/DAML in a matter of hours.

Within the notice and moratorium period you must not do a prohibited act. However, this will not prevent you taking other actions on the file, such as writing letters, conducting searches etc.

9.3.7 Extensions of the moratorium period

The Criminal Finances Act 2017 has made important changes to the moratorium period under POCA. Section 336A of the amended Proceeds of Crime Act enables the moratorium period to be extended by court order and section 336C provides for an automatic extension of the moratorium period in certain cases.

The moratorium period allows law enforcement agencies to gather evidence to determine whether further action, such as restraint of the funds, should take place.

There are occasions where the NCA requires further information to be able to undertake proper analysis and make an informed decision on whether to investigate.

Section 336A – court’s power to extend moratorium period

The court (Crown Court in England, Wales and Northern Ireland and the Sheriff Court in Scotland) may only grant an extension of the moratorium period upon an application by a senior officer if it is satisfied that:

- an investigation is being carried out in relation to a relevant disclosure (but has not been completed),
- the investigation is being conducted diligently and expeditiously,
- further time is needed for conducting the investigation, and
- it is reasonable in all the circumstances for the moratorium period to be extended.

It will be important for the practice that made the SAR to consider (dependent upon whether the practice is on notice of the application and can participate in the proceedings – see below) these requirements have been satisfied by the applicant. In particular, that the investigation is being conducted diligently and expeditiously and that further time is needed for the investigation. This will obviously be fact specific in each instance.

A senior officer is defined as follows:

- Director General of the NCA or any other NCA officer authorised by the NCA;
- A police officer of at least the rank of inspector;
- An officer of HM Revenue and Customs;
- An immigration officer;
- A member of staff at the FCA;
- Director of the Serious Fraud Office; or
- An accredited financial investigator.

The application must be made by the senior officer before the initial moratorium period of 31 days expires. The court may extend the moratorium period by a further 31 days, i.e. the total moratorium period at this stage may be up to a maximum of 62 days. The amount of the extension should of course be based on the four requirements set out above so the practice should consider not just whether an extension request is justified but also whether the amount of extension requested is reasonable in all of the circumstances.

The court may hear further applications to extend the moratorium period (for further 31 day periods) provided that the total number of extensions does not exceed a period of 186 days over and above the initial 31 day moratorium period. In total this means that the moratorium period can be a maximum of 217 days.

Power of the court to exclude and withhold information from interested persons

The court may exclude an interested person (or anybody representing that person) from any part of a hearing to extend the moratorium period. The Court may also order on application that specified information is withheld from an interested person (or anybody representing that person). The court must exclude any interested person from an application to withhold specified information.

An interested person is either the person who made the SAR or any other person who appears to the senior officer to have an interest in the relevant property. The first category is straightforward but the second could in effect be the ultimate client of the practice or any other third party who may have an interest in the underlying property.

The court may withhold the specified information only if it is satisfied that there are reasonable grounds to believe that disclosure would lead to the following:

- evidence of an offence would be interfered with or harmed;
- the gathering of information about the possible commission of an offence would be interfered with;
- a person would be interfered with or physically injured;
- the recovery of property under the Act would be hindered; or
- national security would be put at risk.

What this all means in practice is that a person that has made a SAR may be excluded from participating in the hearing of the application to extend the moratorium

period. This will obviously hamper the ability of that person to analyse whether the application is reasonable or not. Secondly, the person (even if present in the hearing) may also be prevented from seeing important information on the basis that, if disclosed, to the person it may lead to one of the above prejudicial consequences. A possible difficulty here will be what the person does and does not know and whether they can sensibly either take instructions from its ultimate client (see risks of tipping off below) or take their own action to minimise the risks of a lengthy moratorium period with all the risks of tipping off.

Risks of tipping off

Despite the fact that these amendments allow a maximum moratorium period of 217 days, the extent to which the tipping off provisions have been dis - applied for the purposes of extension proceedings is specifically limited. Once a firm is on notice of an application to extend the moratorium period, it may inform its client of the existence of the application to extend the moratorium period without committing the tipping off offence. However, the firm is permitted to disclose "only such information as is necessary for the purposes of notifying the customer or client that an application...has been made" and no more than that. In effect the risks of tipping off are still present as the firm cannot disclose in those discussions the content of the SAR to the client, or even the basis for its suspicion.

The extensions may be problematic in time critical transactions but in most instances the extensions should be rare and given that they have to be made in 31 day increments are challengeable at different stages.

You will have to be careful however in dealing with clients and third parties and ensuring that no disclosures are made about a SAR which may prejudice any investigation. If you are seeking to challenge an application to extend time, then you should also consider whether it may properly do so without taking instructions and generally whether it would be in the best interests of your ultimate client to do so.

Section 336C – Automatic extension of the moratorium period.

If an application is made under section 336A and the initial 31 day moratorium period would end before that application is heard by the court, then the moratorium period is automatically extended from the time when it would otherwise end to the date the court determines the application. Also, if an appeal is made against a decision to extend the period and the moratorium period ends before that appeal is heard, then the moratorium period is automatically extended from the time that it would otherwise end to the date when the appeal is heard. However, the maximum period of any such automatic extension is a period of 31 days from the date when the period would otherwise end.

If an application is made under section 336A and is refused and if the period would otherwise end before the end of 5 days after that hearing, then the period will be extended for a further 5 days from the hearing date. This is presumably a safeguard for the investigating authority to take any further action (such as a restraint order) before the period again expires.

9.3.8 Contacting the NCA/UKFIU

For DAML enquiries, all contact with the UKFIU DAML Team is via email:
DAML@nca.x.gsi.gov.uk

For queries regarding SAR Online/general enquiries you can contact the UKFIU helpdesk by phone on 0207 238 8282 and select option 2 or 3. or by email at ukfiusars@nca.x.gsi.gov.uk.

9.3.9 Confidentiality of SARs

The NCA is required to treat your SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their practice is not disclosed to other persons.

If you have specific concerns regarding your safety if you make a SAR, you should raise this with the NCA either in the report or through the helpdesk. If you have concerns about your immediate safety following the making of a SAR you should contact your local police.

If you fear the confidentiality of a SAR you made has been breached call the SARs confidentiality breach line on 0800 234 6657.

9.4 Sharing of information within the regulated sector and joint disclosure reports (not yet in force)

Sections 339ZB-G of POCA [not yet in force] introduce a gateway for the sharing of information between persons and entities in the regulated sector on a voluntary basis and for the making of joint disclosure reports (super SARs). The provisions seek to encourage the sharing of information across the private and public sectors to combat money laundering by providing protection for what would otherwise be a breach of confidentiality if certain conditions are fulfilled. The conditions are summarised at 9.4.1 below. However, these provisions do not override legal professional privilege. A legal professional will therefore only be able to share information if legal professional privilege does not apply.

Where information is requested from one regulated person by another on a voluntary basis there are requirements imposed to notify the NCA. After information has been shared a joint disclosure report can be made to the NCA on behalf of the parties both disclosing and receiving the information, a so called 'super SAR'. Making either a required notification or a joint disclosure report will be treated as satisfying the requirements of sections 330 and 331 to make a disclosure in the regulated sector (see paragraphs 6.6.2 and 6.6.3).

9.4.1 Conditions

Information to be voluntarily disclosed must have come to a person in the course of business in the regulated sector and may only be disclosed to another person in the sector.

Disclosure must follow a request from either an authorised NCA officer or another regulated person.

A disclosure request must abide by certain formalities. It must state that it is made in connection with AML suspicions; identify the person (if known); describe the information sought, and; specify the person(s) to whom it is requested the information is disclosed.

If made by another person in the regulated sector a request must also set out the grounds for suspicion or provide information enabling the recipient to decide if the information should be disclosed.

In all cases, the person making the disclosure must be satisfied that disclosing the information may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.

9.4.2 Required Notification

A required notification must be made to the NCA either when a request is made by one person to another for voluntary disclosure of information, or before a person voluntarily shares information with another following a request to do so by the NCA.

These notifications will satisfy the requirements to make a disclosure under sections 330 and 331 (failure to disclose in the regulated sector).

9.4.3 Joint Disclosure Reports

A joint disclosure report can be made to the NCA by the parties who have given and received information by way of voluntary disclosure. A joint disclosure report will be treated as satisfying the requirements to make a disclosure for the purposes of sections 330 and 331.

The Joint Money Laundering Information Taskforce (JMLIT) was set up in 2016 to facilitate information sharing in the regulated sector and it may be advisable to consider any guidance that they issue following their piloting of these measures. It is anticipated that the NCA will in due course update their guidance on making SARs to accommodate the new provisions.

9.5 Feedback on SARs

The NCA provides some feedback on the value of SARs they have received, although such feedback will always be anonymised to protect the confidentiality of those who submitted it. Feedback is provided:

- in the NCA's 'SARs Annual Report';
- in meetings of the NCA's 'Legal Sector Engagement Group'; and
- In meetings of the NCA's 'SARs Regime Committee'.

Chapter 10 – Enforcement

10.1 General comments

The UK AML/CTF regime is one of the most robust in Europe. Breaches of obligations under the regime are backed by disciplinary and criminal penalties.

Law enforcement agencies and AML supervisors are working co-operatively with regulated professions to assist compliance and increase understanding of how to effectively mitigate risks. However, be in no doubt of the seriousness of the possible sanctions for a failure to comply, nor the willingness of supervisory and enforcement bodies to take appropriate action against non-compliance.

10.2 Supervision under the Regulations

Regulation 7 provides for several bodies to be supervisory authorities for different parts of the regulated sector.

Where a person in the regulated sector is covered by more than one supervisory authority, either the supervisory authorities must decide between them who is to be the sole supervisor of the person, or they must co-operate in the performance of their supervisory duties.

A supervisory authority must:

- identify and assess the international and domestic risks of money laundering and terrorist financing to which its sector is subject;
- monitor effectively the persons for whom it is responsible;
- take necessary measures to ensure those persons comply with the requirements of the Regulations;
- comply with its obligations under Regulation 46(2), which include:
 - adopting a risk-based approach to supervision;
 - ensuring its employees and officers have access to information on money laundering and terrorist financing risks;
 - basing the operation of its supervisory activities on the risk profiles it has prepared for its sector;
 - keeping a record of its supervisory actions and reasons for not acting in a particular case; and
 - taking effective measures to encourage its sector to report breaches of the Regulations;
- take appropriate measures, in accordance with a risk-based approach, to review practices' risk assessments and policies, controls and procedures;
- report to the NCA any suspicion that a person it is responsible for has engaged in money laundering or terrorist financing;
- make up to date information on money laundering and terrorist financing available to the persons it supervises;

- co-operate and co-ordinate their activities with other supervisory authorities, HM Treasury and law enforcement authorities; and
- collect certain information about the persons its supervises, and any other information it considers necessary for exercising its supervisory function.

Supervisory authorities that are also self-regulatory bodies are subject to additional obligations which are set out in Regulation 49.

10.2.1 Legal Sector Supervisors

The named supervisory authorities for the legal sector are:

- the Chartered Institute of Legal Executives;
- the Council for Licenced Conveyancers;
- the Faculty of Advocates;
- the Faculty Office of the Archbishop of Canterbury;
- the General Council of the Bar;
- the General Council of the Bar of Northern Ireland;
- the Law Society;
- the Law Society of Northern Ireland; and
- the Law Society of Scotland.

The supervisory authority listed in the Regulations for solicitors in England and Wales is the Law Society of England and Wales. This responsibility has been delegated in part to the Solicitors Regulation Authority (SRA).

The General Council of the Bar is the named supervisory authority for the Bar of England and Wales. It discharges its regulatory functions through the Bar Standards Board.

10.2.2 Other supervisors

Other supervisory authorities which may be of relevance to some legal professionals include:

- The Financial Conduct Authority – www.fca.org.uk
- The Insolvency Practitioners Association – www.insolvency-practitioners.org.uk; and
- The Chartered Institute of Taxation – www.tax.org.uk

Where a supervisory authority reaches agreement with another supervisor about who is to supervise the legal professional, this agreement will be made known to the legal professional in accordance with Regulation 7(3).

In all other cases of supervisory overlap, and where you have questions about AML supervision, you should contact your supervisory authority.

The Joint Money Laundering Steering Group (JMLSG) provides guidance to the financial sector which the FCA considers when assessing compliance with AML/CTF obligations.

[Read JMLSG's guidance](#)

10.2.3 Enforcement powers under the Regulations

Part 8 of the Regulations gives supervisory authorities a variety of powers for performing their functions under the Regulations.

The powers are:

- Regulation 66: power to require information from, and attendance of, relevant and connected persons without a warrant;
- Regulation 69: power to enter and inspect without a warrant;
- Regulation 70: power to enter a premises under a warrant; and
- Regulation 71: power to retain documents taken under Regulation 66 or 70.

In addition, Part 9 of the Regulations gives the FCA and HMRC powers to impose civil penalties, prohibit an individual from having a management role within a relevant person and/or seek an injunction restraining the contravention of a relevant requirement under the Regulations.

10.3 Disciplinary action against legal professionals

Conduct which fails to comply with AML/CTF obligations may also be a breach of your professional obligations. For further information contact your supervisory authority.

10.4 Offences and penalties

Not complying with AML/CTF obligations puts you at risk of committing criminal offences. Below is a summary of the offences and the relevant penalties. In addition to the principal offences, you could also be charged with offences of conspiracy, attempt, counselling, aiding, abetting or procuring a principal offence, depending on the circumstances.

10.4.1 POCA - relevant offences and penalties

Section	Description	Penalty
327	Conceals, disguises, converts, transfers or removes criminal property	On summary conviction – up to six months' imprisonment or a fine or both
328	Arrangements regarding criminal property	
329	Acquires, uses or has possession of criminal property	On indictment – up to 14 years' imprisonment or a fine or both

330	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – regulated sector	On summary conviction – up to six months' imprisonment or a fine or both
331	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – nominated officer in the regulated sector	On indictment – up to five years' imprisonment or a fine or both
332	Failure to disclose knowledge or suspicion of money laundering – nominated officer in non-regulated sector	
333A	Tipping off – regulated sector	On summary conviction - up to three months' imprisonment or a fine not exceeding level 5 or both. On conviction on indictment- up to two years' imprisonment or a fine or both.
342	Prejudicing an investigation	On indictment – up to five years' imprisonment or a fine or both

10.4.2 Terrorism Act- relevant offences and penalties

Section	Description	Penalty
15	Fundraising	On summary conviction – up to six months' imprisonment or a fine or both On indictment – up to 14 years' imprisonment or a fine or both
16	Use and possession	
17	Funding arrangements	
18	Money laundering	
19	Failure to disclose	
21A	Failure to disclose – regulated sector	

21	Tipping off –regulated sector	<p>On summary conviction- up to three months' imprisonment or a fine not exceeding level 5 on the standard scale, or both</p> <p>On conviction on indictment- up to two years' imprisonment, or a fine or both</p>
----	-------------------------------	--

10.4.3 Regulations - relevant offences and penalties

Schedule 6 lists a number of relevant requirements, the breach of which is an offence. In addition to the offence of breaching a relevant requirement, the Regulations contain offences of prejudicing investigations and disclosure offences.

Breach of a relevant requirement

The relevant requirements most likely to be applicable to legal professionals are those imposed under the Regulations listed in the table below. You should consult Schedule 6 and consider whether there are any further relevant requirements that apply to your business.

Regulation	Description	Penalty
18	Risk assessment by a relevant person	On summary conviction – a fine On indictment – up to two years' imprisonment or a fine or both
19	Policies, controls and procedures	
20	Policies, controls and procedures (group level)	
21	Internal controls	
23	Requirement on authorised persons to inform the FCA	
24	Training	
25	Directions to a parent organisation from a supervisory authority	
26	Acting as a beneficial owner, officer or manager without approval	
27	Application of CDD measures	

28	Application of CDD measures
30	Timing of verification
31(1)	Requirement to cease transactions where unable to apply CDD measures required by Regulation 28
33(1) and (4)-(6)	Obligation to apply enhanced due diligence
35	Enhanced due diligence: politically exposed persons
37	Application of simplified due diligence
39(2) and (4)	Reliance
40(1) and (5)-(7)	Record keeping
41	Data protection
43	Corporate bodies: obligations
44	Trustee obligations
45(2) and (9)	Register of beneficial ownership
56(1) and (5)	Requirement to be registered
57(1) and (4)	Applications for registration
66	Power to require information
69(2)	Entry and inspection without a warrant
70(7)	Entry of premises under warrant
77(2) and (6)	Power to impose civil penalties, suspension and removal of authorisation
78(2) and (5)	Prohibitions

Offence of prejudicing investigations

Under Regulation 87 a person commits the offence of prejudicing an investigation if:

- They know or suspect that an officer or proper person is acting in connection with an investigation which is being, or is about to be, conducted, or
- They conceal, destroy or dispose of, or cause or permit the falsification, concealment, destruction or disposal of documents relevant to an investigation.

It is not an offence if:

- The person did not know or suspect that the disclosure is likely to prejudice the investigation;
- The disclosure is made in the exercise of a function under, or in compliance with a requirement imposed by, the Regulations, TACT, POCA or any Act relating to criminal conduct or benefit from criminal conduct; or
- The person is a professional legal adviser and the disclosure is to a client in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.

The penalty for an offence under Regulation 87 is:

- On summary conviction:
 - In England or Wales, a fine or a term of imprisonment not exceeding three months or both;
 - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, fine not exceeding the statutory maximum or both.
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

Information offences

Under Regulation 88(1) a person commits an offence if, in purported compliance with a requirement imposed on them under the Regulations, they knowingly or recklessly make a statement which is false or misleading in a material particular.

The penalty for an offence under Regulation 88(1) is:

- On summary conviction:
 - In England or Wales, a fine or a term of imprisonment not exceeding three months or both
 - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, a fine not exceeding the statutory maximum or both.
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

Under Regulation 88(3), it is an offence to disclose information in contravention of a relevant requirement. It is a defence for the person to prove that they reasonably

believed the disclosure was lawful or that the information had already lawfully been made publicly available.

The penalty for an offence under Regulation 88(3) is:

- On summary conviction:
 - In England or Wales, a fine or a term of imprisonment not exceeding three months or both;
 - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, a fine not exceeding the statutory maximum or both.
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

10.5 Joint liability

Offences under the Regulations can be committed by a practice as a whole, whether it is a body corporate, partnership or unincorporated association.

However, if it can be shown that the offence was committed with the consent, contrivance or neglect of an officer, partner or member, then both the practice and the individual can be jointly liable.

10.5 Prosecution authorities

The Crown Prosecution Service is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Crown Office and Procurator Fiscal Service is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Director of Public Prosecutions for Northern Ireland is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Revenue and Customs Prosecutions Office is a prosecuting authority for offences under POCA and the Regulations.

The FCA is a prosecuting authority under POCA and the Regulations as a result of section 402 of the Financial Services and Markets Act 2000.

Chapter 11 – Civil liability

11.1 General comments

The Proceeds of Crime Act 2002 aims to deprive wrongdoers of the benefits of crime, not compensate the victims. The civil law provides an opportunity for victims to take action against wrongdoers and those who have assisted them, through a claim for constructive trusteeship. Victims often target the professional adviser in civil claims because they are more likely to be able to pay compensation, often by reason of their professional indemnity cover.

If you believe that you may have acted as a constructive trustee, you should seek legal advice.

11.2 Constructive trusteeship

Constructive trusteeship arises as a result of your interference with trust property or involvement in a breach of fiduciary duty. These are traditionally described respectively as knowing receipt and knowing assistance.

Your liability in either case is personal, an equitable liability to account, not proprietary. A constructive trustee has to restore the value of the property they have received or compensate the claimant for the loss resulting from the assistance with a breach of trust or fiduciary duty. See *Lord Millett in Dubai Aluminium Co Ltd v Salaam* [2002] 3 WLR 1913,1933.

The state of your knowledge is key to this liability. Records of CDD measures undertaken and disclosures or your notes provide evidence of your knowledge and intentions.

11.3 Knowing receipt

Liability for knowing receipt will exist where a person receives property in circumstances where the property is subject to a trust or fiduciary duty and contrary to that trust applies the property for their use and benefit. Considering each element in turn:

11.3.1 Receipt

- You must have received the property in which the claimant has an equitable proprietary interest.
- The property must be received:
 - in breach of trust;
 - in breach of a fiduciary duty, or
 - legitimately, but then misapplied.

11.3.2 For your use and benefit

When you receive money, e.g. as an agent, or, as in the case of a client account, as a trustee of a bare trust, then you are not liable for knowing receipt as it is not received for your use or benefit. You may however still be liable for knowing assistance.

Receiving funds that you apply in satisfaction of your fees will however be beneficial receipt and could amount to knowing receipt.

11.3.3 You must be at fault

What constitutes fault here is the subject of some debate. The Court of Appeal in *BCCI v Akinele* [2001] Ch.437 held that the test is whether you acted unconscionably. The test is a subjective one which includes actual knowledge and willful blindness. The factors the court identified were that:

1. You need not have acted dishonestly. It is enough to know a fiduciary or trust duty has been breached.
2. Your knowledge of the funds' provenance should be such that it was unconscionable for you to retain any benefit.

It is unclear whether a reckless failure to make enquiries a reasonable person would have made would be sufficient to establish liability. In *Dubai Aluminium Co Ltd v Salaam* [2002] 3 WLR 1913 1933 Lord Millett described knowing receipt as dishonest assistance. However, that may well have been specific to the particular facts he was considering.

11.4 Knowing assistance

If you help in a breach of fiduciary or trust duties then you are personally liable for the damage and loss caused. See *Twinsectra v Yardley* [2002] WLR 802.

The requirements to establish liability of this kind are:

11.4.1 Assistance in a breach of trust or fiduciary duty

The breach need not have been fraudulent, (see *Royal Brunei Airlines v Tan* [1995] 2 AC 378), and you do not need to know the full details of the trust arrangements you help to breach, nor the obligations incumbent on a trustee/fiduciary. You assist if you either:

- know that the person you are assisting is not entitled to do the things that they are doing; or
- have sufficient ground for suspicion of this

11.4.2 Fault test

There must be dishonesty, not just knowledge. The test for dishonesty is objective. The Privy Council in *Eurotrust v Barlow Clowes* [2006] 1 All ER stated that the test is whether your conduct is dishonest by the standards of reasonable and honest people, taking into account your specific characteristics and context, i.e. your intelligence, knowledge at the relevant time, and your experience.

Conscious impropriety is not required; it is enough to have shown willful blindness by deliberately failing to make the enquiries that a reasonable and honest person would make.

11.5 Making a disclosure to the NCA

11.5.1 While awaiting consent/DAML from the NCA

Your position can be difficult. While the client will be expecting you to implement their instructions, you may be unable to do so, or give explanations, as you may risk a tipping off offence.

The client may seek a court order for the return of the funds on the basis that you are breaching their retainer.

Case law provides no direct authority on the point, but a ruling on the obligations of banks is helpful in suggesting the courts' likely view of the obligations imposed on legal professionals. In *K v Nat West* the Court of Appeal ruled that a bank's contract with the customer was suspended whilst the moratorium period was in place, so the customer had no right to an injunction for return of monies. The court also said that as a matter of discretion, the court would not force the bank to commit a crime.

The Court of Appeal also approved the use of a letter to the court from the bank as evidence of its suspicion. Provision of evidence in these circumstances is permitted under s333(2)(b) of Proceeds of Crime Act as an exception to the tipping off provisions.

11.5.2 Where the NCA grants consent/DAML

In continuing with a transaction you will have to show that either:

- Although you had sufficient suspicion to justify a disclosure to the NCA, your concerns were not such as to render them accountable on a constructive trustee basis. Courts are likely to take into account the fact that you will generally operate in the regulated sector, and assume a degree of sophistication as a result of anti-money laundering training. Legal professionals are expected to be able to account for decisions to proceed with transactions; or
- Your suspicions were either removed or reduced by subsequent information or investigations.

The Courts have provided limited assistance in this area. *Bank of Scotland v A Limited* [2001]1WLR 751 stated that complying with a client's instructions was a commercial risk which a bank had to take. While the court gave some reassurance on the unlikelihood of any finding of dishonesty against an institution that had sought guidance from the court and did not pay funds away, this is of limited assistance because it is for the positive act of paying away funds that protection will be needed.

Such protection is not readily available. In *Amalgamated Metal Trading v City of London Police* [2003] 1 WLR 2711 the court held that while a court could make a declaration on whether particular funds were the proceeds of crime, a full hearing would be required with both the potential victim and the client participating. There

would have to be proof on the balance of probabilities that the funds were not the proceeds of crime. In practice this is highly unlikely to be practical.

11.6 Civil liability in relation to SARs

Under section 338(4A) of the Proceeds of Crime Act 2002: '[w]here an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made'.

Chapter 12 – Money laundering warning signs

Note: The following sections of this chapter do not apply to barristers or advocates for the reasons set out in section 1.1.1:

- 12.2.3 (Use of client accounts)
- 12.3.1 (Administration of estates)
- 12.3.4 (Powers of attorney/deputyship)

12.1 General comments

The Regulations require you to conduct ongoing monitoring of your business relationships and take steps to be aware of transactions with heightened money laundering or counter-terrorist financing risks.

The Proceeds of Crime Act 2002 requires you to report suspicious transactions.

This chapter highlights a number of warning signs for legal professionals generally and for those dealing with particular types of work, to help you decide whether you have reasons for concern or the basis for a disclosable suspicion.

12.2 General warning signs during a retainer

Because money launderers are always developing new techniques, no list of examples can be fully comprehensive; however, here are some key factors which may arise after client and retainer acceptance and give you cause for concern.

12.2.1 Secretive clients

While face-to-face contact with clients is not always necessary, an excessively obstructive or secretive client may be a cause for concern.

12.2.2 Unusual instructions

Instructions that are unusual in themselves, or that are unusual for your practice or your client, may give rise to a cause for concern.

Instructions outside your area of expertise

Taking on work which is outside your practice's normal range of expertise can be risky because money launderers might use such practices to avoid answering too many questions. An inexperienced legal professional might be influenced into taking steps which a more experienced legal professional would not contemplate. Be wary of instructions in niche areas of work in which your practice has no background, but in which the client claims to be an expert.

If your client is based a long way from your offices, consider why you have been instructed. For example, have your services been recommended by another client or is the matter based near your practice? Making these types of enquiries makes good business sense as well as being a sensible anti-money laundering check.

Changing instructions

Instructions or cases that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes.

The following situations could give rise to a cause for concern. Legal professionals should consider Accounts Rules if appropriate:

- a client deposits funds into your client account but then ends the transaction for no apparent reason;
- a client tells you that funds are coming from one source and at the last minute the source changes;
- a client unexpectedly asks you to send money received into your client account back to its source, to the client or to a third party.

Unusual retainers

Be wary of:

- disputes which are settled too easily as this may indicate sham litigation;
- loss-making transactions where the loss is avoidable;
- dealing with money or property where you suspect that either is being transferred to avoid the attention of a trustee in a bankruptcy case, HMRC, or a law enforcement agency;
- settlements paid in cash, or paid directly between parties – for example, if cash is passed directly between sellers and buyers without adequate explanation, it is possible that mortgage fraud or tax evasion is taking place;
- transactions which appear to be complex or unusually large, having regard to the parties involved; and
- unusual patterns of transactions which have no apparent economic purpose.

12.2.3 Use of client accounts

Only use client accounts to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting the proceeds of crime through a client account can give the funds the appearance of legitimacy, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into a banking system can become part of the placement stage of money laundering. Therefore, the use of cash may be a warning sign.

Establish a policy on handling cash

Large payments made in actual cash may also be a sign of money laundering. It is good practice to establish a policy of not accepting cash payments above a certain limit either at your office or into your bank account.

Clients may attempt to circumvent such a policy by depositing cash directly into your client account at a bank. You may consider advising clients in such circumstances that they might encounter a delay in completion of the final transaction. Avoid

disclosing your client account details as far as possible and make it clear that electronic transfer of funds is expected.

If a cash deposit is received, you will need to consider whether you think there is a risk of money laundering taking place and whether it is a circumstance requiring a disclosure to the NCA.

Source of funds

Accounts staff should monitor whether funds received from clients are from credible sources. For example, it is reasonable for monies to be received from a company if your client is a director of that company and has the authority to use company money for the transaction.

However, if funding is from a source other than your client, you may need to make further enquiries, especially if the client has not told you what they intend to do with the funds before depositing them into your account. If you decide to accept funds from a third party, perhaps because time is short, ask how and why the third party is helping with the funding.

You do not have to make enquiries into every source of funding from other parties. However, you must always be alert to warning signs and in some cases you will need to get more information.

In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Assess the risk in these cases and ask questions if necessary.

Disclosing client account details

Think carefully before you disclose your client account details. They allow money to be deposited into your account without your knowledge. If you need to provide your account details, ask the client where the funds will be coming from. Will it be an account in their name, from the UK or abroad? Consider whether you are prepared to accept funds from any source that you are concerned about.

Keep the circulation of client account details to a minimum. Discourage clients from passing the details on to third parties and ask them to use the account details only for previously agreed purposes.

12.2.4 Suspect territory

Retainers involving countries which do not have comparative money laundering standards may increase the risk profile of the retainer.

Consider whether extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.

Note also that EDD measures must be applied where a transaction or business relationship is with a person established in a 'high risk third country' (subject to the limited exception set out in Regulation 33(2)). See section 4.12.3.

12.3 Private client work

12.3.1 Administration of estates

The administration of estates is a regulated activity. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a low risk of money laundering for those working in this area.

Source of funds

When you are acting either as an executor, or for executors, there is no blanket requirement that you should be satisfied about the history of all of the funds which make up the estate under administration; however you should be aware of the factors which can increase money laundering risks.

Consider the following when administering an estate:

- where estate assets have been earned in a foreign jurisdiction, be aware of the wide definition of criminal conduct in POCA and the provisions relating to overseas criminal conduct;
- where estate assets have been earned or are located in a suspect territory, you may need to make further checks about the source of those funds.

The wide nature of the offences of 'acquisition, use and possession' in section 329 of POCA may lead to a money laundering offence being committed at an early point in the administration. The section 328 offence may also be relevant.

Be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent/DAML are avoided. A key benefit of the *Bowman v Fels* judgment is that a legal professional who makes a disclosure is now able to continue work on the matter, so long as they do not transfer funds or take any other irrevocable step.

How the estate may include criminal property

An extreme example would be where you know or suspect that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

If you know or suspect that the deceased person improperly claimed welfare benefits or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required. While administering an estate, you may discover or suspect that beneficiaries are not intending to pay the correct amount of tax or are avoiding some other financial charge (for example, by failing to disclose gifts received from the deceased fewer than seven years before death). Although these matters may not actually constitute money laundering (because no criminal conduct has yet occurred so there is no 'criminal property'), solicitors should carefully consider their position in conduct terms with respect to Principle 1 of the SRA Handbook.

Grant of probate

A UK grant of probate may be required before UK assets can be released, while for overseas assets the relevant local laws will apply. Remain alert to warning signs, for example if the deceased or their business interests are based in a suspect territory.

If the deceased person is from another jurisdiction and a legal professional is dealing with the matter in the home country, it may be helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

12.3.2 Trusts

Trust work is a regulated activity.

Trusts can be used as a money laundering vehicle. One risk period for trusts is when the trust is set up, as if the funds going into the trust are clean, it is only by the settlor, beneficiaries or other persons who control the trust requiring the trustees to use them for criminal purposes that they may form the proceeds of crime.

When setting up a trust, be aware of general money laundering warning signs and consider whether the purpose of the trust could be to launder criminal property. Could funds be being paid offshore illegitimately to reduce properly taxable profits in an onshore jurisdiction? Information about the purpose of the trust, including why any unusual structure or jurisdiction has been used, can help allay concerns. Similarly, information about the provider of the funds, the trust's beneficial owners and potential beneficiaries and those who have control of the funds, as required by the Regulations, will assist.

Whether you act as a trustee yourself, or for trustees, the nature of the work may already require information which will help in assessing money laundering risks, such as the location of assets and the identity of the trust's beneficial owners and potential beneficiaries. Again, any involvement of a suspect jurisdiction, especially those with strict bank secrecy and confidentiality rules, or without similar money laundering procedures, may increase the risk profile of the retainer.

If you think a money laundering offence has, or may have, been committed that relates to money or property which already forms part of the trust property, or is intended to do so, consider whether your instructions involve you in a section 328 arrangement offence. If they do, consider the options for making a disclosure.

Consider also whether a section 330 disclosure obligation has been triggered.

12.3.3 Charities

In common with trusts, while the majority of charities are used for legitimate reasons, they can be used as money laundering/terrorist financing vehicles.

If you are acting for a charity, consider its purpose and the organisations with which it is aligned. A charity which is registered with the Charity Commission is likely to be low risk. If you are receiving money on the charity's behalf from an individual or a company donor, or a bequest from an estate, be alert to unusual circumstances including large sums of money.

There is growing concern about the use of charities for terrorist funding. HM Treasury maintains a consolidated list of individuals and entities to whom you may not provide funds, economic resources, and in relation to terrorism, financial services. See also 9.6 of OFSI's Financial Sanctions Guidance.

<https://www.gov.uk/government/publications/financial-sanctions-faqs>

12.3.4 Powers of attorney/deputyship

Whether acting as, or on behalf of, an attorney or deputy, you should remain alert to money laundering risks.

Consider also your obligations to identify the authority of attorney or deputy to act on behalf of the client and verify their identity pursuant to Regulation 28(10).

If you are acting as an attorney you may learn financial information about the donor relating, for example, to non-payment of tax or wrongful receipt of benefits. You will need to consider whether to make a disclosure to the NCA.

Where the public guardian has an interest - because of a deputyship or registered enduring power of attorney - consider whether the Office of the Public Guardian (OPG) needs to be informed. Informing the OPG is unlikely to be tipping off because it is unlikely to prejudice an investigation.

If you discover or suspect that a donee has already completed an improper financial transaction that may amount to a money laundering suspicion, a disclosure to the NCA may be required (depending on whether legal professional privilege applies). However, it may be difficult to decide whether you have a suspicion if the background to the information is a family dispute.

12.4 Property work

12.4.1 Ownership issues

Properties owned by nominee companies or multiple owners may be used as money laundering vehicles to disguise the true owner and/or confuse the audit trail. Whilst you will need to identify the property-owning vehicle's beneficial owners where it is your client, consider advising a client in a property transaction whose counterparty is evidently a nominee company or recently formed special purpose vehicle, to obtain some information about the vehicle's beneficial owner.

Be alert to sudden or unexplained changes in ownership. One form of laundering, known as flipping, involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but you should be alert to the possibility of being misled about the true ownership of the property. You may wish to undertake further CDD measures on the person providing the funding.

12.4.2 Methods of funding

Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, as a legal professional, you will have information about how your client intends to fund the transaction, and will expect to be updated if those details change, for example if a mortgage falls through and new funding is obtained.

This is a sensible risk assessment measure which should help you decide whether you need to know more about the transaction.

Private funding

Purchase funds can comprise all or some private funding, with the balance of the purchase price being provided via a mortgage. Transactions that do not involve a mortgage have a higher risk of being fraudulent.

Look out for:

- large payments from private funds, especially if your client has a low income
- payments from a number of individuals or sources

If you are concerned:

- ask your client to explain the source of the funds. Assess whether you think their explanation is valid - for example, the money may have been received from an inheritance or from the sale of another property;
- consider whether the beneficial owners were involved in the transaction in the funds flow.

Remember that payments made through the mainstream banking system are not guaranteed to be clean.

Funds from a third party

Third parties often assist with purchases, for example relatives often assist first time home buyers. You may be asked to receive funds directly from those third parties. You will need to decide whether, and to what extent, you need to undertake any CDD measures in relation to the third parties. You may need to explain the identity of third party payers to your pooled client account to your bank on request.

Consider whether there are any obvious warning signs and what you know about:

- your client;
- the third party;
- their relationship; and
- the proportion of the funding being provided by the third party.

Consider your obligations to the lender in these circumstances – you are normally required to advise lenders if the buyers are not funding the balance of the price from their own resources.

Where you act for a vendor, you will also typically receive funds from the buyer or their solicitors, which you may hold on the buyer's behalf, pending an exchange or completion process. Where funds come direct from an unrepresented buyer you will need to undertake full CDD on the buyer.

Direct payments between buyers and sellers

You may discover or suspect that cash has changed hands directly, between a seller and a buyer, for example at a rural auction.

If you are asked to bank the cash in your client account, this presents a problem because the source of the cash is not your client and so checks on the source of the funding can be more difficult. The auction house may be able to assist because of checks they must make under the Regulations. However, you may decide to decline the request.

If you suspect that there has been a direct payment between a seller and a buyer, consider whether there are any reasons for concern (for example, an attempt to involve you in tax evasion) or whether the documentation will include the true purchase price.

A client may tell you that money is changing hands directly when this is not the case. This could be to encourage a mortgage lender to lend more than they would otherwise, because they believe that private funds will contribute to the purchase. In this situation, consider your duties to the lender.

12.4.3 Valuing

An unusual sale price (an evident overvalue or undervalue) can be an indicator of money laundering. While you are not required to get independent valuations, if you become aware of a significant discrepancy between the sale price and what you would reasonably expect such a property to sell for, consider asking more questions.

Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains beneficial ownership.

12.4.4 Lender issues

You may discover or suspect that a client is attempting to mislead a lender client to improperly inflate a mortgage advance - for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm's length may warrant particularly close consideration.

However, until the improperly obtained mortgage advance is received there is not any criminal property for the purposes of disclosure obligations under POCA.

If you suspect that your client is making a misrepresentation to a mortgagee you must either dissuade them from doing so or cease acting. Even if you no longer act for the client you may still be under a duty to advise the mortgage company.

If you discover or suspect that a mortgage advance has already been improperly obtained, consider advising the mortgage lender.

If you are acting in a re-mortgage and discover or suspect that a previous mortgage has been improperly obtained, you may need to advise the lender, especially if the re-mortgage is with the same lender. You may also need to consider making a disclosure to the NCA as there is criminal property (the improperly obtained mortgage advance).

Legal professional privilege

If your client has made a deliberate misrepresentation on their mortgage application you should consider whether the crime/fraud exemption to legal professional privilege will apply, so that no waiver to confidentiality will be needed before a disclosure is made.

However, you will need to consider matters on a case-by-case basis and if necessary, seek legal advice.

Tipping off offences

You may be concerned that speaking to the lender client conflicts with [tipping off](#) offences.

A key element of these offences is the likelihood of prejudicing an investigation. The risk of this is small when disclosing to a reputable lender or your insurer. The financial services sector is also regulated for the purposes of anti-money laundering and subject to the same obligations. There is also a specific defence of making a disclosure for the purposes of preventing a money laundering offence.

In relation to asking further questions of your client and discussing the implications of the Proceeds of Crime Act 2002, there is a specific defence for tipping off for legal advisers who are seeking to dissuade their client from engaging in a money laundering offence.

For further advice on tipping off, see section 6.8.

For further information about avoiding tipping off in a particular case, contact the NCA's Financial Intelligence Helpdesk on 020 7238 8282.

12.4.5 Tax issues

Tax evasion of any type, whether committed by your client or the other party to a transaction, can result in you committing a section 328 arrangements offence.

Your firm may also be exposed to the offence of corporate failure to prevent the facilitation of tax evasion under the Criminal Finances Act 2017 if one of your employees or associated persons facilitates tax evasion.

Abuse of the Stamp Duty Tax procedure may also have money laundering implications, for example if the purchase price is recorded incorrectly.

If a client gives you instructions which offend the Stamp Duty Land Tax procedure, you must consider your position in relation to your professional obligations. If you discover the evasion after it has occurred, you are obliged to make a disclosure, subject to any legal professional privilege.

12.5 Company and commercial work

The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason legal professionals working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

12.5.1 Forming a new company

If you work on the formation of a new company, be alert to any signs that it might be misused for money laundering or terrorist financing.

If the company is being formed in a foreign jurisdiction, you should clarify why this is the case. In countries where there are few anti-money laundering requirements, you should make particularly careful checks.

Refuse the retainer if you have doubts or suspicions.

12.5.2 Holding of funds

If you wish to hold funds as stakeholder or escrow agent in commercial transactions, consider the checks you wish to make about the funds you intend to hold, before the funds are received and whether it would be appropriate to conduct CDD measures on all those on whose behalf you are holding funds, particularly if any of them are unrepresented.

Consider any proposal that you collect funds from a number of individuals, whether for investment purposes or otherwise. This could lead to wide circulation of your client account details and payments being received from unknown sources.

12.5.3 Private equity

Legal professionals could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business);
- the formation of a private equity fund;
- ongoing legal issues relating to a private equity fund; and
- execution of transactions on behalf of a member of a private equity firm's group of companies, (a private equity sponsor), that will normally involve a vehicle company acting on its behalf, (newco).

Who is the client?

Start-up phase

In this phase, as you will be approached by individuals or a company seeking to become established (and in certain cases authorised) your client would be the individuals or company and you would therefore conduct CDD accordingly.

Formation of private equity funds

Your client may be the private equity sponsor or it may be an independent sponsor.

Consider whether you are advising the fund itself and whether you need to identify its investor beneficial owners.

You should therefore identify who your client is and apply the CDD measures according to their client type as set out in Chapter 4.

Where the client is a newco, you will need to obtain documentation evidencing the establishment of the newco and consider the issue of beneficial ownership.

Generally private equity work will be considered at low risk of money laundering or terrorist financing for the following reasons:

- private equity firms in the UK are also covered by the Regulations as a financial institution and they are regulated by the FCA;
- investors in private equity funds may be large institutions, some of which will also be regulated for money laundering purposes ;
- where the private equity sponsor or fund manager is regulated in the UK, EEA or a comparable jurisdictions, it is likely to have followed CDD processes prior to investors being accepted but their risk-based procedures and reputational risk appetite may be different from yours;
- the investment is generally illiquid and the return of capital is unpredictable;
- the terms of the fund documentation control the transfer of interests and the return of funds to investors.

Factors which may alter this risk assessment include:

- where the private equity sponsor or an investor is located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the 4th Directive;
- where the investor is either an individual or an investment vehicle itself (a private equity fund of funds);
- where the private equity sponsor is seeking to raise funds for the first time.

You may wish to consider the JMLSG Guidance.

The following points should be considered when undertaking CDD measures in relation to private equity work:

- where your client qualifies for simplified due diligence you do not have to identify beneficial owners unless there is a suspicion of money laundering; but ensure you identify your client correctly as where you are acting for the benefit of the fund as opposed to for the benefit of the investment manager, you will need to identify and consider the fund's investor beneficial owners;
- where simplified due diligence does not apply you need to consider the business structure of the client and conduct CDD on the client in accordance with that structure;

- where there is an appropriately regulated professional closely involved with the client who has detailed knowledge of the beneficial owners of the client, you may consider relying on them in accordance with Regulation 39;
- whether an unregulated private entity firm, fund manager or other person involved with the transaction is an appropriate source of information regarding beneficial ownership of the client should be determined on a risk-sensitive basis, issues to consider include:
 - the profile of the private equity sponsor, fund manager, (if different), or such other person;
 - their track record within the private equity sector; and
 - their willingness to explain identification procedures and provide confirmation that all beneficial owners have been identified.
- where you are using another person as an information source for beneficial owners, where there are no beneficial owners within the meaning of Regulation 6, the source may simply confirm their actual knowledge of this, or if beneficial owners do exist, the source should provide you with the identifying details of the beneficial owner or an assurance that the beneficial owners have been identified and that the details will be provided on request.
- where there is a tiered structure, such as a feeder fund or fund of funds structure, you must identify the beneficial owner but you may decide having made enquiries that no such beneficial owners exist even though you have got to the top of the structure.
- where it is envisaged that you will be acting for a newco which is to be utilised at a future point in a flotation or acquisition, it is only once they are established and signed up as a party to the transaction that you need to commence CDD measures on the newco. However, once you start acting for a newco, you will need to consider identification for it, and its beneficial owner. You may therefore wish to commence the process of identifying any beneficial owner in advance.

12.5.4 Collective investment schemes

Undertaking work in relation to retainers involving collective investment schemes may pose similar problems when undertaking CDD as for private equity work.

The risk factors with respect to a collective investment scheme will be decreased where:

- the scheme is only open to tax exempt institutional investors;
- investment managers are regulated individuals or entities;
- a prospectus is issued to invite investment.

Factors which will increase the risks include where:

- the scheme is open to non-tax exempt investors;
- the scheme or its investors are located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the third directive;

- neither the scheme nor the investment managers are regulated and do not conduct CDD on the investors.

You may also wish to take into account the JMLSG Guidance.

In addition to the points to consider outlined for private equity work, where a collective investment scheme has issued a prospectus it is advisable to review a copy of the prospectus to understand the intended structure of the investment scheme.

Chapter 13 – offences and reporting practical examples

13.1 General comments

Chapters 6 and 7 of this guidance worked through the theory of the law relating to when a money laundering offence has occurred, the requirements for making a disclosure and when you are unable to make a disclosure because of LPP or are exempted from making a disclosure due to privileged circumstances.

This chapter contains:

- flowcharts to give an overview of how all the obligations link together; and
- examples to help put the theory into context.

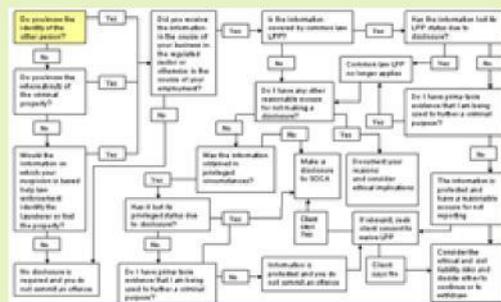
This chapter does not replace application of the legislation to your situation; nor should it be viewed without reference to the detailed discussion of the law in the rest of the guidance.

Further examples may be added to future editions of this guidance.

13.2 Principal offences

If you suspect that property involved in a retainer is criminal property, offences under section 327 and section 329 are relatively straightforward to assess. However, an arrangement offence under section 328 may be more complicated, particularly with transactional matters.

Do I have a suspicion that a principal money laundering offence is occurring?



[Download the decision chart](#) (PDF, 25kb)

13.2.1 Do I have an arrangement?

Under section 328, an arrangement must be created at a particular point in time. If you have formed a suspicion, first consider whether an arrangement already exists. For example, a client may instruct you to act for them in the purchase of a property, including the drafting of the contract and transfer documents. When you are instructed there will already an arrangement between the vendor and the purchaser, but not yet an arrangement for the purposes of section 328.

If an arrangement within section 328 already exists, any steps you take to further that arrangement will probably mean you are concerned in it. In this case, you would immediately need to consider making a disclosure.

13.2.2 No pre-existing arrangement

If there is no pre-existing arrangement, the transactional work you carry out may bring an arrangement under section 328 into existence. You may become concerned in the arrangement by, for example, executing or implementing it, which may lead you to commit an offence under section 328, and possibly under section 327 or 329.

Consider whether you need to make an authorised disclosure to:

- obtain consent/DAML to proceed with the transaction
- provide yourself with a defence to the principal money laundering offences

If you are acting within the regulated sector, consider whether you risk committing a failure to disclose offence, if you do not make a disclosure to the NCA.

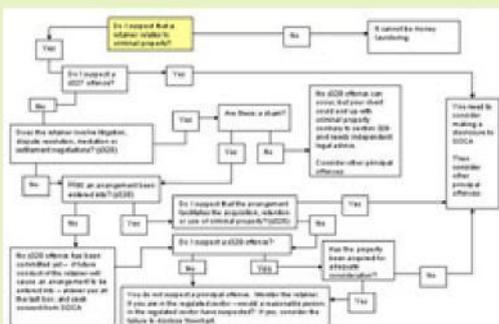
The following two flowcharts show the issues to consider when deciding whether to make a disclosure to the NCA.

I suspect continuation of a retainer will lead to me being a party to a principal offence. Do I have a defence?



[Download the decision chart](#) (PDF, 24kb)

I suspect someone else of a principal offence, or should reasonably suspect them, and am concerned I may commit a failure to disclose offence. Do I have a defence?



[Download the decision chart](#) (PDF, 27kb)

13.3 Should I make a disclosure?

13.3.1 Property transactions

Considering further the earlier example of a suspect contract for the purchase of a property, the following issues will be relevant when considering the disclosure requirements under POCA.

- If the information on which your suspicion is based is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.
- If the information was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of POCA, which include making a disclosure to the NCA.
- If neither of these situations applies, the communication will still be confidential. However, the material is disclosable under POCA and an authorised disclosure should be made

You have the option of withdrawing from the transaction rather than making an authorised disclosure, but you may still need to make a disclosure to avoid committing a failure to disclose offence.

What if I cannot disclose?

If you decide that either you cannot make a disclosure due to LPP or you are exempt from making a disclosure due to privileged circumstances, you have two options:

- you can approach the client for a waiver of privilege to make a disclosure and obtain consent/DAML to carry out the prohibited act, or
- you should consider your ethical obligations and whether you need to withdraw from the transaction

Waiver of privilege

When approaching your client for a waiver of privilege, you may feel less concerned about tipping off issues if your client is not the suspect party but is engaged in a transaction which involves criminal property. However, if you suspect that your client is implicated in the underlying criminal conduct, consider the tipping off offence and whether it is appropriate to discuss these matters openly with your client.

If you raise the matter with your client and they agree to waive privilege, you can make a disclosure to the NCA on your own or jointly with your client and seek consent if required.

If you are acting for more than one client on a matter, all clients must agree to waive privilege before you can make a disclosure to the NCA.

Refusal to waive privilege

Your client, whether sole or one of a number for whom you act, may refuse to waive privilege, either because he does not agree with your suspicions or because he does not wish a disclosure to be made. Unless your client provides further information which removes your suspicions, you must decide whether you are being used in a criminal offence, in which case neither LPP nor privileged circumstances apply.

If your client refuses to waive privilege but accepts that in proceeding with the transaction he may be committing an offence, you might conclude that you are being used in a criminal offence in which case neither exemption applies. In such circumstances it is not appropriate to tell the client that you are making the disclosure, as the risks of tipping off are increased.

If you are unable to make a disclosure, consider the ethical and civil risks of continuing in the retainer and consider withdrawing.

Consent/DAML and progressing the retainer

If you make a disclosure and consent/DAML is needed, consider whether you can continue working on the retainer before you receive that consent/DAML.

This will depend on whether an arrangement already exists or whether the further work will bring the arrangement into existence. Provided there is no pre-existing arrangement you should be free to continue your preparatory activities. However, the arrangement/prohibited act should not be finalised without appropriate consent/DAML.

13.3.2 Company transactions***Criminal property in a company***

The extent of the regulatory and legal obligations affecting companies and businesses means that there is an increased possibility that breaches will have been committed by your client that constitute criminal conduct and give rise to criminal property under POCA.

For example, the Companies Act 1985 contains many offences which will give rise to criminal property as defined by POCA. There does not need to be a criminal conviction, nor even a prosecution underway. If criminal conduct has, (or is suspected to have) taken place, and a benefit has been achieved, the result is actual or notional criminal property.

For a number of offences, the only benefit to your client (for the purposes of POCA) is saved costs. For example, it is criminal conduct to fail to notify the Information Commissioner that a

company will be processing 'personal data'. The saved notification fee should be treated as criminal property for the purposes of POCA.

It may be difficult to establish whether property or funds which are the subject of the transactions are the 'saved costs' in whole or in part and are therefore tainted. If you are dealing with the whole of a company's business or assets, no distinction is necessary. In other cases, it would be wrong to assume that because some assets are tainted, they all are, or that you are dealing with the tainted ones.

In most cases, unless there is some basis for suspecting that the assets in question result from saved costs, no disclosure or consent/DAML may be required in respect of the principal offence. However, a disclosure may still be required in respect of the failure to disclose offences.

Mergers and acquisitions

In typical corporate merger/acquisition/sale/take-over transactions, there are a number of issues to consider.

Legal professionals acting in company transactions will be acting in the regulated sector and so will have dual disclosure obligations, under the failure to disclose offence and in respect of the principal offences.

Different tests have to be applied to determine whether a disclosure can be made. When you are considering whether you are obliged to make a disclosure to avoid committing a failure to disclose offence, either LPP or privileged circumstances may apply.

When you are considering whether you must make a disclosure as a defence to the principal offences, only LPP is relevant.

For example, when you are acting for a vendor, you may receive information from the client about the target company which is protected under LPP and exempt from disclosure due to privileged circumstances. However, you may receive information from other representatives of the client (such as other professional advisers) which may only be exempt due to privileged circumstances. If information received is initially privileged, you need to consider whether the privilege is lost in the course of the transaction.

The information may be put into a data room and the purchaser, as part of the due diligence inquiries, may raise questions of the vendor's legal representatives which, in effect, result in the information being received again by the vendor's legal representatives.

That second receipt from the purchaser, or their legal representative, would not be protected by privileged circumstances. It will lose its exemption from disclosure unless the information was also subject to LPP which had not been waived when it was placed in the data room (eg a letter of advice from a legal professional to the vendor).

Consider whether privilege is removed by the crime/fraud exception. You may suspect, or have reasonable grounds to suspect someone of money laundering (which may simply mean they possess the benefits of a criminal offence contrary to section 329). Where the information on which the suspicion is based could be protected by LPP or exempted due to privileged circumstances, consider whether the crime/fraud exception applies

This may depend on:

- the nature of the transaction;
- the amount of the criminal property;

- the strength of the evidence.

These factors are considered in more detail below with respect to specific types of company sales.

Asset sales

In the case of an asset sale, all or some of the assets of the business may be transferred. If any asset transferred to a new owner is criminal property, a money laundering offence may be committed:

- The vendor may commit a section 327 offence by transferring the criminal property;
- Both the vendor and purchaser may be entering into an arrangement contrary to section 328;
- The purchaser may be committing a section 329 offence by possessing the criminal property

Adequate consideration defence

When looking at the purchaser's position, you will need to consider whether there would be an adequate consideration defence to a section 329 possession offence. This is where the purchase price is reasonable and constitutes adequate consideration for any criminal property obtained. In such a case, should the purchaser effectively be deprived of the benefit of that defence by section 328.

It is a question of interpretation whether sections 328 and 329 should be read together such that, if the defence under section 329 applies, an offence will also not be committed by the vendor under section 328. You should consider this point and take legal advice as appropriate.

Disclosure obligations after completion

As well as making disclosures relating to the transaction, vendors and purchasers will need to consider disclosure obligations in respect of the position after completion.

The purchaser will, after the transaction, have possession of the assets and may be at risk of committing a section 329 offence (subject to the adequate consideration defence outlined above).

The vendor will have the sale consideration in their possession. If the amount of the criminal property is material, the sale consideration may indirectly represent the underlying criminal property and the vendor may commit an offence under section 329.

Whether the criminal property is material or not will depend on its impact on the sale price. For example, the sale price of a group of assets may be £20m. If the tainted assets represent 10 per cent of the total, and the price for the clean assets alone would be £18m, it is clear that the price being paid is affected by, and represents in part, the criminal property.

If a client commits one of the principal money laundering offences, whether you are acting for the vendor or purchaser, you will be involved in a prohibited act. You will need to make a disclosure along with your clients and obtain appropriate consent/DAML.

When considering whether to advise your client about their disclosure obligations, remember the tipping off offences.

Am I prevented from reporting due to LPP?

Where you are acting for either the purchaser or vendor and conclude that you may have to make a disclosure and seek consent/DAML, first consider whether LPP applies. As explained above, this depends on how you received the information on which your suspicion is based.

Generally, when acting for the purchaser, if the information comes from the data room, LPP will not apply. When acting for the vendor, LPP may apply if the information has come from the client for the purpose of obtaining legal advice.

The crime/fraud exception

Where LPP applies, you will also need to consider whether the crime/fraud exception applies. The test is whether there is prima facie evidence that you are being used for criminal purposes.

Whether the crime/fraud exception applies will also depend on the purpose of the transaction and the amount of criminal property involved. For example, if a company wished to sell assets worth £100m, which included £25 of criminal assets, it would be deemed that the intention was not to use legal professionals for criminal purposes but to undertake a legitimate transaction. However, if the amount of criminal property was £75m, the prima facie evidence would be that the company did intend to sell criminal property and the exception would apply to override LPP.

Real cases will not all be so clear-cut. Consider the parties' intentions. If you advise your client of money laundering risks in proceeding with a transaction and the client decides, despite the risks, to continue without making a disclosure, you may have grounds to conclude that there was prima facie evidence of an intention to use your services for criminal purposes and therefore that privilege may be overridden.

Remember that for the purposes of the crime/fraud exception, it is not just the client's intention that is relevant.

Where LPP applies and is not overridden by the crime/fraud exception, it is nonetheless possible for your client to waive the privilege in order for a disclosure to be made.

Share sales

A sale of a company by way of shares gives rise to different considerations to asset sales. Unless shares have been bought using the proceeds of crime they are unlikely to represent criminal property, so their transfer will not usually constitute a section 327 offence, (for the vendor), or a section 329 offence, (for the purchaser).

However, the sale of shares could constitute a section 328 offence, depending on the circumstances, particularly if the criminal property represents a large percentage of the value of the target company. Consent/DAML may be needed if:

- the benefit to the target company from the criminal conduct is such that its share price has increased;
- as part of the transaction directors will be appointed to the board of the target company and they will use or possess criminal property; or
- the purpose of the transaction is to launder criminal property. That is, it is not a genuine commercial transaction.

Is the share value affected by criminal property?

If a company has been used to commit criminal offences, some or all of its assets may represent criminal property. The value of the shares may have increased as a result of that criminal activity. When the shares are then sold, by converting a paper profit into cash, the vendor and the purchaser have both been involved in a prohibited arrangement

For example, if 10 per cent of the profits of a company are earned from criminal activity, it is likely that the share price would be lower if only the legitimate profits were taken into account.

However, if the value of the criminal property is not sufficient to affect the purchase/sale price, the transaction is unlikely to be considered a prohibited arrangement since the vendor does not benefit from the company's criminal conduct. For example, a company is being purchased for £100m and within it is £25 of saved costs. If the costs had been paid by the company, it is unlikely that the price would be £99,999,975. The business is still likely to be valued at £100m.

Where criminal property is immaterial

Even if the value of criminal property is very small and immaterial to the purchase price, purchasers still need to consider their position after the acquisition. While shareholders do not possess a company's assets, the target company and directors may subsequently transfer, use or possess the assets for the purposes of the principal money laundering offences in sections 327 and 329.

If as part of the transaction, the purchaser proposes appointing new directors to the board of the target company, those directors may need to make a disclosure and seek consent/DAML so that they may transfer use or possess and use the criminal property.

In this case, you, and the vendors and the existing and new directors, may still need to make a disclosure, (subject to LPP issues), and seek consent/DAML, because they will be involved in an arrangement which involves the acquisition, use or control of criminal property by the new directors contrary to section 328.

In summary, the position may be as follows where the amount of the criminal property is immaterial:

- The target company will possess the proceeds of criminal conduct and may need to make a disclosure. If you discover this in privileged circumstances or it is protected by LPP, you cannot make a disclosure unless the fraud/crime exception applies.
- Those individuals or entities which, as a result of the transaction, will be in a position after completion to possess and use criminal property will need to make a disclosure and seek consent/DAML before completion.
- The legal professionals acting on the transaction and the vendor may also need to make a disclosure if they are involved in an arrangement which facilitates the acquisition or use of criminal property.
- Whenever a disclosure must be made, you must first consider whether privilege applies and, if applicable, whether the fraud/crime exception applies.

Shareholders

Generally, in a purchase or sale transaction, you will act for the company, not for its shareholders. However, it is possible for shareholders to become involved in an

arrangement prohibited by section 328. This is most likely to happen when the transaction requires a Class I or Class II circular to shareholders under the listing rules.

Firstly, consider whether the shareholders are, or may become, aware – perhaps through the risk warnings in the circular – of the risk of criminal conduct. Unless they are so aware, they are unlikely to have the necessary suspicion to be at risk of committing a money laundering offence.

Secondly, where shareholders are aware of the criminal conduct, consider whether the amount of criminal property is material to the transaction. That is, it would have an impact on the price or terms. If it is material, by voting in favour of it the shareholders will become concerned in a prohibited arrangement and will be required to make a disclosure and seek consent/DAML.

Also consider, in the context of an initial public offering, what risk warnings to include in any prospectus. You may need to give shareholders notice of their disclosure obligations via such a risk warning.

It is good practice to discuss the issue with the NCA to ensure that there are no tipping off concerns if details of the risks are set out in the public circular.

When each shareholder requires consent/DAML from the NCA, their express authority to make the disclosure will be required. It may be simplest to ask the shareholders to authorise the board of the vendor to make a disclosure and seek consent/DAML on their behalf at the same time as asking them to give conditional approval for the transaction.

Overseas conduct

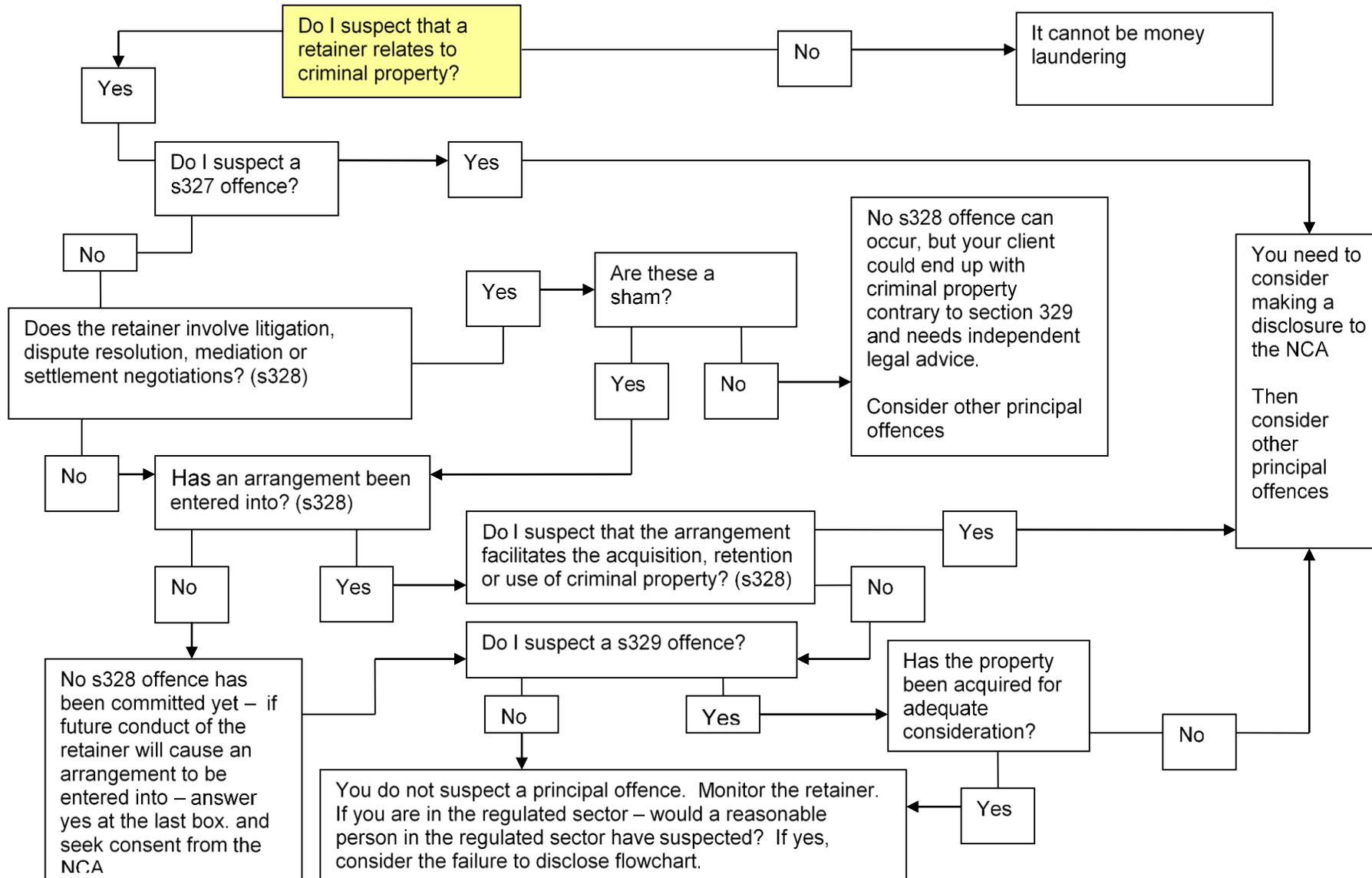
Where your suspicion of criminal conduct relates in whole or in part to overseas conduct, be aware of the wide definition of criminal conduct.

For example, you might discover or suspect that a company or its foreign subsidiary has improperly manipulated its accounting procedures so that tax is paid in a country with lower tax limits. Or you might form a concern about corrupt payments to overseas commercial agents which might be illegal in the UK.

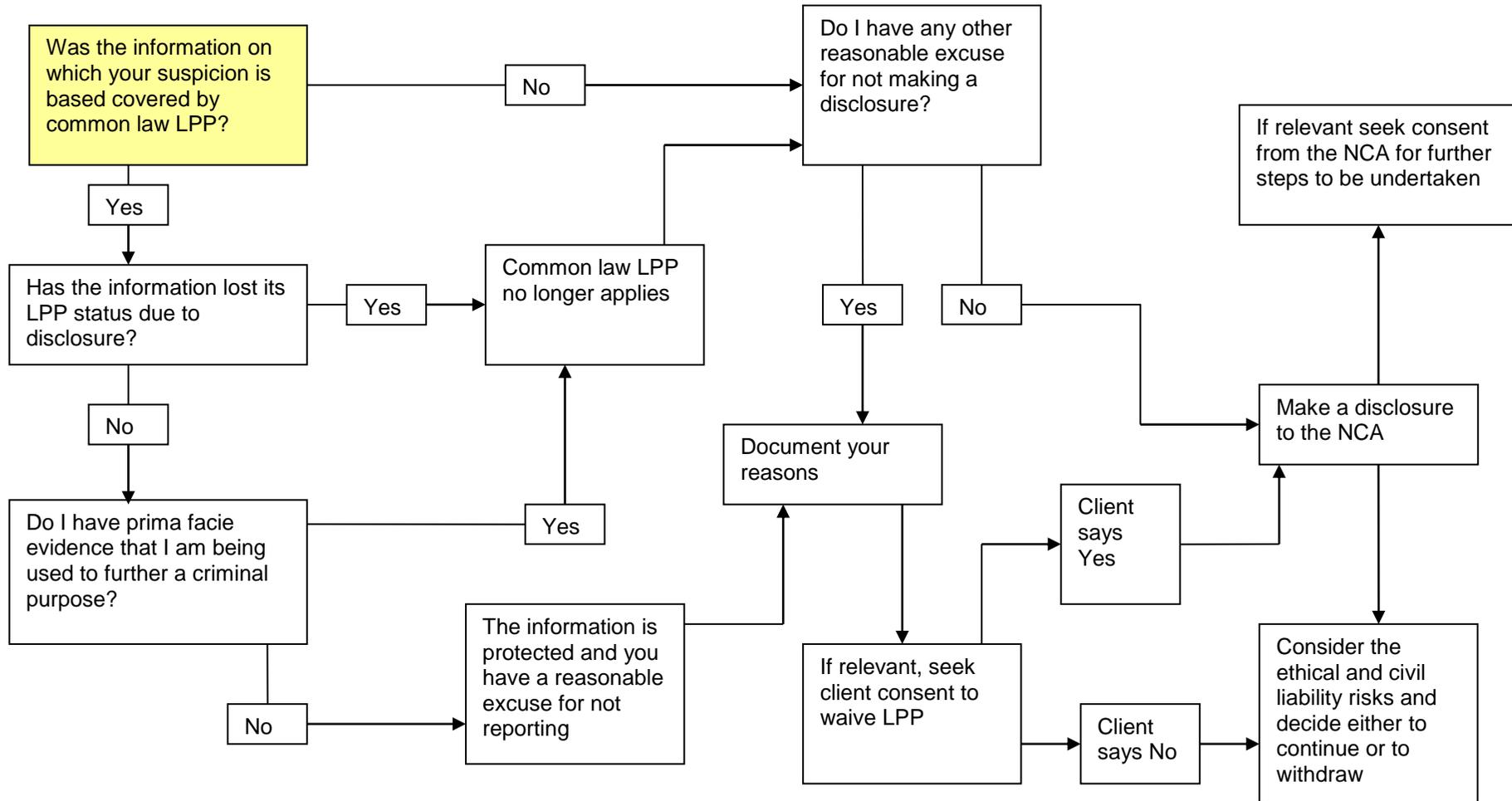
Even where the conduct is lawful overseas, in serious cases it will still be disclosable if the money laundering is taking place in the UK and the underlying conduct would be criminal if it had occurred in the UK.

In some cases the only money laundering activity in the UK may be your involvement in the transaction as a UK legal professional.

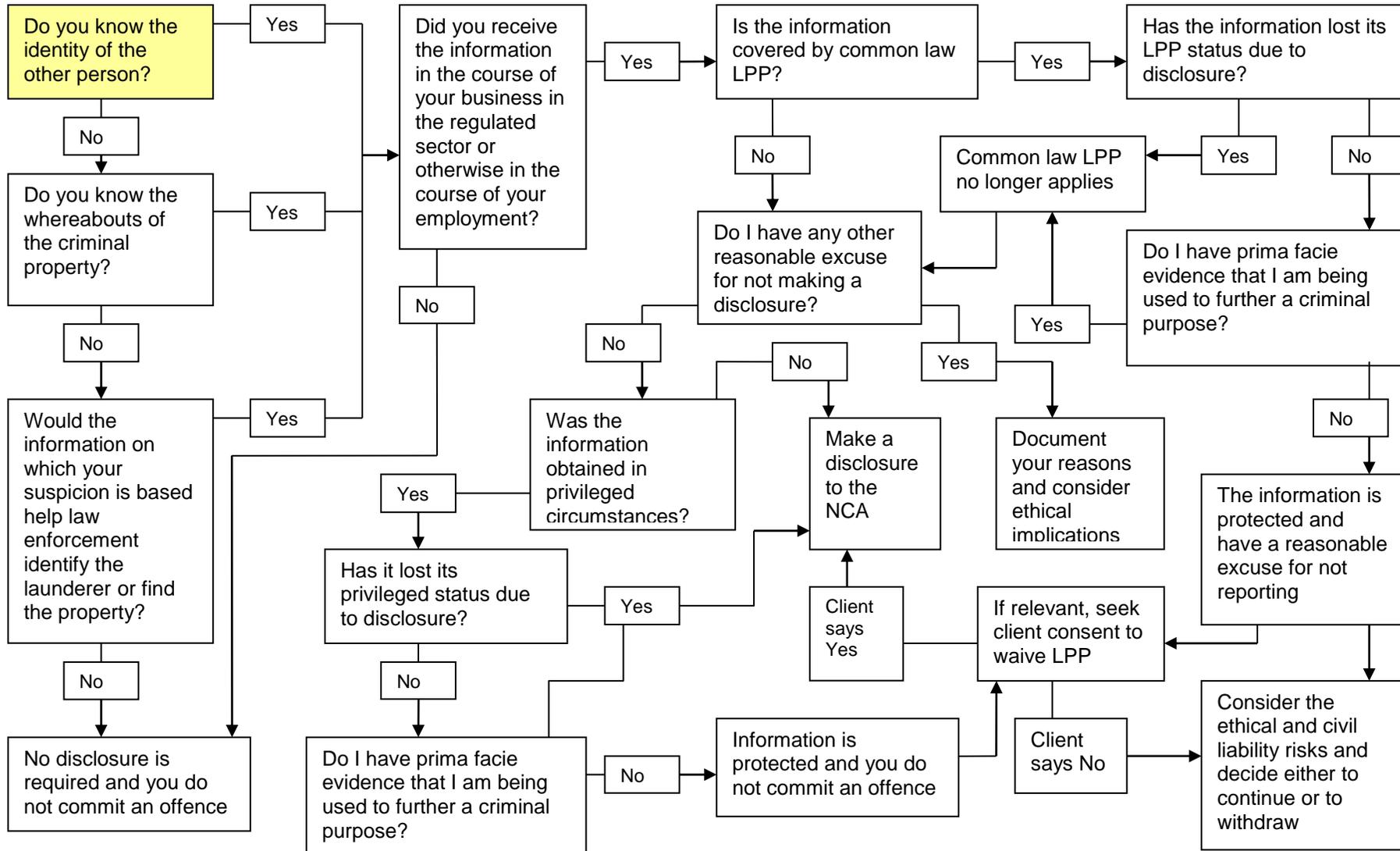
Annex I - flowchart A



Annex II Flowchart B



Annex III Flowchart C



*Federation of Law Societies
of Canada*



*Fédération des ordres professionnels
de juristes du Canada*

Anti-Money Laundering and Terrorist Financing Working Group

Final Report on the Model Rules

Amended October 1, 2018



INTRODUCTION

1. The Federation of Law Societies of Canada and its member law societies have been actively engaged in the fight against money laundering and the financing of terrorist activities for more than 15 years. Ensuring effective anti-money laundering and terrorist financing rules and regulations for the legal profession continues to be a strategic priority of the Federation.
2. Two model rules, aimed at limiting the handling of cash by members of the legal profession and ensuring legal counsel engage in due diligence in identifying their clients, have been the cornerstone of the regulators' anti-money laundering and anti-terrorism financing initiatives. The No Cash and Client Identification and Verification Model Rules (the "Model Rules") adopted in 2004 and 2008 respectively have been implemented by all Canadian law societies.
3. In October 2016, the Federation Council asked the CEOs Forum to establish a working group of senior staff to review the Model Rules. The Council recognized that a review of the Model Rules was overdue, particularly in light of a number of developments on the anti-money laundering and counter-terrorist financing landscape, including amendments to federal anti-money laundering and terrorist financing regulations, and the report of the mutual evaluation of Canada's federal anti-money laundering regime by the Financial Action Task Force ("FATF").
4. The Anti-Money Laundering and Terrorist Financing Working Group (the "Working Group") is co-chaired by Jim Varro, Director, Office of the CEO at the Law Society of Ontario and Frederica Wilson, Executive Director, Regulatory Policy and Public Affairs and Deputy CEO at the Federation. The other members of the Working Group are:
 - Susan Robinson – Executive Director, Law Society of Prince Edward Island
 - Chioma Ufodike – Manager, Trust Safety, Law Society of Alberta
 - Elaine Cumming – Professional Responsibility Counsel, Nova Scotia Barristers' Society
 - Deb Armour – Chief Legal Officer, Law Society of British Columbia
 - Jeanette McPhee – CFO and Director of Trust Regulation, Law Society of British Columbia
 - Leah Kosokowsky – Director, Regulation, Law Society of Manitoba
 - Anthony Gonsalves – Team Manager, Professional Regulation, Law Society of Ontario
 - Sylvie Champagne – Secrétaire de l'Ordre et Directrice du contentieux, Barreau du Québec
 - Nicholas Handfield – Chef, Services juridiques et relations institutionnelles, Chambre des notaires de Québec
 - Brenda Grimes – Executive Director, Law Society of Newfoundland and Labrador

5. From October 2017 until mid-March 2018 the Working Group held a consultation on a number of proposed amendments to the Model Rules and the introduction of a new Trust Accounting Model Rule. The Working Group received comments on the proposed rule changes from nine of the 14 law societies, the Canadian Bar Association, the Ontario Bar Association and several individual lawyers. In addition to providing feedback on the amendments proposed by the Working Group and on the proposed new Trust Accounting Model Rule, a number of commentators recommended other changes to the rules. Where such additional changes were consistent with ones explored in the consultation, or were simple matters of wording, the Working Group has responded to them in the final amendments. There were, however, some recommendations that were outside the scope of the consultation. That development, together with the fact that the government introduced new amendments to the federal anti-money laundering regulations part-way through the consultation period that are relevant to the rules, led the Working Group to conclude that there would be merit in a second, focused review of the rules in the near future. Finally, the Working Group's research highlighted the potential value of a risk-based approach to law societies' anti-money laundering and anti-terrorism financing regulation. The Working Group suggests that the Federation may wish to consider a move in that direction in the future.
6. The final proposed amendments and the new trust accounting rule for approval by the Council are set out in full in appendices to this report. The proposed amendments and new rule, the rationale for them and a summary of the feedback received together with the Working Group's response to the feedback are discussed in the body of the report.

NO CASH MODEL RULE

Definitions

7. In its consultation report, the Working Group proposed the addition of several definitions to the No Cash rule. Those additions have been maintained, but additional changes have been made to the definitions section to ensure consistency with the definitions in the Client Identification and Verification rule. This includes revisions to the definitions of "financial institution" and "public body" and the addition of a definition of "financial services cooperative".

Exceptions

8. To reflect the intention to restrict the situations in which legal counsel can accept large amounts of cash, the Working Group had recommended the deletion of some of the exceptions in the rule. In response to feedback from a number of law societies and others, the Working Group reconsidered some of the proposed amendments to the circumstances in which legal counsel may accept more than \$7,500 in cash. It is now proposed that exceptions for cash received from a peace officer, law enforcement agency or other agent of the Crown and to pay bail be maintained. The only exception that has been eliminated is that relating to cash received pursuant to a court order.

Other Amendments

9. The Working Group has maintained amendments to section 1 of the rule to clarify the amount of cash a lawyer may accept. The rule now specifies that a lawyer must not accept cash in an amount greater than \$7,500. In response to feedback received during the consultation, the section has also been amended to delete the words “or transaction”. The Working Group agreed that it is clearer to tie the cash limit to client matters. Pursuant to the amended rule, legal counsel may not accept cash in an aggregate amount greater than \$7,500 for any one client matter.
10. Also for greater clarity, the Working Group has removed the words “from a person” from section 1 and has changed “shall” to “must” or “will” (as appropriate) throughout the rule.

CLIENT IDENTIFICATION AND VERIFICATION RULE

Definitions

11. The Working Group is proposing a number of amendments to the definitions in the Client Identification and Verification rule, primarily to align with amended definitions in the federal regulations where similar terms are used in the Model Rule. These include the addition of definitions of “credit union central”, “disbursements”, “expenses”, “financial services cooperative” and “professional fees” and the deletion of the definition of “proceedings”. Amendments are also proposed to existing definitions including “financial institution”, “funds”, “public body”, and “securities dealer”. With the exception of additional changes to ensure the definitions refer to provinces and territories, the amendments to the definitions are unchanged from the version contained in the consultation document.
12. As reported in the consultation report, the Working Group discussed whether a band defined under the *Indian Act* (Canada) should be added to the definition of “public body”, although the corresponding definition in the federal regulations do not include Indian bands. This issue first arose some years ago and was the subject of research by the Federation, but no determination was made at that time. The Working Group considers this an important issue and to ensure that it is carefully considered, it is conducting additional research and will report on the issue at a later date.

Requirement to Identify Client

13. One of the amendments proposed in the consultation was the addition of language to subsection 2(1) of the client identification rule to situate the requirements of the section in the broader context of lawyers’ due diligence obligations. The amended provision reads (new language underlined):

2(1) Subject to subsection (3), a lawyer who is retained by a client to provide legal services must comply with the requirements of this Rule in keeping with the lawyer’s obligation to know their client, understand the client’s dealings in relation to the retainer with the client and manage any risks arising from the professional business relationship with the client.

14. The proposed amendment attracted comments from several law societies, most asking for clarification about the extent of the obligations referred to and one law society questioning whether the additional language would create “unintended conduct obligations for lawyers.” The members of the Working Group note that the additional language is intended to articulate existing obligations not create new ones. The Working Group considers it important to remind members of the profession that they have obligations beyond the specific duties set out in the rule and that the provisions in the rule must be understood in light of those obligations. The Working Group is recommending that the amendment be made, but recognizes that members of the profession will need guidance to fully understand their obligations. Guidance on this issue will be included in the guidelines and educational material for the profession that the Working Group is preparing.
15. Section 3 of the rule has been reorganized to clarify the information that legal counsel must obtain and record to identify clients who are individuals. The provisions addressing individuals and those addressing organizations have been separated and minor amendments have been made to the wording of the section.

Verification of Client Identity - Exemptions

16. In the consultation report, the Working Group proposed deleting certain exemptions to the obligation to verify client identity when a lawyer “engages in or gives instructions in respect of the receiving, paying or transferring of funds.” In response to feedback received during the consultation the Working Group has decided to recommend deleting only two of the existing exemptions: those dealing with funds paid or received pursuant to a court order or a settlement of any legal or administrative proceeding (subsections 5 (2)(d) (the first phrase) and (e)). It is the view of the members of the Working Group that there is some risk of money laundering in both cases and that eliminating the exemptions will not cause significant inconvenience to lawyers or their clients.
17. Prompted by feedback during the consultation from a number of sources questioning the exemption for electronic funds transfers (“EFTs”), the Working Group also considered whether it should recommend the deletion of that exemption. Under the existing rule, members of the legal profession are not required to verify the identity of a client when the financial transactions in which they are involved, or about which they provide instructions, are done by EFT. The primary rationale for the exception is that financial institutions, which conduct EFTs, assert extensive controls over these transactions. Pursuant to the definition of “electronic funds transfer” in the rule, only EFTs conducted by financial institutions are covered by the exemption. In addition, as the definition makes clear, neither the sending nor receiving account holders handle or control the transfer of the funds. Finally, the rule requires that the EFT transmission records contain important identifying information including the date of the transfer, the amount, and the names of the sending and receiving account holders and the parties or persons conducting and receiving the EFT.
18. Although the Working Group did not propose any change to this exemption, some commentators raised concerns about the possible breadth of the exemption and suggested that they present a risk of money laundering or terrorism financing activities even with the monitoring and controls placed on EFTs by financial institutions. The

Working Group agrees that there is merit in considering whether to remove the exemption, but in order to ensure that there is appropriate consultation on the issue, has decided to defer a decision on a possible recommendation to the next phase of its work. In the meantime the Working Group is recommending minor amendments to sections 4 and 5 of the rule to more clearly identify the EFT exemption.

Verification of Client Identity – Obligations

19. The Working Group consulted on a number of amendments to the provisions relating to the requirement to verify identity. Most were based on changes to the federal regulations, including a recommendation to remove the “reasonable measures” standard from the client verification provisions (subsection 6(1)). Another reflected the Working Group’s view that due diligence in knowing the client, their business, and how it intersects with the lawyer’s services, should include an inquiry into the source of funds involved in a transaction (subsection 6(1)(a)).
20. Although some respondents to the consultation expressed concern about the removal of the “reasonable measures” standard from subsection 6(1), the proposed change was generally well received. One of the concerns expressed was that the change could limit access to justice in some circumstances. The members of the Working Group note that the requirement to verify identity of clients does not apply in every lawyer-client relationship, but only when the receipt, payment or transfer of funds is involved. In addition there are a number of options for satisfying the verification requirement. In the view of the members of the Working Group, the requirements will increase the effectiveness of the rules in managing the risks of money laundering and terrorism financing activities, and are unlikely to create a barrier to the provision of legal services.
21. Questions were, however, raised about the proposed new requirement to obtain information about the source of funds (subsection 6(1)(a)). As drafted, the revised provision will require counsel to inquire into the source of funds involved in the financial transaction that triggers the verification requirement. To respond to feedback from the consultation and to ensure legal counsel understand the scope of this new obligation, the Working Group will provide additional guidance in the guidelines being prepared for the profession on the rules.
22. There were also questions about the meaning of “independent source documents” referred to in the version of subsection 6(1)(b) contained in the consultation report. Changes have been made to this section to clearly identify the requirement to verify identity using the documents or information specified in what is now subsection 6(6) of the rule.

Verification of Client Identity - Methods

23. Proposed changes to the methods that can be used to verify the identity of clients prompted numerous questions. A number of respondents concluded, for example, that the amendments would require all client verification to be done in person (eliminating the use of agents) and others raised concerns about the potential impact of the changes to verification methods in circumstances that would not actually trigger the verification requirement. The Working Group has made a number of changes to the final proposed

amendments to clarify their intent, and will provide detailed guidance in the materials being prepared for the profession on when they must simply *identify* their clients (or third parties) and when they must *verify* the client's (or third parties') identity.

24. New provisions have been added at subsections 6(2) and 6(3) to make it clear that counsel *may* use an agent in any circumstances to obtain the required verification information and *must* use an agent when a client is not physically present in Canada. In all cases, the lawyer must have a written agreement with the agent, and upon receiving from the agent the information obtained to verify identity, must review it to ensure that it is valid and current.
25. Additional amendments to the provisions on the use of an agent that were made to respond to changes to the corresponding provisions in the federal regulations are unchanged from the consultation report. Key changes include
 - (i) a requirement to satisfy oneself that the information obtained through an agent is valid,
 - (ii) the ability to rely on an agent's previous verification in the circumstances set out, and
 - (iii) no requirement for subsequent verification unless there are doubts about the information related to the original verification (the test before was 'if the lawyer recognizes the person').
26. Although the amendments to the provisions outlining the methods that may be used to verify identity (subsection 6(6)) are largely unchanged following the consultation, the Working Group has revised the heading of the section to more clearly indicate that it sets out the documents and information that can be used. In response to feedback received from the consultation about unfairness to lawyers in small firms or those that are not affiliated with other firms, the Working Group has removed a proposed amendment that would have permitted reliance on previous verification by an affiliated firm.
27. The amended rule will require the identity of clients who are individuals to be verified in one of the following ways:
 - (i) by reference to a current government issued photo identification document;
 - (ii) by reference to information in an individual's credit file; or
 - (iii) by a dual process method using information from a reliable source confirming the client's name and address, name and date of birth, or existence of a deposit account, credit card, or loan in the client's name.
28. Additional amendments speak to verifying the identity of individuals under the age of 15. In the case of those under the age of 12, it is the identity of the parent or guardian that must be verified. For those between 12 and 15, identity may be verified by referring to information from a reliable source that contains the name and address of one of the child's parents and confirming that it is the child's address.

Identifying Directors, Shareholders and Owners of Organizations

29. The consultation report contained several significant amendments to the requirements relating to identity verification for clients that are organizations (subsection 6(7)), including a proposal to delete the “reasonable efforts” standard, creating a requirement to *obtain*, rather than simply to *make reasonable efforts to obtain*, the names of all directors of an organization, and the names and addresses of the owners. Tracking changes to the federal regulations, the proposed amendments also introduced a requirement to “take reasonable measures to confirm the accuracy of the information obtained.” Responding to a criticism of both the law societies’ rules and the federal regulations, the Working Group also proposed the addition of a requirement to obtain beneficial ownership information. Although these amendments elicited less feedback than anticipated, some respondents raised serious concerns. One law society suggested that “these proposed amendments would place an incredibly onerous responsibility on lawyers and might in fact be impossible to comply with in certain circumstances.”
30. The Working Group understands these concerns and in the consultation report acknowledged the potential challenges to compliance with the beneficial ownership requirement, writing that “in the absence of a robust corporate registry system that includes beneficial ownership information, complying with this requirement may sometimes be difficult.” This concern was repeated in submissions of the Federation to the House of Commons Standing Committee on Finance in the spring, in which the Federation called for the creation of publicly accessible registries of beneficial owners. Despite these concerns, the Working Group initially concluded that as drafted, the amendments set a reasonable requirement and specifically acknowledge that it may not be possible to obtain the information. However, additional feedback from the law societies has persuaded the Working Group that in the absence of publicly accessible information on beneficial owners, a mandatory requirement in the rule would be neither appropriate nor effective. The Working Group has therefore revised the proposed amendment to subsection 6(7) to require legal counsel to “make reasonable efforts” to obtain the names and addresses of persons who own or control 25% or more of an organization. As obtaining the corresponding information for the beneficiaries and settlors of trusts would pose similar challenges, the “reasonable efforts” standard will apply to this requirement as well.
31. The changes to subsection 6(7) have necessitated changes to other subsections of the rule to ensure an effective requirement. Pursuant to the revised subsection 6(10), when legal counsel are not able to obtain the prescribed information on the directors, trustees and owners of organizations they must “take reasonable measures to ascertain the identity of the most senior managing officer of the organization.” The original proposal to require counsel to also “treat the activities in respect of that organization as requiring ongoing monitoring...” has been replaced with a requirement to determine whether the information received from the client in respect of their activities and funds, and the client’s instructions are consistent with the purpose of the retainer and the other information obtained under the rule. The revised provision would also require counsel to assess whether there is a risk that they might be assisting in or encouraging fraud or other illegal conduct.

32. The members of the Working Group believe that it is essential that the regulators address the money laundering and terrorism financing risks present in legal practice through robust rules that will assist legal counsel in avoiding unwitting involvement in these illegal activities. The potential for individuals to hide their identity as the actual owners of organizations has been identified as presenting a significant risk for money laundering and the financing of terrorist activities, and the Working Group remains convinced that requiring legal counsel to identify those who own or control organizations is necessary. For that reason the Working Group recommends that the Federation revisit the proposal for a mandatory requirement to obtain beneficial ownership information if and when publicly accessible registries are created.

Timing of Verification

33. Proposals made to address concerns raised by some law societies about the length of time permitted for verifying the identity of an organization after engaging in or giving instructions in the matter have not been changed. Although the Working Group did receive some feedback questioning the move from a 60 to a 30 day deadline for verification, most of the feedback was supportive of the amendment. The members of the Working Group also concluded that the shorter deadline, which is consistent with the federal regulations, is more consistent with the purpose of the provision.
34. Two additional amendments related to subsequent verification are also recommended for approval (see subsections 6(12) and 6(14)). For both individuals and organizations, a lawyer who has previously verified the individual or organizational client need not do so again “unless the lawyer has reason to believe the information, or the accuracy of it, has changed.” These changes were included in the consultation report, but minor changes have been made to the wording to ensure consistency between the two subsections.

Ongoing Monitoring

35. In its consultation, the Working Group proposed the addition of a new provision requiring ongoing monitoring of clients (section 10) to determine whether the client’s information and instructions are consistent with the purpose of the retainer and to ensure the lawyer is not assisting in or encouraging dishonesty, fraud, crime or illegal conduct. The proposal was prompted by a provision in the federal regulations relating to ongoing monitoring of the business relationship with a client in the context of assessing risks relating to money laundering associated with the relationship. The Working Group also proposed the addition of a reference to ongoing monitoring to the provision requiring a lawyer to withdraw from representation of the client if, once retained, the lawyer becomes aware that they would be assisting the client in fraud or other illegal conduct.
36. Respondents to the consultation flagged the need for clarity about the steps lawyers will be expected to take to comply with the ongoing monitoring provision and the circumstances in which the requirement will apply. The Working Group agrees that guidance on the application of the section is needed and will provide it in the materials for the profession that are being prepared.
37. Concern was also expressed about the fact that one of the identified purposes of ongoing monitoring is “ensuring that the lawyer is not assisting in or encouraging

dishonesty, fraud, crime or illegal conduct.” It was suggested that this sets too high a standard. The Working Group notes that members of the legal profession are bound by rules of professional conduct not to “knowingly assist in or encourage any dishonesty, fraud, crime, or illegal conduct.” To address the concerns that were raised in the consultation, the provision has been amended to be consistent with the existing professional conduct obligation.

Other amendments

38. The Working Group is proposing a few other minor amendments for greater clarity and consistency. These include the substitution of “must” or “will” for the word “shall” as appropriate throughout the rule.

TRUST ACCOUNTING MODEL RULE

39. The consultation report included a new trust accounting model rule intended to restrict the use of lawyers’ trust accounts to purposes directly connected to the provision of legal services. As noted in the report, a number of law societies already have such rules. In the view of the Working Group, allowing members of the legal profession to use their trust accounts for purposes unrelated to the provision of legal services unnecessarily increases the risk of money laundering or other illegal activity even when the money in question is not cash.
40. The proposed rule was generally well received, but there were some criticisms and questions about the drafting. The Working Group has redrafted the rule in response. In keeping with the general drafting style of law society rules and regulations, the proposed new model rule now makes it clear that the obligations are imposed on individual lawyers. In response to concerns that the commentary seemed to impose additional obligations on lawyers, it has been removed in the final draft. The Working Group will instead provide guidance on the rule in the guidelines for the profession that are being prepared. Finally, a definition of “money” has been added to the rule for clarity. The proposed rule now reads as follows:

Definitions

“money” includes cash, cheques, drafts, credit card transactions, post office orders, express and bank money orders and electronic transfer of deposits at financial institutions

1. A lawyer must pay into and withdraw from, or permit the payment into or withdrawal from, a trust account only money that is directly related to legal services that the lawyer or the lawyer’s law firm is providing.
2. A lawyer must pay out money held in a trust account as soon as practicable upon completion of the legal services to which the money relates.

Model Rule on Cash Transactions

“cash” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“disbursements” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“expenses” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“financial institution” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada,
- (c) cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company that is regulated by the *Trust and Loan Companies Act* (Canada),
- (h) a trust company or loan company that is regulated by a provincial or territorial Act,

- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory when it accepts deposit liabilities in the course of providing financial services to the public, or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“financial services cooperative” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives*, CQLR, c. C-67.3, or *An Act respecting the Mouvement Desjardins*, S.Q. 2000, c.77, other than a caisse populaire.

“funds” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“professional fees” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“public body” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act* (Ontario) [or equivalent legislation] or similar body incorporated under the law of another province or territory,
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act* (Canada) or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

1. A lawyer must not receive or accept cash in an aggregate amount of greater than \$7,500 Canadian in respect of any one client matter.
2. For the purposes of this rule, when a lawyer receives or accepts cash in a foreign currency the lawyer will be deemed to have received or accepted the cash converted into Canadian dollars at
 - (a) the official conversion rate of the Bank of Canada for the foreign currency as published in the Bank of Canada's Daily Noon Rates that is in effect at the time the lawyer receives or accepts the cash, or
 - (b) if the day on which the lawyer receives or accepts cash is a holiday, the official conversion rate of the Bank of Canada in effect on the most recent business day preceding the day on which the lawyer receives or accepts the cash.
3. Section 1 applies when a lawyer engages on behalf of a client or gives instructions on behalf of a client in respect of the following activities:
 - (a) receiving or paying funds;
 - (b) purchasing or selling securities, real properties or business assets or entities;
 - (c) transferring funds by any means.
4. Despite section 3, section 1 does not apply when the lawyer receives cash in connection with the provision of legal services by the lawyer or the lawyer's firm
 - (a) from a financial institution or public body,
 - (b) from a peace officer, law enforcement agency or other agent of the Crown acting in his or her official capacity,
 - (c) pursuant to pay a fine, penalty, or bail, or
 - (d) for professional fees, disbursements, or expenses, provided that any refund out of such receipts is also made in cash.

Model Rule on Recordkeeping Requirements for Cash Transactions

“cash” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“money” includes cash, cheques, drafts, credit card sales slips, post office orders and express and bank money orders.

1. Every lawyer, in addition to existing financial recordkeeping requirements to record all money and other property received and disbursed in connection with the lawyer’s practice, shall maintain
 - (a) a book of original entry identifying the method by which money is received in trust for a client, and
 - (b) a book of original entry showing the method by which money, other than money received in trust for a client, is received.
2. Every lawyer who receives cash for a client shall maintain, in addition to existing financial recordkeeping requirements, a book of duplicate receipts, with each receipt identifying the date on which cash is received, the person from whom cash is received, the amount of cash received, the client for whom cash is received, any file number in respect of which cash is received and containing the signature authorized by the lawyer who receives cash and of the person from whom cash is received.
3. The financial records described in paragraphs 1 and 2 may be entered and posted by hand or by mechanical or electronic means, but if the records are entered and posted by hand, they shall be entered and posted in ink.
4. The financial records described in paragraphs 1 and 2 shall be entered and posted so as to be current at all times.

5. A lawyer shall keep the financial records described in paragraphs 1 and 2 for at least the six year period immediately preceding the lawyer's most recent fiscal year end. [This paragraph does not apply to lawyers in Quebec as the Barreau requires that such records be retained without any limitation.]

Model Rule on Cash Transactions

“cash” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“disbursements” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“expenses” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“financial institution” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada,
- (c) cooperative credit society, savings and credit union or *caisse populaire* that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company that is regulated by the *Trust and Loan Companies Act* (Canada),
- (h) a trust company or loan company that is regulated by a provincial or territorial Act,

- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory when it accepts deposit liabilities in the course of providing financial services to the public, or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“financial services cooperative” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives*, CQLR, c. C-67.3, or *An Act respecting the Mouvement Desjardins*, S.Q. 2000, c.77, other than a caisse populaire.

“funds” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“professional fees” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“public body” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act (Ontario)* [or equivalent legislation] or similar body incorporated under the law of another province or territory.
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act (Canada)* or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

1. A lawyer ~~shall~~must not receive or accept ~~from a person,~~ cash in an aggregate amount of greater than \$7,500 ~~or more~~ Canadian or more dollars in respect of any one client matter ~~or transaction~~.
2. For the purposes of this rule, when a lawyer receives or accepts cash in a foreign currency ~~from a person~~ the lawyer ~~shall~~will be deemed to have received or accepted the cash converted into Canadian dollars at
 - (a) the official conversion rate of the Bank of Canada for the foreign currency as published in the Bank of Canada's Daily Noon Rates that is in effect at the time the lawyer receives or accepts the cash, or
 - (b) if the day on which the lawyer receives or accepts cash is a holiday, the official conversion rate of the Bank of Canada in effect on the most recent business day preceding the day on which the lawyer receives or accepts the cash.
3. ~~Paragraph~~Section 1 applies when a lawyer engages on behalf of a client or gives instructions on behalf of a client in respect of the following activities:
 - (a) receiving or paying funds;
 - (b) purchasing or selling securities, real properties or business assets or entities;
 - (c) transferring funds by any means.
4. Despite ~~paragraph~~section 3, ~~paragraph~~section 1 does not apply when the lawyer receives cash in connection with the provision of legal services by the lawyer or the lawyer's firm
 - (a) from a financial institution or public body,
 - (b) from a peace officer, law enforcement agency or other agent of the Crown acting in his or her official capacity,
 - (c) pursuant to a court order, or to pay a fine, penalty, or bail, or
 - (d) in an amount of \$7,500 or more for professional fees, disbursements, or expenses or bail, provided that any refund out of such receipts is also made in cash.

- ~~(a) pursuant to a court order, or to pay a fine or penalty, or~~
- ~~(b) in an amount of \$7,500 or more for professional fees, disbursements, expenses or bail, provided that any refund out of such receipts is also made in cash.~~

Model Rule on Recordkeeping Requirements for Cash Transactions

“cash” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“money” includes cash, cheques, drafts, credit card sales slips, post office orders and express and bank money orders.

1. Every lawyer, in addition to existing financial recordkeeping requirements to record all money and other property received and disbursed in connection with the lawyer’s practice, shall maintain
 - (a) a book of original entry identifying the method by which money is received in trust for a client, and
 - (b) a book of original entry showing the method by which money, other than money received in trust for a client, is received.
2. Every lawyer who receives cash for a client shall maintain, in addition to existing financial recordkeeping requirements, a book of duplicate receipts, with each receipt identifying the date on which cash is received, the person from whom cash is received, the amount of cash received, the client for whom cash is received, any file number in respect of which cash is received and containing the signature authorized by the lawyer who receives cash and of the person from whom cash is received.
3. The financial records described in paragraphs 1 and 2 may be entered and posted by hand or by mechanical or electronic means, but if the records are entered and posted by hand, they shall be entered and posted in ink.
4. The financial records described in paragraphs 1 and 2 shall be entered and posted so as to be current at all times.

5. A lawyer shall keep the financial records described in paragraphs 1 and 2 for at least the six year period immediately preceding the lawyer's most recent fiscal year end. [This paragraph does not apply to lawyers in Quebec as the Barreau requires that such records be retained without any limitation.]



Model Rule on Client Identification and Verification

Definitions

1. In this Rule,

“credit union central” means a central cooperative credit society, as defined in section 2 of the *Cooperative Credit Associations Act*, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial or territorial Act other than one enacted by the legislature of Quebec.

“disbursements” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“electronic funds transfer” means an electronic transmission of funds conducted by and received at a financial institution or a financial entity headquartered in and operating in a country that is a member of the [Financial Action Task Force](#), where neither the sending nor the receiving account holders handle or transfer the funds, and where the transmission record contains a reference number, the date, transfer amount, currency and the names of the sending and receiving account holders and the conducting and receiving entities.

“expenses” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“financial institution” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada,

- (c) a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company that is regulated by the *Trust and Loan Companies Act* (Canada),
- (h) a trust company or loan company that is regulated by a provincial or territorial Act;
- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory when it accepts deposit liabilities in the course of providing financial services to the public; or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“financial services cooperative” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives*, CQLR, c. C-67.3, or *An Act respecting the Mouvement Desjardins*, S.Q. 2000, c.77, other than a caisse populaire.

“funds” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“lawyer” means, in the Province of Quebec, an advocate or a notary and, in any other province or territory, a barrister or solicitor;

“organization” means a body corporate, partnership, fund, trust, co-operative or an unincorporated association;

“professional fees” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“public body” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act* (Ontario) [or equivalent legislation] or similar body incorporated under the law of another province or territory,
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act* (Canada) or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

“reporting issuer” means an organization that is a reporting issuer within the meaning of the securities laws of any province or territory of Canada, or a corporation whose shares are traded on a stock exchange that is designated under section 262 of the *Income Tax Act* (Canada) and operates in a country that is a member of the Financial Action Task Force, and includes a subsidiary of that organization or corporation whose financial statements are consolidated with those of the organization or corporation.

"securities dealer" means persons and entities authorized under provincial or territorial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity.

Requirement to Identify Client

2. (1) Subject to subsection (3), a lawyer who is retained by a client to provide legal services must comply with the requirements of this Rule in keeping with the lawyer's obligation to know their client, understand the client's financial dealings in relation to the retainer with the client and manage any risks arising from the professional business relationship with the client.

(2) A lawyer's responsibilities under this Rule may be fulfilled by any member, associate or employee of the lawyer's firm, wherever located.

(3) Sections 3 through 10 do not apply to

(a) a lawyer when he or she provides legal services or engages in or gives instructions in respect of any of the activities described in section 4 on behalf of his or her employer;

(b) a lawyer

(i) who is engaged as an agent by the lawyer for a client to provide legal services to the client, or

(ii) to whom a matter for the provision of legal services is referred by the lawyer for a client, when the client's lawyer has complied with sections 3 through 10,

or,

(c) a lawyer providing legal services as part of a duty counsel program sponsored by a non-profit organization, except where the lawyer engages in or gives instructions in respect of the receiving, paying or transferring of funds other than an electronic funds transfer.

3. A lawyer who is retained by a client as described in subsection 2(1) must obtain and record, with the applicable date, the following information:

(1) for individuals:

(a) the client's full name,

(b) the client's home address and home telephone number,

- (c) the client's occupation or occupations, and
 - (d) the address and telephone number of the client's place of work or employment, where applicable;
- (2) for organizations:
- (a) the client's full name, business address and business telephone number,
 - (b) other than a financial institution, public body or reporting issuer, the organization's incorporation or business identification number and the place of issue of its incorporation or business identification number, if applicable,
 - (c) other than a financial institution, public body or a reporting issuer, the general nature of the type of business or businesses or activity or activities engaged in by the client, where applicable, and
 - (d) the name and position of and contact information for the individual who is authorized to provide and gives instructions to the lawyer with respect to the matter for which the lawyer is retained,
- (3) if the client is acting for or representing a third party, information about the third party as set out in subsections (1) or (2) as applicable.

When Verification of Client Identity Required

4. Subject to section 5, section 6 applies where a lawyer who has been retained by a client to provide legal services engages in or gives instructions in respect of the receiving, paying or transferring of funds.

Exemptions re: certain funds

5. Section 6 does not apply
- (1) where the client is a financial institution, public body or reporting issuer,
 - (2) in respect of funds,
 - (a) paid by or to a financial institution, public body or a reporting issuer;

- (b) received by a lawyer from the trust account of another lawyer;
 - (c) received from a peace officer, law enforcement agency or other public official acting in their official capacity;
 - (d) paid or received to pay a fine, penalty, or bail; or
 - (e) paid or received for professional fees, disbursements, or expenses;
- (3) to an electronic funds transfer.

Requirement to Verify Client Identity

6. (1) When a lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, the lawyer must
- (a) obtain from the client and record, with the applicable date, information about the source of funds described in section 4, and
 - (b) verify the identity of the client, including the individual(s) described in paragraph 3(2)(d), and, where appropriate, the third party using the documents or information described in subsection (6).

Use of Agent

(2) A lawyer may rely on an agent to obtain the information described in subsection (6) to verify the identity of an individual client, third party or individual described in paragraph 3(2)(d) provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4).

(3) Notwithstanding subsection (2), where an individual client, third party or individual described in paragraph 3(2)(d) is not physically present in Canada, a lawyer must rely on an agent to obtain the information described in subsection (4) to verify the person's identity provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4).

Agreement for Use of Agent

(4) A lawyer who enters into an agreement or arrangement referred to in subsection (2) or (3) must:

- (a) obtain from the agent the information obtained by the agent under that agreement or arrangement; and
- (b) satisfy themselves that the information is valid and current and that the agent verified identity in accordance with subsection (6).

(5) A lawyer may rely on the agent's previous verification of an individual client, third party or an individual described in paragraph 3(2)(d) if the agent was, at the time they verified the identity,

- (a) acting in their own capacity, whether or not they were required to verify identity under this Rule, or
- (b) acting as an agent under an agreement or arrangement in writing, entered into with another lawyer who is required to verify identity under this Rule, for the purpose of verifying identity under subsection (6).

Documents and information for verification

(6) For the purposes of paragraph (1)(b), the client's identity must be verified by referring to the following documents, which must be valid, original and current, or the following information, which must be valid and current, and which must not include an electronic image of a document:

- (a) if the client or third party is an individual,
 - (i) an identification document containing the individual's name and photograph that is issued by the federal government, a provincial or territorial government or a foreign government, other than a municipal government, that is used in the presence of the individual to verify that the name and photograph are those of the individual;
 - (ii) information that is in the individual's credit file if that file is

- located in Canada and has been in existence for at least three years that is used to verify that the name, address and date of birth in the credit file are those of the individual;
- (iii) any two of the following with respect to the individual:
- (A) Information from a reliable source that contains the individual's name and address that is used to verify that the name and address are of those of the individual;
 - (B) Information from a reliable source that contains the individual's name and date of birth that is used to verify that the name and date of birth are those of the individual, or
 - (C) Information that contains the individual's name and confirms that they have a deposit account or a credit card or other loan amount with a financial institution that is used to verify that information.
- (b) For the purposes of clauses (6)(a)(iii)(A) to (C), the information referred to must be from different sources, and the individual, lawyer and agent cannot be a source.
- (c) To verify the identity of an individual who is under 12 years of age, the lawyer must verify the identity of one of their parents or their guardian.
- (d) To verify the identity of an individual who is at least 12 years of age but not more than 15 years of age, the lawyer may refer to information under clause (6)(a)iii(A) that contains the name and address of one of the individual's parents or their guardian and verifying that the address is that of the individual.
- (e) if the client or third party is an organization such as a corporation or society that is created or registered pursuant to legislative authority, a written confirmation from a government registry as to the existence, name and address of the organization, including the names of its directors, where applicable, such as

- (i) a certificate of corporate status issued by a public body,
 - (ii) a copy obtained from a public body of a record that the organization is required to file annually under applicable legislation, or
 - (iii) a copy of a similar record obtained from a public body that confirms the organization's existence; and
- (f) if the client or third party is an organization, other than a corporation or society, that is not registered in any government registry, such as a trust or partnership, a copy of the organization's constating documents, such as a trust or partnership agreement, articles of association, or any other similar record that confirms its existence as an organization.

Requirement to Identify Directors, Shareholders and Owners

(7) When a lawyer is engaged in or gives instructions in respect of any of the activities in section 4 for a client or third party that is an organization referred to in paragraph (6)(e) or (f), the lawyer must:

- (a) obtain and record, with the applicable date, the names of all directors of the organization, other than an organization that is a securities dealer; and
- (b) make reasonable efforts to obtain, and if obtained, record with the applicable date,
 - (i) the names and addresses of all persons who own, directly or indirectly, 25 per cent or more of the organization or of the shares of the organization,
 - (ii) the names and addresses of all trustees and all known beneficiaries and settlors of the trust, and
 - (iii) in all cases, information establishing the ownership, control and structure of the organization.

(8) A lawyer must take reasonable measures to confirm the accuracy of the information obtained under subsection (7).

(9) A lawyer must keep a record, with the applicable date(s), that sets out the information obtained and the measures taken to confirm the accuracy of that information.

(10) If a lawyer is not able to obtain the information referred to in subsection (7) or to confirm the accuracy of that information in accordance with subsection (8), the lawyer must

- (a) take reasonable measures to ascertain the identity of the most senior managing officer of the organization;
- (b) determine whether
 - (i) the client's information in respect of their activities,
 - (ii) the client's information in respect of the source of the funds described in section 4, and
 - (iii) the client's instructions in respect of the transaction, are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule;
- (c) assess whether there is a risk that the lawyer may be assisting in or encouraging fraud or other illegal conduct; and
- (d) keep a record, with the applicable date, of the results of the determination and assessment under paragraphs (b) and (c).

Timing of Verification for Individuals

(11) A lawyer must verify the identity of

- (a) a client who is an individual, and
- (b) the individual(s) authorized to provide and giving instructions on behalf of an organization with respect to the matter for which the lawyer is retained,

upon engaging in or giving instructions in respect of any of the activities described in section 4.

(12) Where a lawyer has verified the identity of an individual, the lawyer is not required to subsequently verify that same identity unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Timing of Verification for Organizations

(13) A lawyer must verify the identity of a client that is an organization upon engaging in or giving instructions in respect of any of the activities described in section 4, but in any event no later than 30 days thereafter.

(14) Where the lawyer has verified the identity of a client that is an organization and obtained information pursuant to subsection (7), the lawyer is not required to subsequently verify that identity or obtain that information, unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Record keeping and retention

7. (1) A lawyer must obtain and retain a copy of every document used to verify the identity of any individual or organization for the purposes of subsection 6(1).

(2) The documents referred to in subsection (1) may be kept in a machine-readable or electronic form, if a paper copy can be readily produced from it.

(3) A lawyer must retain a record of the information, with the applicable date, and any documents obtained for the purposes of section 3, subsection 6(7) and subsection 10(2) and copies of all documents received for the purposes of subsection 6(1) for the longer of

- (a) the duration of the lawyer and client relationship and for as long as is necessary for the purpose of providing service to the client, and
- (b) a period of at least six years following completion of the work for which the lawyer was retained.

Application

8. Sections 2 through 7 of this Rule do not apply to matters in respect of which a lawyer was retained before this Rule comes into force but they do apply to all matters for which he or she is retained after that time regardless of whether the client is a new or existing client.

Criminal activity, duty to withdraw at time of taking information

9. (1) If in the course of obtaining the information and taking the steps required in section 3 and subsections 6(1), (7) or (10), a lawyer knows or ought to know that he or she is or would be assisting a client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.

(2) This section applies to all matters, including new matters for existing clients, for which a lawyer is retained after this Rule comes into force.

Monitoring

10. During a retainer with a client in which the lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, the lawyer must:

- (1) monitor on a periodic basis the professional business relationship with the client for the purposes of:
- (a) determining whether
 - (i) the client's information in respect of their activities,
 - (ii) the client's information in respect of the source of the funds described in section 4, and
 - (iii) the client's instructions in respect of transactions are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule, and
 - (b) assessing whether there is a risk that the lawyer may be assisting in or encouraging fraud or other illegal conduct; and

(2) keep a record, with the applicable date, of the measures taken and the information obtained with respect to the requirements of paragraph (1)(a) above.

Duty to withdraw

11. (1) If while retained by a client, including when taking the steps required in section 10, a lawyer knows or ought to know that he or she is or would be assisting the client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.

Application

(2) This section applies to all matters for which a lawyer was retained before this Rule comes into force and to all matters for which he or she is retained after that time.

Federation of Law Societies
of Canada



Fédération des ordres professionnels
de juristes du Canada

Model Rule on Client Identification and Verification Requirements

*Adopted by Council of the Federation of Law Societies of Canada
March 20, 2008 and modified on December 12, 2008*

Definitions

1. In this Rule,

“credit union central” means a central cooperative credit society, as defined in section 2 of the *Cooperative Credit Associations Act*, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec.

“disbursements” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“electronic funds transfer” means an electronic transmission of funds conducted by and received at a financial institution or a financial entity headquartered in and operating in a country that is a member of the [Financial Action Task Force](#), where neither the sending nor the receiving account holders handle or transfer the funds, and where the transmission record contains a reference number, the date, transfer amount, currency and the names of the sending and receiving account holders and the conducting and receiving entities.

“expenses” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“financial institution” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada ~~or a bank to which the *Bank Act* applies,~~
- (c) a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company ~~to which that is regulated by~~ the *Trust and Loan Companies Act* (Canada) ~~applies,~~
- (h) a trust company or loan company that is regulated by a provincial or territorial Act;
- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory ~~where the department or agent~~ when it accepts deposit liabilities in the course of providing financial services to the public; or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“financial services cooperative” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives*, CQLR, c. C-67.3, or *An Act respecting the Mouvement Desjardins*, S.Q. 2000, c.77, other than a caisse populaire.

“funds” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“lawyer” means, in the Province of Quebec, an advocate or a notary and, in any other province, a barrister or solicitor;

“organization” means a body corporate, partnership, fund, trust, co-operative or an

unincorporated association;

~~“proceedings” means a legal action, application or other proceeding commenced before a court of any level, a statutory tribunal in Canada or an arbitration panel or arbitrator established pursuant to provincial, federal or foreign legislation and includes proceedings before foreign courts.~~

“professional fees” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“public body” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act* (Ontario) [or equivalent legislation] or similar body incorporated under the law of another province or territory,
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act* (Canada) or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

“reporting issuer” means an organization that is a reporting issuer within the meaning of the securities laws of any province or territory of Canada, or a corporation whose shares are traded on a stock exchange that is designated under section 262 of the *Income Tax Act* (Canada) and operates in a country that is a member of the

Financial Action Task Force, and includes a subsidiary of that organization or corporation whose financial statements are consolidated with those of the organization or corporation.

"securities dealer" means ~~a person or entity that is~~ persons and entities authorized under provincial or territorial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity.

Client Identity Requirement to Identify Client

2. (1) Subject to subsection (3), a lawyer who is retained by a client to provide legal services must comply with the requirements of this Rule: in keeping with the lawyer's obligation to know their client, understand the client's financial dealings in relation to the retainer with the client and manage any risks arising from the professional business relationship with the client.

(2) A lawyer's responsibilities under this Rule may be fulfilled by any member, associate or employee of the lawyer's firm, wherever located.

- (3) Sections 3 through 9-10 do not apply to
- (a) a lawyer when he or she provides legal services or engages in or gives instructions in respect of any of the activities described in section 4 on behalf of his or her employer;
 - (b) a lawyer
 - (i) who is engaged as an agent by the lawyer for a client to provide legal services to the client, or
 - (ii) to whom a matter for the provision of legal services is referred by the lawyer for a client, when the client's lawyer has complied with sections 3 through 910,
 - (c) a lawyer providing legal services as part of a duty counsel program sponsored by a non-profit organization, except where the lawyer engages in or gives instructions in respect

of the receiving, paying or transferring of funds other than an electronic funds transfer.

3. A lawyer who is retained by a client as described in section subsection 2(1) ~~shall~~must obtain and record, with the applicable date, the following information:

(1) for individuals:

- (a) the client's full name,
- ~~(b) the client's home address and home telephone number,~~
- (c) the client's occupation or occupations, and
- (d) the address and telephone number of the client's place of work or employment, where applicable;

(2) for organizations:

- (a) the client's full name, business address and business telephone number, ~~if applicable,~~
- ~~(b)(a) if the client is an individual, the client's home address and home telephone number,~~
- (b) ~~if the client is an organization,~~ other than a financial institution, public body or reporting issuer, the organization's incorporation or business identification number and the place of issue of its incorporation or business identification number, if applicable,
- ~~(a) if the client is an individual, the client's occupation or occupations,~~
- ~~(b) if the client is an organization,~~
- (c) other than a financial institution, public body or a reporting issuer, the general nature of the type of business or businesses or activity or activities engaged in by the client, where applicable, and
- (d) the name and position of and contact information for the individual who is authorized to provide and gives instructions to the lawyer with respect to the matter for which the lawyer is retained,

(3) if the client is acting for or representing a third party, information about the third party as set out in ~~paragraphs (a) to (f)~~subsections (1) or (2) as applicable.

When Verification of Client Identity and Verification Required

4. Subject to section 5, section 6 applies where a lawyer who has been retained by a client to provide legal services engages in or gives instructions in respect of the receiving, paying or transferring of funds, ~~other than an electronic funds transfer.~~

Exemptions re: certain funds

5. ~~(1)~~ Section 6 does not apply (1) where the client is a financial institution, public body or reporting issuer;
- (2) ~~Section 6 does not apply~~ in respect of funds,
- (a) paid by or to a financial institution, public body or a reporting issuer;
 - ~~(a)~~ received by a lawyer from the trust account of another lawyer;
 - (b) ;
 - ~~(b)(c)~~ received from a peace officer, law enforcement agency or other public official acting in their official capacity;
 - ~~(e)(d)~~ paid or received ~~pursuant to a court order or to pay a fine or~~ penalty; or bail; or
 - ~~(b)~~ ~~paid or received as a settlement of any legal or administrative proceedings; or~~
 - ~~(d)(e)~~ paid or received for professional fees, disbursements, or expenses ~~or bail;~~
- (3) to an electronic funds transfer.

Requirement to Verify Client Identity

6. (1) When a lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, ~~including non-face-to-face transactions, the lawyer shall take reasonable steps to verify the identity of the client, including the individual(s) described in section 3, clause (f)(ii), and, where appropriate, the third~~

party, ~~using what the lawyer reasonably considers to be reliable, independent source documents, data or information.~~ the lawyer must

(a) ~~Examples obtain from the client and record, with the applicable date, information about the source of funds described in section 4, and~~

~~(a)(b) verify the identity of the client, including the individual(s) described in paragraph 3(2)(d), and, where appropriate, the third party using the documents or information described in subsection (6).~~ independent source documents.

Use of Agent

~~(2) For the purposes of subsection (1), independent source documents may include:~~

~~(2) A lawyer may rely on an agent to obtain the information described in subsection (6) to verify the identity of an individual client, third party or individual described in paragraph 3(2)(d) provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4).~~

~~(3) Notwithstanding subsection (2), where an individual client, third party or individual described in paragraph 3(2)(d) is not physically present in Canada, a lawyer must rely on an agent to obtain the information described in subsection (4) to verify the person's identity provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4)~~

Agreement for Use of Agent

~~(4) A lawyer who enters into an agreement or arrangement referred to in subsection (2) or (3) must:~~

~~(a) obtain from the agent the information obtained by the agent under that agreement or arrangement; and~~

~~(b) satisfy themselves that the information is valid and current and that the agent verified identity in accordance with subsection (6).~~

(5) A lawyer may rely on the agent's previous verification of an individual client, third party or an individual described in paragraph 3(2)(d) if the agent was, at the time they verified the identity,

- (a) acting in their own capacity, whether or not they were required to verify identity under this Rule, or
- (b) acting as an agent under an agreement or arrangement in writing, entered into with another lawyer who is required to verify identity under this Rule, for the purpose of verifying identity under subsection (6).

Documents and Information for Verification

(6) For the purposes of paragraph (1)(b), the client's identity must be verified by referring to the following documents, which must be valid, original and current, or the following information, which must be valid and current, and which must not include an electronic image of a document:

- (a) if the client or third party is an individual, ~~valid original government issued~~
 - (i) an identification, ~~including a driver's licence, birth certificate,~~ document containing the individual's name and photograph that is issued by the federal government, a provincial or territorial ~~health insurance~~ government or a foreign government, other than a municipal government, that is used in the presence of the individual to verify that the name and photograph are those of the individual;
 - (ii) information that is in the individual's credit file if that file is located in Canada and has been in existence for at least three years that is used to verify that the name, address and date of birth in the credit file are those of the individual;
 - (iii) any two of the following with respect to the individual:
 - (A) Information from a reliable source that contains the individual's name and address that is used to verify that the

name and address are of those of the individual;

(B) Information from a reliable source that contains the individual's name and date of birth that is used to verify that the name and date of birth are those of the individual, or

~~(A)~~(C) Information that contains the individual's name and confirms that they have a deposit account or a credit card [if such use of the card is not prohibited by the applicable provincial or territorial law], passport or similar record; or other loan amount with a financial institution that is used to verify that information.

(b) For the purposes of clauses (6)(a)(iii)(A) to (C), the information referred to must be from different sources, and the individual, lawyer and agent cannot be a source.

(c) To verify the identity of an individual who is under 12 years of age, the lawyer must verify the identity of one of their parents or their guardian.

(d) To verify the identity of an individual who is at least 12 years of age but not more than 15 years of age, the lawyer may refer to information under clause 6(a)(iii)(A) that contains the name and address of one of the individual's parents or their guardian and verifying that the address is that of the individual.

~~(a)~~(e) if the client or third party is an organization such as a corporation or society that is created or registered pursuant to legislative authority, a written confirmation from a government registry as to the existence, name and address of the organization, including the names of its directors, where applicable, such as

- (i) ~~(i)~~—a certificate of corporate status issued by a public body,
- (ii) ~~(ii)~~—a copy obtained from a public body of a record that the organization is required to file annually under applicable legislation, or
- (iii) a copy of a similar record obtained from a public body that confirms the organization's existence; and

~~(b)(f)~~ ~~(c)~~ if the client or third party is an organization, other than a corporation or society, that is not registered in any government registry, such as a trust or partnership, a copy of the organization's constituting documents, such as a trust or partnership agreement, articles of association, or any other similar record that confirms its existence as an organization.

Requirement to Identify Directors, Shareholders and Owners

~~(3)~~

(7) When a lawyer is engaged in or gives instructions in respect of any of the activities in section 4 for a client or third party that is an organization referred to in ~~subsection paragraph (2)(b)(6)(e)~~ or ~~(cf)~~, the lawyer ~~shall make reasonable efforts to~~ must

(a) obtain and ~~if obtained,~~ record, with the applicable date,

~~(a)~~ the ~~name and occupation~~ names of all directors of the organization, other than an organization that is a securities dealer; and

(b) make reasonable efforts to obtain, and if obtained, record with the applicable date,

~~(b)~~ (i) the ~~name, address~~ names and ~~occupation~~ addresses of all persons who own, directly or indirectly, 25 per cent or more of the organization or of the shares of the organization; and

~~(5)~~ (ii) the names and addresses of all trustees and ~~shall include~~

~~(a)~~ the name, professional all known beneficiaries and address ~~settlers~~ of the ~~person providing the attestation;~~

~~(c)~~ (b) ~~the signature of the person providing the attestation;~~ trust, and

~~(d)~~ (c) ~~(iii)~~ in all cases, information ~~establishing the type ownership, control and number~~ structure of the ~~identifying document provided by the client, third party or instructing individual(s) organization.~~

(68) ~~For~~ A lawyer must take reasonable measures to confirm the ~~purpose~~

~~the accuracy of the information obtained under subsection (4), a guarantor must be a person employed in one of the following occupations in Canada: 7).~~

- ~~(a) — dentist;~~
- ~~(b) — medical doctor;~~
- ~~(c) — chiropractor;~~
- ~~(d) — judge;~~
- ~~(e) — magistrate;~~
- ~~(f) — lawyer;~~
- ~~(g) — notary (in Quebec);~~
- ~~(h) — notary public;~~
- ~~(i) — optometrist;~~
- ~~(j) — pharmacist;~~
- ~~(k) — professional accountant (APA [Accredited Public Accountant], CA [Chartered Accountant], CGA [Certified General Accountant], CMA [Certified Management Accountant], PA [Public Accountant] or RPA [Registered Public Accountant]);~~
- ~~(l) — professional engineer (P.Eng. [Professional Engineer, in a province other than Quebec] or Eng. [Engineer, in Quebec]);~~
- ~~(m) — veterinarian;~~
- ~~(n) — peace officer;~~
- ~~(o) — paralegal licensee in Ontario;~~
- ~~(p) — nurse; or~~
- ~~(q) — school principal.~~

Use of Agent

~~(79) A lawyer may, and where an individual client, third party or individual~~

~~described in s. 3 clause (f)(ii) is not physically present and is outside of Canada, shall, rely on an agent~~ must keep a record, with the applicable date(s), that sets out

(a) the efforts made under paragraph 7(b), and

(b) information obtained and the measures taken to confirm the accuracy of that information obtained under section (7).

(10) If a lawyer is not able to obtain the information described referred to in subsection (2) to verify the person's7) or to confirm that accuracy of that information in accordance with subsection (8), the lawyer must

(a) take reasonable measures to ascertain the identity, which may include, where applicable, an attestation described in of the most senior managing officer of the organization; and

(b) determine whether

(i) the client's information in respect of their activities,

(ii) the client's information in respect of the source of the funds described in section 4, and

(iii) the client's instructions in respect of the transaction

are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule;

(c) assess whether there is a risk that the lawyer may be assisting in or encouraging fraud or other illegal conduct; and

(d) keep a record, with the applicable date, of the results of the determination and assessment under paragraphs (b) and (c).- treat the activities in respect of that organization as requiring ongoing monitoring and if necessary take the steps such monitoring may require, as described in sections 10 of this section, provided the lawyer and the agent have an agreement or arrangement in writingRule.

~~for this purpose.~~

~~(a) A lawyer who enters into an agreement or arrangement referred to in subsection (7) shall obtain from the agent the~~

~~information obtained by the agent under that agreement or arrangement.~~

Timing of Verification for Individuals

(11) A lawyer ~~shall~~must verify the identity of

- (a) a client who is an individual, and
- (b) the individual(s) authorized to provide and giving instructions on behalf of an organization with respect to the matter for which the lawyer is retained,

upon engaging in or giving instructions in respect of any of the activities described in section 4.

(12) Where a lawyer has verified the identity of an individual, the lawyer is not required to subsequently verify that same identity ~~if the lawyer recognizes that person~~unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Timing of Verification for Organizations

(13) A lawyer ~~shall~~must verify the identity of a client that is an organization ~~within 60 days of upon~~ engaging in or giving instructions in respect of any of the activities described in section 4-, but in any event no later than 30 days thereafter.

(14) Where the lawyer has verified the identity of a client that is an organization and obtained information pursuant to subsection ~~6(3(7))~~, the lawyer is not required to subsequently verify that identity or obtain that information, unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Record keeping and retention

7. (1) A lawyer ~~shall~~must obtain and retain a copy of every document used to verify the identity of any individual or organization for the purposes of ~~sections~~subsection 6(1).

- (2) The documents referred to in subsection (1) may be kept in a

machine-readable or electronic form, if a paper copy can be readily produced from it.

(3) A lawyer ~~shall~~must retain a record of the information , with the applicable date, and any documents obtained for the purposes of ~~sections 3~~section 3, subsection 6(7) and ~~6(3)~~subsection 10(2) and copies of all documents received for the purposes of ~~sections~~subsection 6(1) for the longer of

- (a) ~~(a)~~ the duration of the lawyer and client relationship and for as long as is necessary for the purpose of providing service to the client, and
- (b) ~~(b)~~ a period of at least six years following completion of the work for which the lawyer was retained.

Application

8. Sections 2 through 7 of this Rule do not apply to matters in respect of which a lawyer was retained before this Rule comes into force but they do apply to all matters for which he or she is retained after that time regardless of whether the client is a new or existing client.

Criminal activity, duty to withdraw at time of taking information

9. (1) If in the course of obtaining the information and taking the steps required in ~~sections~~section 3 and subsections 6(1), ~~(37)~~ or (10), a lawyer knows or ought to know that he or she is or would be assisting a client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.

(2) This section applies to all matters, including new matters for existing clients, for which a lawyer is retained after this Rule comes into force.

Criminal activity, duty

Monitoring

10. During a retainer with a client in which the lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, the lawyer must:

(1) monitor on a periodic basis the professional business relationship with the client for the purposes of:

(a) determining whether

(i) the client's information in respect of their activities,

(ii) the client's information in respect of the source of the funds described in section 4, and

(iii) the client's instructions in respect of transactions

are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule, and

(b) assessing whether there is a risk that the lawyer may be assisting in or encouraging dishonesty, fraud, crime or other illegal conduct; and

(2) keep a record, with the applicable date, of the measures taken and the information obtained with respect to the requirements of paragraph (1)(a) above.

Duty to Withdraw after being retained

40.

11. (1) If while retained by a client, including when taking the steps required in section 10, a lawyer knows or ought to know that he or she is or would be assisting the client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.

Application

(2) This section applies to all matters for which a lawyer was retained before this Rule comes into force and to all matters for which he or she is retained after that time.

MODEL TRUST ACCOUNTING RULE

Definitions

“money” includes cash, cheques, drafts, credit card transactions, post office orders, express and bank money orders, and electronic transfer of deposits at financial institutions

1. A lawyer must pay into and withdraw from, or permit the payment into or withdrawal from, a trust account only money that is directly related to legal services that the lawyer or the lawyer’s law firm is providing.
2. A lawyer must pay out money held in a trust account as soon as practicable upon completion of the legal services to which the money relates.



Anti-Money Laundering and Terrorist Financing Working Group

Guidance for the Legal Profession

Your Professional Responsibility to Avoid Facilitating or Participating in Money Laundering and Terrorist Financing

February 19, 2019

Table of Contents

Chapter 1: About This Guidance	1
Chapter 2: Understanding the Problem	3
What is Money Laundering?	3
What is Terrorist Financing?	4
Chapter 3: Identifying and Verifying the Identity of Clients	5
Background to the Client Identification and Verification Rule	5
Guidance to the Client Identification and Verification Rule	6
Exemptions.....	6
Identification Requirements	7
Identifying Individuals	7
Identifying Organizations	7
Clients Acting For, or Representing, Third Parties	7
Verifying the Identity of Individuals.....	8
Government-issued Documentation	8
Credit Files	8
The Dual Process Method	9
Verifying the Identity of Children	10
Use of an Agent	10
Timing for Verifying the Identity of Individual Clients	11
Verifying the Identity of Organizations	12
Ascertaining the Beneficial Ownership of an Organization	12
Timing for Verifying the Identity of Organizations	15
Information on the Source of Client Funds	15
Monitoring the Relationship	16
Record-keeping and Retention	17
Duty to Withdraw Representation	17
Chapter 4: Limitations on Accepting Cash from Clients or Third Parties	18
The “No Cash” Rule	18
The \$7500 Threshold	18
Foreign Currency	19
Application of the Rule and Exceptions	19
Suggestions for Implementing the Rule in Your Workplace	20
Chapter 5: Proper Use of Your Trust Account	21
Background to the New Trust Accounting Rule	21
Features of the Model Trust Accounting Rule	22
Appendix A: Examples of Acceptable Photo Identification Documents	23
Appendix B: Examples of Reliable Sources of Information Under the Dual Process Method to Identify an Individual	24
Appendix C: Additional Resources	27
Canada	27
United States	27
International	27



Chapter 1: About This Guidance

Money laundering and terrorist financing, both offences under the *Criminal Code*, are on the rise in Canada. Because of the risks posed by money laundering and terrorist financing, Canada has adopted a comprehensive federal legislative regime to prevent these crimes through the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (“PCMLTFA”) requiring designated individuals and institutions to collect and report to a federal government agency¹ information about financial transactions of their clients, including large cash and suspicious financial transactions. Money laundering and terrorist financing affect us all, and the Canadian government makes serious efforts to prevent and prosecute these criminal acts.

Like all people in Canada, legal professionals² are subject to the *Criminal Code*, but they are exempted from the federal legislative regime under the PCMLTFA due to constitutional principles that protect the rights of clients and the obligations of legal professionals within their confidential relationships. The PCMLTFA was originally applicable to lawyers and Quebec notaries; this led to litigation launched by the Federation of Law Societies of Canada (the “Federation”) and the Law Society of British Columbia, supported by the Canadian Bar Association, challenging the constitutionality of the legislation. The Supreme Court of Canada subsequently recognized that the provisions in the legislation requiring legal counsel to collect and retain information about their clients and their financial transactions and provide that information to government on demand, with expansive government powers to search law offices, provided inadequate protection for solicitor-client privilege and violated the *Canadian Charter of Rights and Freedoms*.³ However, the legal profession must comply with significant, corresponding obligations to ensure they are not facilitating money-laundering and terrorist financing. These obligations are imposed on legal professionals through the regulatory regimes of Canadian law societies.

Lawyers, Quebec notaries, and paralegals in Ontario are obligated, amongst other duties, to identify and verify the identity of clients, to comply with limits on the amount of cash they may accept, to ensure that trust accounts are used only for the direct purpose of providing legal services, and to withdraw from representing a client if they know, or ought to know, that they would be assisting in criminal activity if they continue the representation. In this sense, the responsibilities of legal professionals go beyond the reporting and other duties of other professions and institutions in Canada under the PCMLTFA.

This Guidance, prepared by the Federation on behalf of all Canadian law societies, describes the responsibilities of Canada’s legal professions to ensure they are not facilitating money laundering and terrorist financing. It describes the context for money laundering and terrorist financing in Canada and the sources of the responsibilities to avoid it. The detailed Guidance, which includes red flags and real-life examples, sets out the components of the legal professional’s duties as contained in updated Model Rules approved on October 19, 2018 by the Federation, for adoption by all Canadian law societies. Additional resources appear at the end of the Guidance, and it is anticipated that over time, more will be added to this section for the benefit of legal professionals.

¹ The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

² In this Guidance, the term “legal professionals” includes lawyers, Quebec notaries and licensed paralegals in Ontario.

³ *Canada (Attorney General) v. Federation of Law Societies of Canada*, [2015] 1 SCR 401, 2015 SCC 7 (CanLII).

Avoiding participation in money laundering and terrorist financing is rooted in knowing your client: their identity, their financial dealings in relation to your retainer, and any risks arising from your professional business relationship with them. When working with corporate clients, knowing your client means taking additional steps to ascertain ownership and control of the corporation, and routinely assessing the accuracy of your knowledge about them. Not facilitating money laundering and terrorist financing also means refusing to accept, except in limited circumstances, more than \$7,500 in cash from clients or prospective clients. Finally, the fight against money laundering and terrorist financing requires you to be vigilant and exercise judgment about the use of your trust accounts, pursuant to established parameters.

Law societies take their mandate to regulate the legal profession in the public interest seriously. The rules and regulations implemented by provincial and territorial law societies, based on the Federation's Model Rules, exist to address the conduct of legal professionals, and to prevent them from unwitting involvement in money laundering or terrorist financing. Legal professionals are also required to abide by comprehensive rules of professional conduct that include provisions prohibiting them from knowingly assisting in or encouraging any unlawful conduct. Measures to ensure that legal professionals maintain appropriate practice management systems and comply with law society regulations include annual reporting obligations, practice reviews and financial audits. Law societies also have extensive investigatory and disciplinary powers that include the ability to impose penalties up to and including disbarment when members fail to abide by law society rules and regulations. Lawyers, Ontario paralegals, and Quebec notaries who wittingly participate in criminal activity are, of course, subject to criminal charges and sanctions.

While this Guidance discusses the legal profession's vulnerabilities related to money laundering and terrorist financing, these same vulnerabilities could lead to the profession's unwitting participation in other types of fraud or crime. It is important to understand that the duties and responsibilities contained in the Model Rules reflect the unique position of legal professionals in helping the public with their legal needs and in ensuring compliance with the law. By adhering to these fundamental principles, the legal profession helps to prevent all crime, and to maintain public trust in the justice system. Similarly, the Model Rules protect the right of citizens to independent legal counsel, and ensure that counsel can continue to protect the client's privilege.

Chapter 2: Understanding The Problem

Money laundering and the financing of terrorist activities affect us all. When criminals launder their illicit funds through the purchase and sale of properties, it can inflate the selling prices, making it unaffordable for community members to purchase homes. When criminals launder their dirty funds through front companies and sell products at significantly lower prices, legitimate businesses may be unable to compete. When large amounts of criminal proceeds are invested into our economy, currency exchange and interest rates can become volatile. The consequences of money laundering and terrorist financing are vast and significant – it is incumbent on each of us to prevent these criminal offences.

Legal professionals are perceived as “gatekeepers” within money laundering and terrorist financing systems because of our unique role in facilitating financial transactions. Specifically, legal professionals may be used to:

- give an appearance of legitimacy to a criminal transaction;
- facilitate money laundering through the creation of a company or trust, and/or the purchase and sale of property; and
- eliminate the trail of funds back to a criminal through the use of a professional trust account.⁴

Because of the role they play in facilitating transactions, and the fact that communications for the purpose of obtaining legal advice are protected by solicitor-client privilege, legal professionals may be targeted by criminals. Legal professionals should thus be able to determine the potential money laundering or terrorist financing risks posed by a client, as well as the risks presented by the context of their services. Without such risk-based awareness, legal professionals may find themselves participating in criminal activity, whether knowingly, recklessly, or unintentionally.

What is Money Laundering?

The Financial Action Task Force (“FATF”), an international, intra-governmental body combatting money laundering and terrorist financing, defines money laundering as the processing of criminal proceeds to disguise their illegal origin.⁵ The Criminal Code similarly defines money laundering as the transfer, use, or delivery of property or proceeds with the intent to conceal or convert the property or proceeds, knowing that they were derived from criminal activity.⁶

Criminal proceeds are typically laundered through a three-stage process: placement, layering, and integration. In the placement stage, the launderer introduces the illegal profits into the financial system (for example, by depositing cash with financial institutions changing currency at currency exchanges, or depositing funds into lawyers trust accounts). In the layering stage, the launderer

⁴ The International Bar Association, the American Bar Association, and the Council of Bars and Law Societies of Europe, “A Lawyer’s Guide to Detecting and Preventing Money Laundering,” October 2014 at p. 24, available online: <https://www.anti-moneylaundering.org/AboutAML.aspx#TheGuide>

⁵ Financial Action Task Force, “What is Money Laundering?” online: <http://www.fatf-gafi.org/faq/moneylaundering/>

⁶ Section 462.31(1) (“Laundering proceeds of crime”), *Criminal Code*, R.S.C. 1985, c. C-46.

engages in a series of transactions to distance the funds from their source (for example, by creating trusts or shell companies, buying securities, or buying real estate). Finally, in the integration stage, the launderer integrates the funds into the legitimate economy, i.e. by investment into real estate or business ventures.⁷ Money launderers may try to involve lawyers at any of these stages.

The FATF notes that money-laundering proceeds can be generated through a wide range of illegal activity, including illegal arms sales, smuggling, embezzlement, insider trading, and computer fraud schemes.⁸ In the Canadian context, a 2015 Department of Finance report identified 21 profit-oriented crimes associated with money-laundering.⁹ Those identified as posing a very high threat of money laundering include capital markets fraud, drug trafficking, mortgage fraud, and tobacco smuggling and trafficking. A high threat rating was given to such crimes as currency counterfeiting, human trafficking, illegal gambling, and robbery and theft. Experts have noted that those involved in such crimes range from the “unsophisticated, criminally inclined individuals, including petty criminals and street gang members, to criminalized professionals and organized crime groups.”¹⁰

What is Terrorist Financing?

The FATF does not specifically define the term “terrorist financing.” Instead, they urge states to adopt the United Nations International Convention for the Suppression of the Financing of Terrorism (1999), which prohibits any person from providing or collecting funds in order to carry out an offence as defined in related United Nations treaties, or any other act intended to cause death or serious bodily injury, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.¹¹

Sections 83.02-83.04 of the Criminal Code define the terrorism financing offences. Collectively they prohibit the provision, collection and use of property to facilitate or carry out any terrorist activity.¹² In a 2015 report, the Department of Finance indicated that terrorist financing activities in Canada may include the payment of travel expenses, the procurement of goods, transferring funds to international locations through banks and other financial entities and the smuggling of bulk cash across borders.¹³

The FATF notes that terrorist financing can be challenging to detect for legal professionals without guidance on relevant typologies or unless acting on specific intelligence provided by the relevant authorities.¹⁴ Because of this, legal professionals should consider consulting the reports regularly published by Canada’s Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) on terrorist financing trends and typologies.¹⁵

⁷ What is Money Laundering? *supra* note 2.

⁸ *Ibid.*

⁹ Finance Canada, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, 2015 at p. 19, online: <https://www.fin.gc.ca/pub/mltf-rpcfat/mltf-rpcfat-eng.pdf>

¹⁰ *Ibid.*, at p. 18.

¹¹ International Convention for the Suppression of the Financing of Terrorism, as adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999, online: <http://www.un.org/law/cod/finterr.htm>

¹² Section 83.01(1) (“definition of terrorist activity”), *Criminal Code*, R.S.C. 1985, c. C-46.

¹³ *Supra* note 5 at p. 27.

¹⁴ Financial Action Task Force, “Risk-Based Approach Guidance for Legal Professionals,” 23 October 2008 at p. 42, available online: <http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf>

¹⁵ FINTRAC Typologies and Trends Reports, available online: <http://www.fintrac-canafe.gc.ca/publications/typologies/1-eng.asp>

Chapter 3: Identifying and Verifying the Identity of Clients

Background to the Client Identification and Verification Rule

When retained to provide legal services, you must acquire basic knowledge about your clients and their financial dealings. The Model Rule requirements may be fulfilled by you, or any partner, associate or employee at your firm.

Legal professionals must identify each client, with limited exemptions. Identification is the process of obtaining and recording basic information about the client. Identification requirements differ slightly depending on whether your client is an individual or an organization. If your client is acting for or representing a third party, identifying information about that third party also must be obtained.

Identification and verification are two separate but related concepts. When you engage in or give instructions in respect of receiving, paying or transferring funds on behalf of a client you must also verify your client's identity. Verification is the process of obtaining information to confirm that the client is who or what they say they are. This involves reviewing independent source document(s) or information and comparing it to the actual client. The identity of a third party on whose behalf the client is acting must also be verified. You must also determine the source of the funds being dealt with.

For clients that are corporations, societies, or unregistered organizations, you are required to verify the identity of the person who instructs you on behalf of the organization. You are also required to make reasonable efforts to obtain information about beneficial owners – persons who own, directly or indirectly, 25% or more of the organization. In the event you are unable to do so, the Model Rule asks you to exercise diligence in determining and assessing potential risks associated with those clients.

Overall, the client identification and verification requirements, as stated in section 2 of the Model Rule, are part of your obligation to know your client, and ensure that you understand the intent and purpose of the legal services for which you have been retained. Reference should be made to Model Code of Professional Conduct Rules 3.1-2 (Competence), 3.2-1 (Quality of Service), 3.2-7 (Dishonesty, Fraud by Client or Others), and 3.2-8 (Dishonesty, Fraud when Client an Organization) including their respective commentaries, which elaborate on the standards expected of legal professionals in relationships with clients. The competent legal professional, as defined in Rule 3.1-1 is one who, amongst other things, investigates facts, identifies issues, ascertains client objectives, considers possible options, and develops and advises the client on appropriate courses of action. A legal professional's obligation to provide the requisite quality of service mirrors competent service - this includes communicating effectively with the client and ensuring, where appropriate, that all instructions are in writing or confirmed in writing.

Model Code Rule 3.2-7 and section 11(1) of the Client Identification and Verification Model Rule prohibit legal professionals from knowingly assisting in any illegal conduct or doing or omitting to do anything the legal professional knows or ought to know will assist with a crime. The prohibition means being vigilant when engaged in services involving financial transactions. When suspicions or doubts arise about whether the activities of a legal professional might be assisting in crime or fraud, the obligation is to make reasonable inquiries to obtain information about the subject matter and

objectives of the retainer and record it, and to consider whether withdrawal is required. By complying with the Model Rule and the Model Code, you will provide the appropriate services to clients, managing both their expectations and your duties, in a responsible and professional way.¹⁶

Guidance to the Client Identification and Verification Rule

Exemptions

Not all client relationships are captured by the Model Rule. For example, if you only provide legal services to your employer as in-house or corporate counsel, you are exempt from the requirements to identify the client and to verify the client's identity. Similarly, if you provide legal services through a duty counsel program you are exempted from the verification requirements, except when engaging in, or giving instructions in respect of, the receiving, paying, or transferring of funds. You also are exempted if you are engaged to act as an agent by another legal professional, or when another legal professional has referred a matter to you, provided the other legal professional has complied with the identification and verification requirements.

Other exemptions apply when the funds are from certain sources. The Model Rule does not apply to funds received by a legal professional when those funds are:

- from the trust account of another legal professional;
- paid or received to pay a fine, penalty or bail or for professional fees; disbursements and expenses;
- paid by or to a financial institution, public body, or reporting issuer; or
- an electronic transfer of funds (EFT).

The Model Rule's definition of "electronic funds transfer" specifies that only EFTs conducted by and received at financial institutions headquartered and operating in a country that is a member of the FATF is covered by the exemption. Further, neither the sending nor receiving account holders may handle or transfer the funds. The Model Rule requires that the EFT transmission records contain a reference number, the date, transfer amount, currency, and the names of the sending and receiving account holders and the financial institutions conducting and receiving the EFT. This exemption will likely be subject to future review, as current developments or changes in the financial landscape may warrant a change in this approach.

The previous version of the Model Rule had exemptions for funds paid pursuant to a court order and paid or received pursuant to the settlement of any legal or administrative proceedings. Those exemptions have been removed. In the common situation, the funds in these circumstances are paid from one party to another and to the extent the funds flow through the legal professional's trust account, there is a risk that these types of payments could be in aid of schemes to launder money. To the extent that funds are paid into court as seized funds under forfeiture legislation and then released by the court pursuant to judicial order, it is suggested that these funds would fall under the exemption relating to a law enforcement agency or other public official acting in their official capacity.

¹⁶ This portion of the Guidance is informed by guidance published by FINTRAC, found at: <http://www.fintrac-canafe.gc.ca/guidance-directives/1-eng.asp>

Identification Requirements

You must identify all clients regardless of the nature of the legal services you are providing, subject to limited exemptions. You are not required to identify your client when providing services to your employer as in-house counsel, when acting as an agent for another legal professional, or when providing legal services to a client referred by another legal professional who has already identified the client. The identification requirements also do not apply when you are acting as duty counsel.

Identifying Individuals

When retained by an individual, you must identify the client and record the client's full name, home address and home telephone number, occupation(s), and the address and telephone number of the client's place of work or employment.

Identifying Organizations

When retained by an organization, you must identify it by recording its name, business address and business telephone number, incorporation or business incorporation number, the general nature of its type of business or, and the name, position, and contact information of the individual who is authorized to give you instructions on behalf of the organization with respect to the matter for which you are retained.

Clients Acting For, or Representing, Third Parties

In some circumstances, you may be retained by a client who is acting for, or representing, a third party. In such cases, you must identify the third party, whether it is an individual or an organization.

A third party is a person or organization who instructs another person or organization to conduct an activity or financial transaction on their behalf. When determining whether a third party is giving instructions, it is not about who owns or benefits from the funds, or who is carrying out the transaction or activity, but rather about who gives the instructions to handle the funds or conduct a transaction or particular activity. Ask questions to find out if someone other than your client is pulling the strings. If you determine that the individual or organization who engages you is acting on someone else's instructions, that someone else is the third party. Determine the relationship between the client and the third party.

Verifying the Identity of Individuals

The following sections describe the options available to you when you are required to verify the identity of individual clients or third parties. Verification of identity is required when in the course of providing legal services, you engage in or give instructions in respect of the receiving, paying or transferring of “funds”. Note that “funds” is widely defined and would include the transfer of securities. While much of this section describes how to verify a client in a face-to-face situation, you may choose instead to use an agent as described later in this section.

Government-issued Documentation

You may rely on a valid, original and current federal, provincial or territorial government-issued document containing the individual’s name and photograph. See Appendix A for examples of acceptable government-issued documents. A foreign government issued photo identification document is acceptable if it is equivalent to a Canadian issued photo identification document listed in Appendix A. Note, however, that photo identification documents issued by any municipal government, whether Canadian or foreign, are not acceptable.

You or your agent must view the original document in the presence of the individual in order to compare them with their photo. The photo identification document must show the individual’s name, include a photo of the individual, and have a unique identifier number. It is not acceptable to view photo identification online, through a video conference or through any virtual type of application; nor is a copy or a digitally scanned image of the photo identification acceptable.

Credit Files

Alternatively, you can verify an individual’s identity by relying on information that is in their credit file if that file is located in Canada and has been in existence for at least three years. The information in the credit file must match the name, date of birth and address provided by the individual. If any of the information does not match, you must use another method to verify the individual’s identity.

Note that a credit assessment is not needed to identify an individual through a credit file. Equifax Canada and TransUnion Canada are Canadian credit bureaus that provide credit file information for identification purposes.

To verify an individual’s identity using information in their credit file, you must obtain the information directly from a Canadian credit bureau or a third-party vendor authorized by a Canadian credit bureau to provide Canadian credit information. You cannot rely on a copy of the credit file if provided by the individual. It is acceptable, however, to use an automated system to match the individual’s information with the credit file information.

To rely on a credit file search, the search must be conducted at the time of verifying the individual’s identity. An historical credit file is not acceptable. To be acceptable as a single source for verification of identity, the credit file must match the name, address, and date of birth that the individual provided, be from Canada, and have been existence for at least three years.

The individual does not need to be physically present at the time you verify their identity through a credit file.

The Dual Process Method

You can also use the dual process method to verify a client's identity, by relying on any two of:

- information from a reliable source that contains the individual's name and address;
- information from a reliable source that contains the individual's name and date of birth; and/or,
- information containing the individual's name that confirms they have a deposit account or credit card or other loan amount with a financial institution.

If using the dual process method, the information referred to must be from different sources. Neither the client (or individual instructing on behalf of the client), nor the legal professional (or the professional's agent) may be a source. The information may be found in documents from these sources or may be information that these sources are able to provide. Information refers to facts provided or learned about an individual and can come from various places, in contrast to a document, which refers to an official record that is either written, printed or electronic that provides evidence or facts.

If a document is used, you or your agent must view a valid, original and current document. Original documents do not include those that have been photocopied, faxed or digitally scanned. If information is used, it must be valid and current. Information found through social media is not acceptable.

The individual does not need to be physically present at the time you verify their identity through the dual process method.

A reliable source is an originator or issuer of information that you trust to verify the identity of the client. To be considered reliable under the Model Rule, the source should be well known and considered reputable. The source providing the information cannot be you, your client, or the individual who is being identified; the source must be independent. For example, reliable sources can be the federal, provincial, territorial and municipal levels of government, Crown corporations, financial entities or utility providers.

If a document is used as part of the dual process method, you must ensure that you see the original paper or electronic document, and not a copy. The original document is the one that the individual received or obtained from the issuer either through posted mail or electronically. For example, an original paper document can be a utility statement mailed to an individual by the utility provider, and it can also be a document that the individual received through email or by downloading it directly from the issuer's website. The document must appear to be valid and unaltered in order to be acceptable; if any information has been redacted, it is not acceptable.

An individual can email you the original electronic document they received or downloaded, show you the document on their electronic device (for example, a smartphone, tablet, or laptop), print the electronic document received or downloaded from the issuer, or show it to you in the original

format such as .pdf (Adobe) or .xps (Microsoft viewer). In practical terms, this means that an individual can:

- show you their original paper utility statement in person or by posted mail;
- email or show you on their electronic device an electronic utility statement downloaded directly from the issuer's website;
- print and show you the statement they downloaded from the issuer; or
- email or show you on their electronic device a mortgage statement received by email from the issuer.

See Appendix B for examples of information and documents that can be used for the dual process method of verifying identity.

Verifying the Identity of Children

The Model Rule requires you to take different steps to verify the identity of an individual who is a child.

If verifying the identity of an individual who is under 12 years of age, you must verify the identity of one of the child's parents or guardians.

If verifying the identity of an individual client who is at least 12 years of age but not more than 15 years of age, you can rely on any two of:

- information from a reliable source that contains the individual's parent or guardian's name and address;
- information from a reliable source that contains the individual's parent or guardian's name and date of birth; and/or,
- information containing the individual's parent or guardian's name that confirms the parent or guardian has a deposit account, credit card, or other loan amount with a financial institution.

If that is not possible, you can rely on information from a reliable source that contains the name and address of the child's parent or guardian and a second reliable source that contains the child's name and date of birth. For example, if the child has a passport, that can be used to ascertain their identity directly; if not, you can rely on the parent's driver's license to verify their common address, and use the child's birth certificate to verify the child's name and date of birth.

Use of an Agent

You may rely on an agent to verify the identity of an individual, including in circumstances where the individual is not physically present in Canada.

An agent can be utilized at any time. You may choose to use an agent if the client or third party is elsewhere in Canada and the method of verification is the use of a federal, provincial or territorial government-issued document containing the client's name and photograph, which must be provided in the client's presence. Other methods, as indicated above, do not require the individual's physical presence and as such an agent may not be necessary. If the client or third party is not physically present in Canada, an agent must be relied upon to verify the individual's identity.

The Model Rule requires that you and your agent have an express agreement or arrangement in writing for such purpose. The agreement need not be in any particular form, and it is up to you to decide on the level of formality required. It may take the form of a letter or email, for example. The agreement should set out in sufficient detail the purpose of the agreement and the expectations of the agent. As the responsibility to verify identity is yours, you – not the client or third party – must choose and retain the agent.

The identity verification information provided by the agent should include the information that you would have obtained and documented had you verified identity through one of the methods described above. As such, when using an agent, your records should include, through the agreement itself and the report from the agent:

- the full name of the agent who verified the individual's identity;
- the agent's status or occupation and business address;
- the client identification method the agent used;
- copies of the information and documents obtained by the agent to verify the individual's identity; and,
- the date on which the agent verified the individual's identity.

You should also note the date you received the verification information from the agent, as this relates to the currency of the identification information that you use and the time within which the verification must occur under the Model Rule.

The information on the client's identity that you obtain from the agent must match what the individual has provided to you when you obtained their basic identification information. You must satisfy yourself that the information is valid (authentic and unaltered) and current (not expired) and that your agent verified the individual client's identity through the methods prescribed by the Model Rule. You may also rely on an agent's previous verification of an individual client if the agent was, at the time that they verified the identity, acting in their own capacity or acting as an agent under an agreement or arrangement in writing with another legal professional who is similarly required to verify identity under the Model Rule.

The Model Rule does not specify who may act as an agent. However, given the responsibilities of the agent, you should ensure that the person engaged is reputable, can be relied upon to understand what is required, can capably carry out the required work to verify identity and will provide the information they have obtained as required under the Model Rule.

Timing for Verifying the Identity of Individual Clients

You are required to verify the identity of an individual (client or third party) upon being retained to engage in, or give instructions in respect of, receiving, paying or transferring funds other than an electronic funds transfer. You are not subsequently required to verify that individual's identity unless you have reason to believe the information, or the accuracy of it, has changed.

Verifying the Identity of Organizations

When retained by an organization to engage in, or give instructions in respect of, receiving, paying or transferring funds other than an electronic funds transfer, you must take certain specified steps to verify the client's identity. These additional requirements apply to all organizations with the exception of "financial institutions", "public bodies", and "reporting issuers", as defined in the Model Rule. The requirements to verify the identity of an organization include the requirement to verify the identity of the individual(s) authorized to give instructions on behalf of the organization for the matter for which you are retained.

If retained by a client who is acting for, or representing, a third party that is an organization, you are required to obtain information about that organization, and if applicable, verify the third party's identity, pursuant to your obligation to verify information about clients that are organizations.

In verifying an organization's identity, you have a few options available to you as outlined in the Model Rule. If the organization is created or registered pursuant to legislative authority, you may rely on written confirmation from a government registry as to the existence, name and address of the organization. Documents that you can rely on to confirm the existence of a corporation are: the corporation's certificate of corporate status; a record filed annually under provincial securities legislation; or any other record that confirms the corporation's existence, such as the corporation's published annual report signed by an independent audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government. If the organization is not registered in any government registry, you may rely on documents that establish or create the organization; you can rely on a partnership agreement, articles of association, or any other similar record that confirms the entity's existence. You cannot rely on an agent to verify the identity of an organization.

If an electronic version of a record is used to verify the existence of an organization, you must keep a record of the:

- corporation's registration number or the organization's registration number;
- type of record referred to; and
- source of the electronic version of the record.

For example, a corporation's name and address and the names of its directors can be obtained from a provincial or federal database such as the Corporations Canada database, which is accessible from Innovation, [Innovation, Science and Economic Development Canada](#) website. This information may also be accessed through a subscription to a corporation searching and registration service.

Ascertaining the Beneficial Ownership of an Organization

Except in the case of an organization that is a securities dealer, you must obtain and record, with the applicable date, the names of all directors of the organization. You are also required to make reasonable efforts to obtain information about the beneficial owners of the organization and about the control and structure of the organization. Identifying beneficial ownership is important in order to remove anonymity and identify the actual individuals behind a transaction. The concealment of the beneficial ownership information of accounts, businesses and transactions (i.e. the persons who own 25% or more) is a technique used in money laundering and terrorist activity financing schemes.

Collection and confirmation of beneficial ownership information is an important step in knowing the client and ensuring that the lawyer's work on the transaction is not in aid of money laundering and terrorist financing activity.

Beneficial owners are the actual individuals who are the trustees or known beneficiaries and settlors of a trust, or those who directly or indirectly own or control 25% or more of an organization, such as a corporation, trust or partnership. Another organization cannot be considered the ultimate beneficial owner; the information you must try to obtain is the identity of the actual individuals who are the owners or controllers of the other organization. The purpose of this requirement is for you to obtain sufficient information about the organization's structure so that you know who effectively owns and controls the organization.

The Rule asks you to meet the standard of reasonable efforts to obtain the information. This means applying sound, sensible judgment. Reasonable efforts include searching through as many levels of information as necessary to identify those individuals. In making reasonable efforts to ascertain beneficial ownership, it is important to understand that the names found on legal documentation may not represent the actual owners of an organization. You must exercise judgment in discerning the reasonable efforts that are appropriate for each distinct situation to confirm the accuracy of information obtained, while also considering the risk associated with each situation.

For example, consider the situation where a corporation is governed by a board of directors: you must ascertain both ownership and control of the corporation. You will need to obtain information on the shareholders who own 25% or more of the organization, as they must be recorded as beneficial owners. However, you must also obtain information about the board of directors, who has control of the organization. Once you have obtained information about both shareholders and corporate directors, the Rule also requires you make reasonable efforts to confirm the accuracy of the information pertaining to both ownership and control of the organization.

You may obtain information establishing beneficial ownership, as well as the required control and structure information, from the organization, either verbally or in writing. For example, the organization can:

- provide you with official documentation;
- advise you on the beneficial ownership information, which you can then document for record-keeping purposes; or
- fill out a document that provides the information.

Where the identity of those who own and those who control an organization is not the same, you must consider the ownership and control exercised by both. It is not sufficient to identify only the owners of an organization or those who control it; you must make reasonable efforts to identify both. Remember that you are required to obtain the names and addresses of only those persons who own or control 25% or more of the organization.

If referring to documents or records, the accuracy of the beneficial ownership, as well as ownership, control and structure information related to the organization, may be confirmed by referring to records, such as the:

- Minute book;
- Securities register;
- Shareholders register;
- Articles of incorporation;
- Annual returns;
- Certificate of corporate status;
- Shareholder agreements;
- Partnership agreements; or
- Board of directors' meeting records of decisions.

It is possible for one of these documents to be used to satisfy the two distinct steps, namely to obtain the information and to confirm the accuracy of it. You can also conduct an open-source search, or consult commercially available information. In the case of a trust, the accuracy of the information can be confirmed by reviewing the trust deed, which will provide information on the ownership, control and structure of the trust.

Legal professionals should use their judgment to assess whether the documentation is appropriate. Where possible, official documents, such as a share certificate, should be used to confirm the beneficial ownership information obtained. If no official document exists to confirm accuracy, a signed attestation would be acceptable.

It may not always be possible for you to determine full information totaling 100% of beneficial ownership. For example, a corporation may have several hundred or thousands of shareholders. In these cases, your best efforts might be obtaining general information about the ownership of an organization, which may or may not include the names of the owners with a breakdown of percentages owned.

You must set out the information obtained in a dated record, along with the measures taken to try to confirm the accuracy of that information is required.

If despite your best efforts you are unable to obtain information about the directors, shareholders, and owners of the organization, you must then take reasonable measures to ascertain the identity of the most senior managing officer of the organization, and assess the organizational client's activities in the context of any risks that the transaction(s) may be part of fraudulent or illegal activity. These obligations are responsive to concerns that arise when information cannot be obtained. If the organization's structure is more opaque than transparent, this may be a warning that the organization could be facilitating criminal or other illegal activity.

In ascertaining the identity of the senior managing officer of an organization, you should be aware that this may include, but is not limited to, a director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or an individual who performs any of those functions. It may also include any other individual who reports directly to the organization's board of directors, chief executive officer or chief operating officer. In the case of a partnership, the

most senior managing officer can be one of the partners.

In the case of a trust, the senior managing officer of a trust is the trustee, that is, the person who is authorized to administer or execute on that trust. The reasonable measures standard ultimately requires you to exercise judgment about the potential risks associated with acting for an organizational client whose ownership, control or structure may not be entirely known to you. Because of this, along with ascertaining the identity of the most senior managing officer, you are also required to determine whether the client's information in respect of their activities, the client's information in respect of the source of funds, and the client's instructions in respect of the transaction are consistent with the purpose of their retainer and the information you have obtained about them. You must assess whether there is a risk that you are assisting in, or encouraging, dishonesty, fraud, crime or illegal conduct. Finally, you are obligated to keep a record, with the applicable date, of the results of these assessments.

Timing for Verifying the Identity of Organizations

The Model Rule requires you to verify the identity of an organization upon being retained to engage in, or give instructions in respect of, receiving, paying or transferring funds other than an electronic funds transfer. In no case may the verification occur more than 30 days after you have been retained. You are not subsequently required to verify that same identity unless you have reason to believe the information, or the accuracy of it, has changed.

Information on the Source of Client Funds

In addition to verifying clients' identities when engaging in, or giving instructions in respect of, receiving, paying or transferring funds on behalf of a client, legal professionals are also required to obtain information about the source of the funds relating to the retainer. This requirement applies to both individual and organizational clients.

The rule requires you to inquire about the expected source and origins of the funds related to the legal services to be provided. This may be apparent from the information obtained from the client for the retainer. In general, you should make sufficient inquiries to assess whether there is anything that suggests the proposed transaction is inconsistent with the client's apparent means, and the circumstances of the transaction.

In making this assessment, depending on the circumstances, you may wish to consider questions such as:

- Is someone other than the client providing information about the source of funds?
- Is the disclosed source consistent with the knowledge about the client's profile and activity?
- Is there anything unusual about the source of the funds in the context of the transaction?

For record-keeping purposes, you should also retain supporting documents that relate to how you determined the source of funds.



Consider these red flags about the source of funds:

- Funds are from, or are sent to, countries with high levels of secrecy;
- The client is not located near you and is asking for types of services that are not common for you to provide, or outside your area(s) of law entirely;
- The client expresses a sense of great urgency and asks you to cut corners;
- The funds received are inconsistent with the client's occupation or socio-economic profile.

Monitoring the Relationship

The Model Rule requires you to exercise vigilance about client relationships that involve the receipt, transfer, or payment of funds. As such, when retained by an individual or organizational client to engage in, or give instructions in respect of, receiving, paying or transferring funds other than an electronic funds transfer, you must monitor the professional business relationship on a periodic basis. This means that during the retainer you must periodically assess whether the client's information in respect of their activities and the source of their funds are consistent with the purpose of the retainer and the information about the client that you have obtained under the rule. You also need to assess whether there is a risk that you might be assisting in fraud or other illegal conduct. The Model Rule requires that you keep a dated record of your client monitoring measures, which may include the steps taken and any information obtained.

It may be useful to conceive of your monitoring requirement as a periodic check-in with a client with whom you have an established, long-term relationship. In other circumstances, the monitoring requirement may be triggered when your client provides you with new facts about their activities or source of funds, or when you are faced with unexpected client behavior.

You should use your discretion in defining the frequency of the monitoring. It will depend on the client, the nature of the work, the anticipated duration of the retainer and the services provided. The frequency of monitoring activities may be determined by any risks you believe arise from the retainer with the client in the context of the requirements of the Model Rule. The responsibilities are similar to those outlined in commentary to Model Code of Professional Conduct Rule 3.2-7, which set out your obligations not to engage, or to assist a client in engaging, in criminal activity.¹⁷

¹⁷ [1] A legal professional should be on guard against becoming the tool or dupe of an unscrupulous client, or of others, whether or not associated with the unscrupulous client.

[2] A legal professional should be alert to and avoid unwittingly becoming involved with a client or others engaged in criminal activities such as mortgage fraud or money laundering. Vigilance is required because the means for these and other criminal activities may be transactions for which legal professionals commonly provide services such as: establishing, purchasing or selling business entities; arranging financing for the purchase or sale or operation of business entities; arranging financing for the purchase or sale of business assets; and purchasing and selling real estate.

[3] If a legal professional has suspicions or doubts about whether he or she might be assisting a client or others in dishonesty, fraud, crime or illegal conduct, the legal professional should make reasonable inquiries to obtain information about the client or others and, in the case of the client, about the subject matter and objectives of the retainer. These should include verifying who are the legal or beneficial owners of property and business entities, verifying who has the control of business entities, and clarifying the nature and purpose of a complex or unusual transaction where the purpose is not clear. The legal professional should make a record of the results of these inquiries.

On occasion, ongoing monitoring may require taking additional, enhanced measures. These might include:

- Obtaining additional information about your client (i.e. occupation, assets, information available through a public database, Internet, etc.);
- Obtaining information on the source of funds or source of wealth of your client;
- Obtaining information on the reasons for intended or conducted transactions;
- Gathering additional documents, data or information, or taking additional steps to verify the documents obtained;
- Flagging certain activities that appear to deviate from expectations;
- Reviewing transactions against the usual processes and procedures for such transactions relevant to the legal work for which you are retained.

Record-keeping and Retention

As noted previously, the Model Rule requires you to create and maintain certain records and to date those records. This includes a record of information that identifies each client. Where the retainer with the client involves the receipt, payment or transfer of funds, you must also keep records that contain;

- Information that identifies the source of funds;
- Copies in either paper or electronic format of every document used to verify the identity of the client and any third party;
- Information and any related documents on the directors, owners, beneficial owners and trustees, as the case may be, of an organizational client;
- Information and any related documents on the ownership, control and structure of an organizational client;
- Information and any related documents that confirm the accuracy of the information on directors, owners, beneficial owners and trustees and the ownership, control and structure of an organizational client; and,
- Measures taken and information obtained respecting your monitoring of the professional business relationship with the client.

Client identification and verification of identity records, as well as your records of having taken reasonable measures to obtain beneficial ownership of an organizational client and of your monitoring responsibilities, must be kept for the duration of the client relationship, or for a period of at least six years following the completion of the work for which you were retained, whichever is longer.

Duty to Withdraw Representation

At the core of the Model Rule is the professional responsibility not to participate in, or facilitate, money laundering or terrorist financing.

You must withdraw from representation of a client if, in the course of verifying that client's identity, or monitoring your professional business relationship, you know or ought to know that you are, or would be, assisting a client in fraud or illegal conduct.

Chapter 4: Limitations on Accepting Cash from Clients or Third Parties

The "No Cash" Rule

There have been limits on amount of cash you may receive from a client since the Model Rule on Cash Transactions (known as the "No Cash" rule) was adopted in 2004. Recent amendments have been made to clarify the \$7,500 threshold for accepting cash and the exceptions to the rule. There is also a more robust definition section, explaining terms used in the rule.

The \$ 7,500 Threshold

The rule prohibits you from accepting more than \$7,500 in cash in respect of one client matter under all circumstances, with limited exception as discussed below. The \$7500 threshold applies whether you receive the money in one payment or through aggregate or instalment payments. It also applies whether the cash is received from the client or a third party providing it on behalf of the

Consider the following example:

A legal professional is acting for a personal representative of an estate who has discovered cash amongst the deceased's possessions and wants the legal professional to deposit the funds in her trust account (the legal professional under the retainer is controlling the estate funds). If the client finds \$2,000 in a safety deposit box, that may be deposited in the trust account. If the client finds an additional \$8,000, that entire amount cannot be deposited as it would be an aggregate of \$10,000. In such a circumstance it would be appropriate to advise the client to:

- open an estate account and deposit the cash into that account; or
- suggest that the client use the cash to get a bank draft payable to the legal professional's firm in trust.

Under the rule, legal professionals:

- cannot accept more than \$7,500 cash on a client matter even if there is more than one client on the file. The limit applies with respect to the client matter despite the number of clients.
- cannot accept more than \$7,500 from a client if the cash is tendered incrementally for a matter. It is, therefore, important to track receipt of cash to ensure the total received on the client matter does not exceed \$7500.
- can accept greater than \$7,500 cash from a client for three unrelated matters but only if the amount of cash provided for each individual matter is \$7,500 or less.

"Cash" is defined in the rule and includes Canadian coins or banknotes and those of other countries. Note that bank drafts, money orders, electronic or wire transfers of funds are not considered cash for the purposes of the rule.

Foreign Currency

If you are accepting cash in a foreign currency, be aware that under Section 2 of the rule the currency is deemed to be the equivalent of Canadian dollars at the official conversion rate of the Bank of Canada for the foreign currency in effect that day, or on the most recent business day preceding the day on which you receive or accept the cash if the day it is received or accepted is a holiday.

If the amount of foreign currency as converted is greater than \$7,500 you are prohibited from accepting it unless one of the exceptions applies.

As more fully discussed below, you should ensure that you and your staff are familiar with the rule, including the treatment of foreign currency.

Application of the Rule and Exceptions

It is important to understand that the rule applies not only to receiving cash from clients, but to the circumstances in which you receive cash on behalf of clients. This means that the rule applies when, on behalf of a client, you engage in or give instructions about receiving or paying funds, purchasing or selling securities, real properties or business assets or entities and transferring funds by any means. 'Funds' are defined in the rule as cash, currency, securities and negotiable instruments or other financial instruments that indicate the person's title or right to or interest in them.

There are limited exceptions to the rule limiting the cash you may receive in relation to a client matter. You may receive more than \$7500 in cash in connection with the provision of legal services

- from a financial institution or public body,
- from a peace officer, law enforcement agency or other agent of the Crown acting in his or her official capacity,
- to pay a fine, penalty, or bail, or
- for professional fees, disbursements, or expenses, provided that any refund out of such receipts is also made in cash.

Note that the requirement to refund in cash received for fees, disbursements or expenses applies only when you have received more than \$7,500 in cash. Again, "financial institution", "public body", "professional fees", "disbursements" and "expenses" are all defined terms in the rule.

The rule covers a broad range of activities. Careful consideration is required before determining that an exception applies. When accepting cash for professional fees, disbursements, expenses or bail, it would be prudent for you to:

- consider the purpose for which cash is received, and document the circumstances and any client instructions;
- ensure that the amount received for a retainer is commensurate with the services to be provided (i.e. do not accept a \$50,000 retainer for a \$5,000 matter);
- ensure that you keep appropriate records so that, if cash in excess of the limit is received for a retainer but the client later retains new counsel or the first retainer is otherwise terminated, any refund is paid in cash ; and
- ensure that appropriate accounting systems are in place to document and track the cash transactions, in particular when making a deposit of mixed cash and non-cash funds into trust; this could lead to difficulty in monitoring use.

Suggestions for Implementing the Rule in Your Workplace

The following are suggested procedures to assist in implementing the rule in your legal practice:

- Inform staff about the rule and what to do if a client unexpectedly shows up at the office with cash;
- Ensure that file opening procedures include a requirement to comply with the rule, in particular by requiring that you or your colleagues confirm each cash deposit in the trust accounts;
- Ensure that trust accounting procedures require confirmation of rule compliance before paying money out of trust;
- Appoint someone in the firm to ensure that professional and support staff keep up to date with any rule changes;
- Record any exemption from the “No Cash” rule; and
- Provide information about the rule to new and existing clients in retainer letters, on the firm website, and in mail inserts.

The rule also specifies record keeping requirements for cash transactions. Fully complying with these requirements prevents issues arising in the treatment of cash transactions in your practice.



Chapter 5: Proper Use of Your Trust Account

Background to the New Trust Accounting Rule

A new Model Rule now restricts the use of trust accounts to transactions or matters for which the legal professional or the legal professional's firm is providing legal services. This new model rule is a significant control that will help prevent the misuse of trust accounts, as it prohibits the use of your trust account for purposes unrelated to the provision of legal services.

The regulatory experience of law societies has shown that legal professionals sometimes use their trust accounts for purposes unrelated to the provision of legal services, and effectively act as a bank or deposit-taking institution, i.e. holding money for the limited purpose of transferring the trust money from one party to another without the provision of legal services. The use of trust accounts by clients or other parties for transactions that are completely unrelated to any legal services risks facilitating money laundering through transactions deliberately designed to disguise that the source of funds is from criminal activity. For that reason, trust accounts must not be used except when directly related to the legal services being provided by you or your firm.

Proper usage of a trust account requires you to monitor its usage and exercise your judgment about appropriate activity.

Even when the use of your trust account is related to the provision of legal services, you should ask yourself whether it is appropriate and necessary under the circumstances.



In the Real World

A 2016 discipline decision from the Law Society of British Columbia illustrates the practice and the risks it presents. In LSBC v. Donald Gurney, a lawyer used his trust account to transfer almost \$26 million in connection with four line of credit agreements in which his client was the sole borrower. There were no legal services provided – only the receipt and disbursement of funds. The disciplinary panel found that Gurney had breached his professional and ethic duties by failing to make reasonable inquiries about the transactions, and by using his trust account as a conduit for funds notwithstanding “the series of transactions being objectively suspicious.”

Features of the Model Trust Accounting Rule

"Money" is a defined term and includes cash, cheques, credit card transactions, post office orders, express and bank money orders and electronic transfer of deposits at financial institutions.

Under the rule only money that may be deposited into a trust account is money that is directly related to legal services that you or your firm are providing. The term "legal services", which is not defined in the rule, generally means the application of legal principles and legal judgement to the circumstances or objectives of a person or entity and can include:

- Giving advice with respect to a person's or entity's legal interests, rights or responsibilities of the person or of another person;
- Selecting, drafting, completing or revising documents that affect or relate to the legal interests, rights or responsibilities of a person or entity;
- Appearing as counsel or advocate for a person or entity in a proceeding before a court or an adjudicative body; and
- Negotiating or settling the legal interests, rights or responsibilities of a person or entity.

Money that is not related to the legal services provided by you or your legal practice may not be placed in a trust account.



In the Real World

Ms. G used her trust accounts to disburse business expenses for a client who owns a marina. Ms. G billed her client for drafting contracts, depositing moorage revenue into trust, paying marina operating expenses via trust cheque, and day-to-day bookkeeping services.

When asked for an explanation, Ms. G explained that the client did not utilize the services of an accountant because the client wanted to "keep her funds safe".

As set out in the rule, you must pay out any money remaining in trust following the completion of a transaction or matter as soon as practical.

In the spirit of the rule, you should ideally review client trust ledger accounts at least monthly. Every effort should be made to pay funds due to the client and to third parties within one month of all trust conditions being satisfied, and similarly, to swiftly transfer funds to your chequing account upon billing for your legal fees, disbursements or expenses.

Appendix A

Examples of Acceptable Photo Identification Documents

Source: <http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp>

<u>Type of card or document</u>	<u>Issuing jurisdiction and country</u>
<u>Canadian passport</u>	Canada
<u>Permanent resident card</u>	Canada
<u>Citizenship card (issued prior to 2012)</u>	Canada
<u>Secure Certificate of Indian Status</u>	Canada
<u>Driver's licences</u>	
<u>British Columbia Driver's Licence</u>	British Columbia, Canada
<u>Alberta Driver's Licence</u>	Alberta, Canada
<u>Saskatchewan Driver's Licence</u>	Saskatchewan, Canada
<u>Manitoba Driver's Licence</u>	Manitoba, Canada
<u>Ontario Driver's Licence</u>	Ontario, Canada
<u>Québec Driver's Licence</u>	Québec, Canada
<u>New Brunswick Driver's Licence</u>	New Brunswick, Canada
<u>Nova Scotia Driver's Licence</u>	Nova Scotia, Canada
<u>Prince Edward Island Driver's Licence</u>	Prince Edward Island, Canada
<u>Newfoundland and Labrador Driver's Licence</u>	Newfoundland and Labrador, Canada
<u>Yukon Driver's Licence</u>	Yukon, Canada
<u>Northwest Territories Driver's Licence</u>	Northwest Territories, Canada
<u>Nunavut Driver's Licence</u>	Nunavut, Canada
<u>The DND 404 Driver's Licence</u>	The Department of National Defence, Canada
<u>Provincial services cards</u>	
<u>British Columbia Services Card</u>	British Columbia, Canada
<u>Provincial or territorial identity cards</u>	
<u>British Columbia Enhanced ID</u>	British Columbia, Canada
<u>Alberta Photo Identification Card</u>	Alberta, Canada
<u>Saskatchewan Non-driver photo ID</u>	Saskatchewan, Canada
<u>Manitoba Enhanced Identification Card</u>	Manitoba, Canada
<u>Ontario Photo Card</u>	Ontario, Canada
<u>New Brunswick Photo ID Card</u>	New Brunswick, Canada
<u>Nova Scotia Identification Card</u>	Nova Scotia, Canada
<u>Prince Edward Island Voluntary ID</u>	Prince Edward Island, Canada
<u>Newfoundland and Labrador Photo Identification Card</u>	Newfoundland and Labrador, Canada
<u>Yukon General Identification Card</u>	Yukon, Canada
<u>Northwest Territories General Identification Card</u>	Northwest Territories, Canada
<u>Nunavut General Identification Card</u>	Nunavut, Canada
<u>Type of card or international document</u>	
United States passport	United States
France driver's licence	France
Australian driver's licence	New South Wales, Australia

Appendix B

Examples of Reliable Sources of Information Under the Dual Process Method to Identify an Individual

Source: <http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp>

Documents or information to verify name and address

1. Issued by a Canadian government body

- Any card or statement issued by a Canadian government body (federal, provincial, territorial or municipal)
 - Canada Pension Plan (CPP) statement
 - Property tax assessment issued by a municipality
 - Provincially-issued vehicle registration
- Benefits statement
 - Federal, provincial, territorial, and municipal levels
- CRA documents:
 - Notice of assessment
 - Requirement to pay notice
 - Installment reminder / receipt
 - GST refund letter
 - Benefits statement

2. Issued by other Canadian sources

- Utility bill (for example, electricity, water, telecommunications)
- Canada 411
- T4 statement
- Record of Employment
- Investment account statements (for example, RRSP, GIC)
- Canadian credit file that has been in existence for at least 6 months
- Product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months)

3. Issued by a foreign government

- Travel visa

Documents or information to verify name and date of birth

1. Issued by a Canadian government body

- Any card or statement issued by a Canadian government body (federal, provincial, territorial or municipal)
 - Canada Pension Plan (CPP) statement of contributions
 - Original birth certificate
 - Marriage certificate or government-issued proof of marriage document (long-form which includes date of birth)
 - Divorce documentation
 - A permanent resident card
 - Citizenship certificate
 - Temporary driver's licence (non-photo)

2. Issued by other Canadian sources

- Canadian credit file that has been in existence for at least 6 months
- Insurance documents (home, auto, life)
- Product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months)

Documents or information to verify name and confirm a financial account

Confirm that the individual has a deposit account, credit card or loan account by means of:

- Credit card statement
- Bank statement
- Loan account statement (for example. mortgage)
- Cheque that has been processed (cleared, non-sufficient funds) by a financial institution
- Telephone call, email or letter from the financial entity holding the deposit account, credit card or loan account.
- Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months)
- Use of micro-deposits to confirm account

How to rely on the credit file for the dual process method

A Canadian credit file that has been in existence for at least 6 months can be referred to as one source to verify name and address, name and date of birth or name and confirmation of a financial account. A second source from the dual process method, for example a CRA notice of assessment, must be relied on to verify the second category of information. In this instance, the two sources are the credit bureau that provided the credit file and CRA as the source of the notice of assessment. The information from these two sources must match the information provided by the individual.

The reference number for a credit file must be unique to the individual and associated to the credit file; it cannot be a reference number created by the legal professional.

Information from a credit bureau can also be obtained if they are acting as an aggregator and compiling original sources, often referred to as tradelines, so long as the identifying information is obtained from those tradelines. In this instance, the credit bureau must provide **two** independent, original tradelines as sources that verify the individual's **name and address, name and date of birth or name and confirmation of financial account**. Each tradeline is a source, not the credit bureau.

If the full financial account number is not provided because it was truncated or redacted, it is not acceptable. The legal professional must also confirm that each tradeline originates from a different source.

Appendix C

Additional Resources

Canada

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) [website](#) contains links to numerous publications and guidance documents. For example, there is a useful guidance document on [Methods of identify individuals and confirm the existence of entities](#) and, for those lawyers practicing in the area of real estate transactions, an operational brief on [Indicators of Money Laundering in Financial Transactions Related to Real Estate](#).

Provincial law societies will have different levels of information available to their members. At the time of publishing this Guidance, the [Law Society of British Columbia](#) has published numerous FAQs, Discipline Advisories, and articles in its *Bencher Bulletins* on topics related to client ID and verification, the “no cash rule”, and other red flags that lawyers should watch out for. Similarly, the Law Society of Ontario has a [dedicated FAQ page for cash transactions](#) and the Law Society of Alberta has a [page dedicated to client ID and verification](#). Contact your law society for more information.

United States

The American Bar Association, the International Bar Association, and the Council of Bars and Law Societies of Europe co-authored in 2010 a comprehensive guide for lawyers in detecting and preventing money laundering in their practices (“[Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing](#)”).

Various sections of the ABA have also produced materials that may be useful and relevant. The Criminal Justice Group has formed a [Task Force on Gatekeeper Regulation and the Profession](#). The [International Anti-Money Laundering Committee](#) facilitates discussion and examination of issues related to AML through the organization of educational programs and sessions for ABA members.

International

The Financial Action Task Force (FATF) is an international body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering and terrorist financing. Their website contains links to various country reports and guidance documents, including their 2008 [Risk-Based Guidance for Legal Professionals](#).

The International Bar Association’s ([IBA Anti-Money Laundering Forum](#)) is a mechanism that brings together information on AML legislation and compliance requirements, organized by jurisdiction. The [IBA Anti-Money Laundering Forum Reading Room](#) contains links to a range of AML resources (presentations, articles, books, websites and media); however, it should be noted that the links do not appear to have been updated since 2012.

The Council of Bars and Law Societies of Europe (CCBE) Anti-Money Laundering Committee follows the work of the FATF and developments in European jurisdictions on AML legislation. The [Committee’s website](#) contains links to position papers, letters, guides and recommendations, and reports and studies.



Model Rule on Cash Transactions

Adopted by the Council of the Federation of Law Societies of Canada September 11, 2004;
amended October 19, 2018.

Definitions

“**cash**” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“**disbursements**” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“**expenses**” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“**financial institution**” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada,
- (c) cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company that is regulated by the *Trust and Loan Companies Act* (Canada),
- (h) a trust company or loan company that is regulated by a provincial or territorial Act,
- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory when it accepts deposit liabilities in the course of providing financial services to the public, or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“**financial services cooperative**” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives, CQLR, c. C-67.3*, or *An Act respecting the Mouvement Desjardins, S.Q. 2000, c.77*, other than a caisse populaire.

“**funds**” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“**professional fees**” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“**public body**” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act* (Ontario) [or equivalent legislation] or similar body incorporated under the law of another province or territory,
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act* (Canada) or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

1. A lawyer must not receive or accept cash in an aggregate amount greater than \$7,500 Canadian in respect of any one client matter.
2. For the purposes of this rule, when a lawyer receives or accepts cash in a foreign currency the lawyer will be deemed to have received or accepted the cash converted into Canadian dollars at
 - (a) the official conversion rate of the Bank of Canada for the foreign currency as published in the Bank of Canada’s Daily Noon Rates that is in effect at the time the lawyer receives or accepts the cash, or
 - (b) if the day on which the lawyer receives or accepts cash is a holiday, the official conversion rate of the Bank of Canada in effect on the most recent business day preceding the day on which the lawyer receives or accepts the cash.
3. Section 1 applies when a lawyer engages on behalf of a client or gives instructions on behalf of a client in respect of the following activities:
 - (a) receiving or paying funds;
 - (b) purchasing or selling securities, real properties or business assets or entities;
 - (c) transferring funds by any means.

.../3

4. Despite section 3, section 1 does not apply when the lawyer receives cash in connection with the provision of legal services by the lawyer or the lawyer's firm
 - (a) from a financial institution or public body,
 - (b) from a peace officer, law enforcement agency or other agent of the Crown acting in his or her official capacity,
 - (c) to pay a fine, penalty, or bail, or
 - (d) for professional fees, disbursements, or expenses, provided that any refund out of such receipts is also made in cash.

Model Rule on Recordkeeping Requirements for Cash Transactions

“**cash**” means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada and coins or bank notes of countries other than Canada;

“**money**” includes cash, cheques, drafts, credit card sales slips, post office orders and express and bank money orders.

1. Every lawyer, in addition to existing financial recordkeeping requirements to record all money and other property received and disbursed in connection with the lawyer's practice, shall maintain
 - (a) a book of original entry identifying the method by which money is received in trust for a client, and
 - (b) a book of original entry showing the method by which money, other than money received in trust for a client, is received.
2. Every lawyer who receives cash for a client shall maintain, in addition to existing financial recordkeeping requirements, a book of duplicate receipts, with each receipt identifying the date on which cash is received, the person from whom cash is received, the amount of cash received, the client for whom cash is received, any file number in respect of which cash is received and containing the signature authorized by the lawyer who receives cash and of the person from whom cash is received.
3. The financial records described in paragraphs 1 and 2 may be entered and posted by hand or by mechanical or electronic means, but if the records are entered and posted by hand, they shall be entered and posted in ink.
4. The financial records described in paragraphs 1 and 2 shall be entered and posted so as to be current at all times.
5. A lawyer shall keep the financial records described in paragraphs 1 and 2 for at least the six year period immediately preceding the lawyer's most recent fiscal year end. [This paragraph does not apply to lawyers in Québec as the Barreau du Québec requires that such records be retained without any limitation.]



Model Rule on Client Identification and Verification

Adopted by the Council of the Federation of Law Societies of Canada March 20, 2008; amended December 12, 2008; amended October 19, 2018.

Definitions

1. In this rule,

“**credit union central**” means a central cooperative credit society, as defined in section 2 of the *Cooperative Credit Associations Act*, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial or territorial Act other than one enacted by the legislature of Quebec.

“**disbursements**” means amounts paid or required to be paid to a third party by the lawyer or the lawyer’s firm on a client’s behalf in connection with the provision of legal services to the client by the lawyer or the lawyer’s firm which will be reimbursed by the client;

“**electronic funds transfer**” means an electronic transmission of funds conducted by and received at a financial institution or a financial entity headquartered in and operating in a country that is a member of the **Financial Action Task Force**, where neither the sending nor the receiving account holders handle or transfer the funds, and where the transmission record contains a reference number, the date, transfer amount, currency and the names of the sending and receiving account holders and the conducting and receiving entities.

“**expenses**” means costs incurred by a lawyer or law firm in connection with the provision of legal services to a client which will be reimbursed by the client including such items as photocopying, travel, courier/postage, and paralegal costs;

“**financial institution**” means

- (a) a bank that is regulated by the *Bank Act*,
- (b) an authorized foreign bank within the meaning of section 2 of the *Bank Act* in respect of its business in Canada,
- (c) a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial or territorial Act,
- (d) an association that is regulated by the *Cooperative Credit Associations Act* (Canada),
- (e) a financial services cooperative,
- (f) a credit union central,
- (g) a company that is regulated by the *Trust and Loan Companies Act* (Canada),
- (h) a trust company or loan company that is regulated by a provincial or territorial Act;

- (i) a department or an entity that is an agent of Her Majesty in right of Canada or of a province or territory when it accepts deposit liabilities in the course of providing financial services to the public; or
- (j) a subsidiary of the financial institution whose financial statements are consolidated with those of the financial institution.

“financial services cooperative” means a financial services cooperative that is regulated by *An Act respecting financial services cooperatives*, CQLR, c. C-67.3, or *An Act respecting the Mouvement Desjardins*, S.Q. 2000, c.77, other than a caisse populaire.

“funds” means cash, currency, securities and negotiable instruments or other financial instruments that indicate the person’s title or right to or interest in them;

“lawyer” means, in the Province of Quebec, an advocate or a notary and, in any other province or territory, a barrister or solicitor;

“organization” means a body corporate, partnership, fund, trust, co-operative or an unincorporated association;

“professional fees” means amounts billed or to be billed to a client for legal services provided or to be provided to the client by the lawyer or the lawyer’s firm;

“public body” means

- (a) a department or agent of Her Majesty in right of Canada or of a province or territory,
- (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent in Canada of any of them,
- (c) a local board of a municipality incorporated by or under an Act of a province or territory of Canada including any local board as defined in the *Municipal Act (Ontario)* [or equivalent legislation] or similar body incorporated under the law of another province or territory,
- (d) an organization that operates a public hospital authority and that is designated by the Minister of National Revenue as a hospital under the *Excise Tax Act (Canada)* or an agent of the organization,
- (e) a body incorporated by or under an Act of a province or territory of Canada for a public purpose, or
- (f) a subsidiary of a public body whose financial statements are consolidated with those of the public body.

"reporting issuer" means an organization that is a reporting issuer within the meaning of the securities laws of any province or territory of Canada, or a corporation whose shares are traded on a stock exchange that is designated under section 262 of the *Income Tax Act* (Canada) and operates in a country that is a member of the Financial Action Task Force, and includes a subsidiary of that organization or corporation whose financial statements are consolidated with those of the organization or corporation.

"securities dealer" means persons and entities authorized under provincial or territorial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity.

Requirement to Identify Client

2. (1) Subject to subsection (3), a lawyer who is retained by a client to provide legal services must comply with the requirements of this Rule in keeping with the lawyer's obligation to know their client, understand the client's financial dealings in relation to the retainer with the client and manage any risks arising from the professional business relationship with the client.
- (2) A lawyer's responsibilities under this Rule may be fulfilled by any member, associate or employee of the lawyer's firm, wherever located.
- (3) Sections 3 through 10 do not apply to:
 - (a) a lawyer when he or she provides legal services or engages in or gives instructions in respect of any of the activities described in section 4 on behalf of his or her employer;
 - (b) a lawyer
 - (i) who is engaged as an agent by the lawyer for a client to provide legal services to the client, or
 - (ii) to whom a matter for the provision of legal services is referred by the lawyer for a client, when the client's lawyer has complied with sections 3 through 10, or,
 - (c) a lawyer providing legal services as part of a duty counsel program sponsored by a non-profit organization, except where the lawyer engages in or gives instructions in respect of the receiving, paying or transferring of funds other than an electronic funds transfer.
3. A lawyer who is retained by a client as described in subsection 2(1) must obtain and record, with the applicable date, the following information:
 - (1) for individuals:
 - (a) the client's full name,
 - (b) the client's home address and home telephone number,
 - (c) the client's occupation or occupations, and
 - (d) the address and telephone number of the client's place of work or employment, where applicable;

(2) for organizations:

- (a) the client's full name, business address and business telephone number,
- (b) other than a financial institution, public body or reporting issuer, the organization's incorporation or business identification number and the place of issue of its incorporation or business identification number, if applicable,
- (c) other than a financial institution, public body or a reporting issuer, the general nature of the type of business or businesses or activity or activities engaged in by the client, where applicable, and
- (d) the name and position of and contact information for the individual who is authorized to provide and gives instructions to the lawyer with respect to the matter for which the lawyer is retained.

(3) if the client is acting for or representing a third party, information about the third party as set out in subsections (1) or (2) as applicable.

When Verification of Client Identity Required

4. Subject to section 5, section 6 applies where a lawyer who has been retained by a client to provide legal services engages in or gives instructions in respect of the receiving, paying or transferring of funds.

Exemptions re: certain funds

5. Section 6 does not apply

- (1) where the client is a financial institution, public body or reporting issuer,
- (2) in respect of funds,
 - (a) paid by or to a financial institution, public body or a reporting issuer;
 - (b) received by a lawyer from the trust account of another lawyer;
 - (c) received from a peace officer, law enforcement agency or other public official acting in their official capacity;
 - (d) paid or received to pay a fine, penalty, or bail; or
 - (e) paid or received for professional fees, disbursements, or expenses;
- (3) to an electronic funds transfer.

Requirement to Verify Client Identity

6. (1) When a lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, the lawyer must
- (a) obtain from the client and record, with the applicable date, information about the source of funds described in section 4, and
 - (b) verify the identity of the client, including the individual(s) described in paragraph 3(2)(d), and, where appropriate, the third party using the documents or information described in subsection (6).

Use of Agent

- (2) A lawyer may rely on an agent to obtain the information described in subsection (6) to verify the identity of an individual client, third party or individual described in paragraph 3(2)(d) provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4).
- (3) Notwithstanding subsection (2), where an individual client, third party or individual described in paragraph 3(2)(d) is not physically present in Canada, a lawyer must rely on an agent to obtain the information described in subsection (4) to verify the person's identity provided the lawyer and the agent have an agreement or arrangement in writing for this purpose as described in subsection (4).

Agreement for use of Agent

- (4) A lawyer who enters into an agreement or arrangement referred to in subsection (2) or (3) must:
 - (a) obtain from the agent the information obtained by the agent under that agreement or arrangement; and
 - (b) satisfy themselves that the information is valid and current and that the agent verified identity in accordance with subsection (6).
- (5) A lawyer may rely on the agent's previous verification of an individual client, third party or an individual described in paragraph 3(2)(d) if the agent was, at the time they verified the identity,
 - (a) acting in their own capacity, whether or not they were required to verify identity under this Rule, or
 - (b) acting as an agent under an agreement or arrangement in writing, entered into with another lawyer who is required to verify identity under this Rule, for the purpose of verifying identity under subsection (6).

Documents and information for verification

- (6) For the purposes of paragraph (1)(b), the client's identity must be verified by referring to the following documents, which must be valid, original and current, or the following information, which must be valid and current, and which must not include an electronic image of a document:
 - (a) if the client or third party is an individual,
 - (i) an identification document containing the individual's name and photograph that is issued by the federal government, a provincial or territorial government or a foreign government, other than a municipal government, that is used in the presence of the individual to verify that the name and photograph are those of the individual;

- (ii) information that is in the individual's credit file if that file is located in Canada and has been in existence for at least three years that is used to verify that the name, address and date of birth in the credit file are those of the individual;
- (iii) any two of the following with respect to the individual:
 - (A) Information from a reliable source that contains the individual's name and address that is used to verify that the name and address are of those of the individual;
 - (B) Information from a reliable source that contains the individual's name and date of birth that is used to verify that the name and date of birth are those of the individual, or
 - (C) Information that contains the individual's name and confirms that they have a deposit account or a credit card or other loan amount with a financial institution that is used to verify that information.
- (b) For the purposes of clauses (6)(a)(iii)(A) to (C), the information referred to must be from different sources, and the individual, lawyer and agent cannot be a source.
- (c) To verify the identity of an individual who is under 12 years of age, the lawyer must verify the identity of one of their parents or their guardian.
- (d) To verify the identity of an individual who is at least 12 years of age but not more than 15 years of age, the lawyer may refer to information under clause (6)(a)(iii)(A) that contains the name and address of one of the individual's parents or their guardian and verifying that the address is that of the individual.
- (e) if the client or third party is an organization such as a corporation or society that is created or registered pursuant to legislative authority, a written confirmation from a government registry as to the existence, name and address of the organization, including the names of its directors, where applicable, such as
 - (i) a certificate of corporate status issued by a public body,
 - (ii) a copy obtained from a public body of a record that the organization is required to file annually under applicable legislation, or
 - (iii) a copy of a similar record obtained from a public body that confirms the organization's existence; and
- (f) if the client or third party is an organization, other than a corporation or society, that is not registered in any government registry, such as a trust or partnership, a copy of the organization's constituting documents, such as a trust or partnership agreement, articles of association, or any other similar record that confirms its existence as an organization.

Requirement to Identify Directors, Shareholders and Owners

- (7) When a lawyer is engaged in or gives instructions in respect of any of the activities in section 4 for a client or third party that is an organization referred to in paragraph (6)(e) or (f), the lawyer must:
- (a) obtain and record, with the applicable date, the names of all directors of the organization, other than an organization that is a securities dealer; and
 - (b) make reasonable efforts to obtain, and if obtained, record with the applicable date,
 - (i) the names and addresses of all persons who own, directly or indirectly, 25 per cent or more of the organization or of the shares of the organization,
 - (ii) the names and addresses of all trustees and all known beneficiaries and settlors of the trust, and
 - (iii) in all cases, information establishing the ownership, control and structure of the organization.
- (8) A lawyer must take reasonable measures to confirm the accuracy of the information obtained under subsection (7).
- (9) A lawyer must keep a record, with the applicable date(s), that sets out the information obtained and the measures taken to confirm the accuracy of that information.
- (10) If a lawyer is not able to obtain the information referred to in subsection (7) or to confirm the accuracy of that information in accordance with subsection (8), the lawyer must
- (a) take reasonable measures to ascertain the identity of the most senior managing officer of the organization;
 - (b) determine whether
 - (i) the client's information in respect of their activities,
 - (ii) the client's information in respect of the source of the funds described in section 4, and
 - (iii) the client's instructions in respect of the transaction, are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule;
 - (c) assess whether there is a risk that the lawyer may be assisting in or encouraging fraud or other illegal conduct; and
 - (d) keep a record, with the applicable date, of the results of the determination and assessment under paragraphs (b) and (c).

Timing of Verification for Individuals

- (11) A lawyer must verify the identity of
- (a) a client who is an individual, and
 - (b) the individual(s) authorized to provide and giving instructions on behalf of an organization with respect to the matter for which the lawyer is retained
- upon engaging in or giving instructions in respect of any of the activities described in section 4.
- (12) Where a lawyer has verified the identity of an individual, the lawyer is not required to subsequently verify that same identity unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Timing of Verification for Organizations

- (13) A lawyer must verify the identity of a client that is an organization upon engaging in or giving instructions in respect of any of the activities described in section 4, but in any event no later than 30 days thereafter.
- (14) Where the lawyer has verified the identity of a client that is an organization and obtained information pursuant to subsection (7), the lawyer is not required to subsequently verify that identity or obtain that information, unless the lawyer has reason to believe the information, or the accuracy of it, has changed.

Record Keeping and Retention

7. (1) A lawyer must obtain and retain a copy of every document used to verify the identity of any individual or organization for the purposes of subsection 6(1).
- (2) The documents referred to in subsection (1) may be kept in a machine-readable or electronic form, if a paper copy can be readily produced from it.
- (3) A lawyer must retain a record of the information, with the applicable date, and any documents obtained for the purposes of section 3, subsection 6(7) and subsection 10(2) and copies of all documents received for the purposes of subsection 6(1) for the longer of
- (a) the duration of the lawyer and client relationship and for as long as is necessary for the purpose of providing service to the client, and
 - (b) a period of at least six years following completion of the work for which the lawyer was retained.

Application

8. Sections 2 through 7 of this Rule do not apply to matters in respect of which a lawyer was retained before this Rule comes into force but they do apply to all matters for which he or she is retained after that time regardless of whether the client is a new or existing client.

Criminal activity, duty to withdraw at time of taking information

9. (1) If in the course of obtaining the information and taking the steps required in section 3 and subsections 6(1), (7) or (10), a lawyer knows or ought to know that he or she is or would be assisting a client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.
- (2) This section applies to all matters, including new matters for existing clients, for which a lawyer is retained after this Rule comes into force.

Monitoring

10. During a retainer with a client in which the lawyer is engaged in or gives instructions in respect of any of the activities described in section 4, the lawyer must:
- (1) monitor on a periodic basis the professional business relationship with the client for the purposes of:
- (a) determining whether
- (i) the client's information in respect of their activities,
- (ii) the client's information in respect of the source of the funds described in section 4, and
- (iii) the client's instructions in respect of transactions are consistent with the purpose of the retainer and the information obtained about the client as required by this Rule, and
- (b) assessing whether there is a risk that the lawyer may be assisting in or encouraging fraud or other illegal conduct; and
- (2) keep a record, with the applicable date, of the measures taken and the information obtained with respect to the requirements of paragraph (1)(a) above.

Duty to withdraw

11. (1) If while retained by a client, including when taking the steps required in section 10, a lawyer knows or ought to know that he or she is or would be assisting the client in fraud or other illegal conduct, the lawyer must withdraw from representation of the client.

Application

- (2) This section applies to all matters for which a lawyer was retained before this Rule comes into force and to all matters for which he or she is retained after that time.

*Federation of Law Societies
of Canada*



*Fédération des ordres professionnels
de juristes du Canada*

Model Trust Accounting Rule

Approved by the Council of the Federation of Law Societies of Canada on October 19, 2018.

Definitions

“**money**” includes cash, cheques, drafts, credit card transactions, post office orders, express and bank money orders, and electronic transfer of deposits at financial institutions

1. A lawyer must pay into and withdraw from, or permit the payment into or withdrawal from, a trust account only money that is directly related to legal services that the lawyer or the lawyer’s law firm is providing.
2. A lawyer must pay out money held in a trust account as soon as practicable upon completion of the legal services to which the money relates.



**Anti-Money Laundering and Terrorist Financing
Working Group**

**Guidance on Monitoring
Obligations**

Client Identification and Verification

July 6, 2020

Monitoring

The Client Identification and Verification rule requires legal professionals who are retained in respect of a financial transaction¹ to periodically monitor their professional business relationship with their client. This requirement applies to all clients in such circumstances, including long-standing clients.

What is required?

While retained in respect of a financial transaction, you must periodically assess:

- (1) Whether the information you have obtained about (i) your client's activities, (ii) the source of funds used in the transaction, and (iii) your client's instructions are consistent with the purpose of the retainer and the information you have about the client; and
- (2) Whether there is a risk that you may be assisting in or encouraging fraud or other illegal conduct.

You must also keep a record of the measures you have taken to comply with the monitoring requirements, including the applicable date and the client information that you have obtained. The record must be kept for at least six years following completion of the work for which you were retained.

What steps should you take?

The nature, degree and frequency of periodic monitoring and what information should be recorded will depend on what is reasonable in each case considering the client, the nature of the work, the anticipated duration of the retainer and the services provided. The measures taken should be commensurate with the risk associated with these or other relevant factors. More thorough or frequent monitoring may be required when the circumstances indicate an elevated risk.

Although risk must be assessed on a case by case basis, some examples of factors indicating an elevated risk include: unusual or inconsistent client behaviour, activities, or instructions; a transaction of relatively high value is undertaken without financing; the financing arrangements or source of funds are unclear or unexplained; the client has modest income relative to the transaction without a reasonable explanation; the client is an elected official or other politically exposed person² as defined by legislation; the transaction involves a country identified by competent authorities as having weak anti-money laundering laws and measures.

You are required to apply your professional judgment to assess risks in any given circumstance.³

¹ This means "to engage in, or give instructions in respect of receiving, paying or transferring of funds". Common examples include providing legal services in relation to the purchase or sell of business entities, arranging financing for the purchase or sale of business entities or assets, and purchasing or selling real estate.

² For information on politically exposed persons (PEPs) see <https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide12/12-eng>.

³ For more detail on identifying and assessing risk see the Federation of Law Societies of Canada's Risk Assessment Case Studies for the Legal Profession.

Duty to withdraw representation

If while retained, including in the course of obtaining the required information and taking the steps under the monitoring requirements, you know or ought to know that you are or would be assisting a client in fraud or other illegal conduct, you must withdraw from representation of the client.⁴

The Client Identification and Verification rule is designed to mitigate risks of involvement in or facilitation of money laundering or terrorist financing. The *Model Code of Professional Conduct* rules for the legal profession also require legal professionals to be diligent against potential client dishonesty, fraud or other illegal activities.⁵

You are encouraged to contact a practice advisor or the equivalent at your Law Society for further guidance on what may be required in a particular matter.

⁴ See Client Identification and Verification rule ss. 9(1) and 11.

⁵ See the Federation of Law Societies of Canada's *Model Code of Professional Conduct* rules 3.2-7 (dishonesty, fraud by client or others) and 3.2-8 (dishonesty, fraud when client an organization), in particular, regarding the duty to withdraw.



Anti-Money Laundering and Terrorist Financing Working Group

Guidance on Using an Agent

Client Identification and Verification

July 6, 2020

Use of Agents

The Client Identification and Verification rule requires legal professionals to verify an individual's identity when they are retained to provide legal services in respect of a financial transaction.¹

You **may use an agent** to verify the identity of an individual at any time.

When must an agent be used?

If the individual whose identity is to be verified is outside of Canada and you cannot meet with them in person, you must use an agent for the verification.

You also must use an agent when relying on the government-issued document method for verification if the client or third party is located elsewhere in Canada and you, or a partner, associate or employee at your firm, cannot meet with them in person.

Agreement or arrangement in writing

When you are using an agent to verify identity you must have a written agreement with the agent. The agreement does not need to be in any particular form; it may be a letter or email, for example. However, the agreement should set out in sufficient detail the purpose of the arrangement and what the agent is expected to do.

Who may act as an agent?

There are no set qualifications or credentials for who may act as an agent to verify identity. You must use your professional judgment to choose a suitable agent.

The responsibility for verifying an individual's identity is yours, even when using an agent. You should always choose the agent; don't rely on your client or the individual whose identity is being verified to find the agent.

You should ensure that the agent is reputable, reliable, accountable, and, where feasible, familiar with anti-money laundering due diligence requirements. For instance, in the case of a potential agent who is a member of a regulated profession, you should check the agent's status and contact information with the regulator.²

Caution should be used when seeking an agent in a country other than Canada, particularly where the individual or the subject matter of the retainer involves a high-risk jurisdiction³. In some cases, embassies or consulates may offer verification of identity services.

If you do not know a suitable candidate to act as agent, you should check with the regulator for the legal profession in the jurisdiction where the individual is located.

¹ This means "to engage in or give instructions in respect of the receipt, payment or transfer of funds".of business entities, arranging financing for the purchase or sale of business entities or assets, and purchasing or selling real estate.

² As a general guidance, the following professionals may be suitable to act as agents within Canada: lawyers; Quebec notaries; Ontario paralegals; British Columbia notaries; notaries public; peace officers; justices of the peace; professional accountants; banks and other financial and life insurance companies, brokers and agents; securities dealers; and real estate brokers and real estate agents.

³ Resources to help identify a high-risk jurisdiction include current sanctions imposed by the Government of Canada and information on countries from the Financial Action Task Force (FATF).

Information from the agent

You must obtain from the agent and keep a record of all information they use to verify the individual's identity. The information from the agent should include:

- The agent's full name, occupation and business address;
- The method(s) used to verify the client's identity;
- Copies of the information and documents obtained by the agent to verify the individual's identity; and
- The date on which the agent verified the individual's identity.

You should also record the date the agent delivered the information to you.

Due diligence

You must be satisfied that the verification information obtained from the agent is valid (authentic and unaltered) and current (not expired) and that the agent verified the individual's identity through a prescribed method (government-issued documentation, credit file, or dual process method) in accordance with the rules. The verification information must match the basic identification information provided by the client.

Previous verification

You may rely on an agent's previous verification of an individual if the agent was, at that time, acting in their own capacity (e.g. as a legal advisor verifying identity) or as an agent under an agreement or arrangement in writing with another legal advisor required to verify identity under the Client Identification and Verification rule. You must still have an agreement or arrangement in writing in these circumstances and the previous verification must meet the requirements of the Client Identification and Verification rule.



Anti-Money Laundering and Terrorist Financing Working Group

Risk Assessment Case Studies for the Legal Profession

February 2020

Table of Contents

Overview	1
Misuse of Trust Accounts	3
Purchase and Sale of Real Estate Property & Other Transactions ...	4
Creation and Management of Trusts and Companies	8
Managing Client Affairs and Making Introductions.	11
Disputes and Litigation.....	22
Red Flags Quick Reference Guide.....	24

OVERVIEW

The practice of law exposes members of the legal profession¹ to unique risks and vulnerabilities in relation to money laundering. Criminals may target legal advisors to lend legitimacy to their illicit operations or make use of trust accounts to launder proceeds of criminal activity. Legal advisors are also necessary to complete real estate transactions and set up trusts, both common vehicles for cleaning dirty money.

As a legal advisor you have important legal and ethical duties in relation to money laundering and other crimes. Under the rules of professional conduct, legal advisors must not knowingly assist in or encourage any fraud, crime or other illegal conduct. Additionally, you must withdraw if a client persists in instructing you to act contrary to law or professional ethics. As a legal advisor it is important for you to be aware of a recent amendment to the Criminal Code that added a recklessness standard to the offence of money laundering. This amendment makes it an offence to deal with property or proceeds of property “knowing or believing or being reckless as to whether” they are the proceeds of crime².

Understanding these duties and knowing how to recognize the risks and vulnerabilities are essential to protecting you and your practice, the legal profession, and the public.

This document is designed to help you become familiar with and learn how to spot red flags, as well as to guide practical responses when faced with situations of possible money laundering. It is recommended that you review the document periodically, as a preventative measure, to enhance your ability to spot and avoid problems.

The following case studies³, which describe the scenario, identify red flags, and include commentary on how you can respond, are divided thematically according to common methods that criminals use in targeting legal advisors⁴:

¹ Members of the legal profession in Canada include lawyers, Quebec notaries, and Ontario paralegals. For simplicity the term legal advisor is used throughout the document to refer to all members of the profession.

² Section 462.31, effective June 21, 2019.

³ The case studies are adapted from the Financial Action Task Force’s (FATF) Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (2013), the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe’s A Lawyer’s Guide to Detecting and Preventing Money Laundering (2014), case law and other open source materials.

⁴ See, for example, FATF Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (2013).

1. Misuse of trust accounts
2. Purchase and sales of real estate property and other transactions
3. Creation and management of trusts and companies
4. Managing client affairs and making introductions
5. Disputes and litigation

A quick reference guide of red flags is included as an Appendix.

Several of the case studies include reference to individuals who come from, or transactions that involve, “countries that pose a geographic risk.” These are countries that have been identified by competent authorities as posing a high risk for money laundering based on, among other things, prevalence of corruption and financial crime, and weakness of anti-money laundering laws and measures⁵.

Some case studies refer to “politically exposed persons” (PEPs). These are individuals who are or have been entrusted with prominent public functions within domestic or foreign governments, or international organizations, as well as their family and business associates⁶. Due to the opportunity that PEPs have to influence decisions and control resources, they are vulnerable to corruption.

Heightened scrutiny and enhanced risk assessment measures are required when a case involves a PEP and/or a country that poses a geographic risk.

If you have questions about a case or circumstance in which you are involved that may relate to money laundering, you may wish to consult your law society or independent legal counsel.

⁵ Government of Canada-imposed Economic Sanctions (https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng), FATF (<http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/>), FINTRAC (<https://www.fintrac-canafe.gc.ca/new-neuf/1-eng#tab2>), United Nations Security Council (<https://www.un.org/securitycouncil/sanctions/information>).

⁶ Defined under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*, S.C. 2000, c. 17, section 9.3, PEPs include the head of state or government, member of executive council of a government, member of a legislature, deputy minister (or equivalent), ambassador, senior military officer, president of a state-owned corporation, head of a government agency, judge, and president of a political party represented in a legislature, as well as the personal . Domestic PEPs include officials at the federal and provincial/territorial level as well as a mayor of a municipality. The head of international organizations are also considered PEPs. See the PCMLTFA for a full list of PEPs and visit FINTRAC’s website for more information on PEPs: <https://www.fintrac-canafe.gc.ca/publications/general/faq-pep-eng>.

1. MISUSE OF TRUST ACCOUNTS

SCENARIO:

Aborted transaction and transfer of funds without substantial legal work done

A law firm was approached by a new client seeking legal services on some asset purchases. The firm assigned the matter to a junior lawyer, who was keen to grow their client list and help bring new work into the firm. The new client also seemed eager to retain the lawyer and the firm. At the client's request, the lawyer gave the client the law firm's trust account details before the client identification and verification checks on the client were completed or the engagement letter was signed. The client quickly deposited funds in the law firm's trust account.

Following the deposit of funds, the client did not immediately respond to communications or requests to attend at the firm's office and she did not give any further instructions. When the client responded to the lawyer a few days later by email, the client explained that she no longer intended to purchase the assets and asked for the deposited funds to be returned; however, she requested they be sent to a third party, rather than to the original account.



RED FLAGS

- Urgency on the part of the client to deposit funds.
- Transaction is aborted shortly after funds deposited.
- Client initially appears keen but becomes difficult to reach following the deposit of funds.
- Client requests the deposited funds be returned before any substantive legal work has commenced.
- Client requests that deposited funds be sent to a new account or a third party, rather than returned to the same account.
- Client avoids personal contact without good reason.

What can you do?

Client funds should not be deposited into your trust account until you have completed your due diligence and risk assessment of the client, including the required client identification and verification steps, established the details of the transaction (including its purpose), and satisfied yourself that there is no reasonable risk that acting for the client or on the transaction will involve assisting in or encouraging any fraud or other illegal conduct including money laundering.

To avoid the risk of a client depositing funds into your trust account before you have taken these due diligence steps, you should not provide the client with the details of your trust account. Any unused client trust funds should be returned to the client or the original payor (if received from someone on behalf of the client).

Where a client directs that funds deposited into your trust account be paid out to a third party, you should, at a minimum seek an explanation for the directions. If you have concerns about the bona fides of the proposed payment, you should return the funds to the original source. You should also consult your regulator's rules regarding the acceptance and return of cash or other money.

2. PURCHASE AND SALE OF REAL ESTATE PROPERTY AND OTHER TRANSACTIONS

SCENARIO:

Investing potential proceeds of crime

A client retained a legal advisor for the purchase of a residential property. The client did not come into the office and communicated by telephone and email only. At the outset of the engagement, the client indicated that he wished to pay the total purchase price for deposit into the law firm's trust account before the final agreement was reached.

The legal advisor's due diligence suggested that the sum provided was a large amount relative to the client's employment income. After the client's funds were deposited the client became slower to respond with instructions and seemed less interested in the details of the transaction as it progressed. At one point, the legal advisor told the client about an easement discovered on title that would allow his neighbour to drive through the back part of the property. The client did not seem concerned about this or ask many questions. The purchase of the property went ahead for a sum smaller than that deposited.



RED FLAGS

- Client's unusual request to deposit funds early in the transaction, especially before the purchase price had been finalized.
- Sum deposited appears large relative to the client's income.
- Client becomes evasive and less interested in the transaction despite depositing a large sum of money.
- Transaction results in surplus funds from the initial large deposit.

What can you do?

You should be wary of clients who are prepared to deposit large sums into a trust account at the very outset of an engagement (and certainly prior to the agreement being finalized). Advise the client on a more common or appropriate time to deposit funds (i.e. just prior to closing). If the funds the client has deposited are large relative to their socio-economic profile, you should consider conducting enhanced verification of the source of funds.

This may include asking for additional information and documents demonstrating how the client acquired and maintained the funds (e.g. banking and investment records, receipts, contracts). Be wary of accepting client funds in excess of those required for the transaction and associated expenses (e.g. fees and disbursements).

SCENARIO: Unexplained source of wealth used to purchase property⁷

A couple with some wealth recently immigrated to Canada from a country that poses a geographic risk. They retained a legal advisor to assist with the purchase of a large residential property and to set up a company. The home was paid for without any financing. The couple separated soon after moving to Canada. Despite separating, they continued to buy and develop residential properties together, usually without financing through their joint company.

At one point, the ex-husband transferred his interest in the company to a real estate agent they had been using for the purchases, only to transfer the interest back a short time later. The couple did not have any employment or business interests in Canada beyond real estate investing. The ex-husband was an extensive gambler and required income from the properties to pay for these activities.



RED FLAGS

- Clients coming from a high risk country.
- Unexplained source of wealth for the purchase of properties.
- Purchase of several residential properties without financing over a short period of time.
- Potential marriage of convenience (separating soon after entering Canada).
- Unusual transfer of the client's interest in the company only to be returned for no apparent reason.
- Client heavily involved in gambling activities.

What can you do?

In addition to verifying the source of funds, when a client is from a high-risk country and has wealth of a mysterious origin, you should conduct further inquiries including requesting additional supporting documentation. Additional red flags – extensive gambling, possible marriage of convenience, large purchases without financing – also indicate the need for caution. Unless you are satisfied to a reasonable standard that the money is not the proceeds of crime, you must not act or continue to act for the clients.

⁷ Based on *Wang v. Kesarwani*, 2017 ONSC 6821 (CanLII).

SCENARIO:

Back-to-back sales from client with low income relative to amounts paid

An individual in his 20s who worked as a labourer approached a legal advisor to purchase multiple real estate properties. The client appeared to have negotiated good prices for the properties. The legal advisor believed the client was getting a very good deal even in the current slow market. The client claimed to be funding the purchases from previous real estate sales. Shortly after the purchases, the client instructed another lawyer to re-sell the same properties at a higher price. The purchasers were also in their early 20s with low-paying jobs. The client had in fact taken out mortgages on these properties using false documents, generating proceeds of crime. The multiple re-sales helped to launder those funds.

RED FLAGS



- Funds at the client's disposal appear large relative to the client's income.
- Client and other parties appear to be young for high value transactions given their income.
- Properties are paid for without financing.
- Client engaged in back to back property transactions, out of sync with normal market dynamics.
- Reason for the transactions is unclear.
- Purported value of the properties rapidly increases with each subsequent transaction despite the short period of time in between transactions.
- Client changes legal advisor in a short time period for no apparent reason.

What can you do?

If a client with a low to modest income and no other apparent source of wealth proposes to buy property with no financing, additional information is required. In this case, you need to conduct enhanced due diligence on the source of funds including obtaining supporting documentation for the "previous real estate sales" that reportedly generated the initial funding.

Before acting you must be satisfied that the explanation provides a reasonable basis for concluding that the transactions are legitimate. A subsequent legal advisor hired in a back to back sale should also inquire about the reasons for the client retaining new legal representation.

SCENARIO:

Criminal uses elderly parents to launder proceeds of crime

An elderly couple and their adult son met with a legal advisor about the purchase of a home. The son explained he was there to support his parents. The parents acknowledged this and presented valid identification. The son did most of the talking for his parents during the meeting. The parents' income consisted of a modest pension. They lived in a trailer home, which they planned to keep for their son's use. About half of the purchase price for the new home came from a bank account in the parents' name, which the son helped to set up. The balance was financed through a private mortgage in the parents' names.

The legal advisor assisted the couple in purchasing the property speaking mainly with the son and, as instructed, registered title in the parents' names. The mortgage, which was over \$300,000, was paid off immediately. The son returned to the legal advisor's office soon after and inquired about new wills for his parents. The son turned out to be a career criminal using his parents to launder proceeds of crime from drug trafficking, fraud, and auto theft.



RED FLAGS

- Third party, rather than the clients, appears to be directing decision making.
- Disproportionate amount of private funding or availability of cash, which is inconsistent with the known legitimate income of the clients.
- There is uncertainty about who the real beneficiary or owner is.
- Mortgage repaid significantly prior to the maturity date with no logical explanation.

What can you do?

Although it is not uncommon for family members to assist in legal matters, you should carefully consider who you are really acting for and whether there may be capacity issues. Additional steps may be necessary to confirm who is giving the instructions and to ascertain who are the true beneficiaries of the transactions. Enhanced verification of the source of funds is also warranted when the client's income is modest, they have no other apparent source of wealth (such as selling property) and they are financing only a portion of the purchase price.

3. CREATION AND MANAGEMENT OF TRUSTS AND COMPANIES

SCENARIO:

Creation of a private trust

A woman contacted a mid-sized law firm seeking legal advice on creating a trust. She found the law firm through an internet search. The woman was from a country that poses a geographic risk. She provided a valid visa as proof of identification. She asked the lawyer to prepare a trust to handle an inheritance she received back in her home country. The trust was to be funded via wire transfer of the inheritance into the law firm's trust account in Canada. She asked for a legal opinion on tax issues and filing requirements in relation to the trust.

The client wanted to be the trustee with her adult children, one of whom lives in Canada named as the beneficiaries. She did not have a Canadian residence or bank account. The client also wanted an introduction to a chartered accountant and a banker in Canada. The type of trust requested by the client was a normal structure familiar to most legal counsel with experience with trusts. The goal of the client appeared to be asset management for the benefit of her children. While the tax consequences may have been complex, the plan itself was relatively typical.

RED FLAGS



- Client is not known to the legal advisor and the source of the connection (i.e., internet search) does not add any comfort.
- Client comes from a country that poses a geographic risk.
- The funds are to be wired from outside of the country into the law firm's trust account.
- Client does not have a bank account in the jurisdiction.
- Client requires introduction to multiple professionals (i.e. certified accountant and banker) indicating lack of connection with the jurisdiction.

What can you do?

Despite the fact that the plan for the trust is not unusual, several factors give cause for concern and suggest a potential money laundering risk, including the client's geographic location, limited connection to the jurisdiction, and rationale for selecting the legal advisor. There is also no compelling reason for the funds to flow through the legal advisor's trust account. In such cases, you should advise the client to open a Canadian bank account and not accept the funds directly into your trust account.

Additional inquiries should be made into the source of funds, including a request for supporting documentation. If after further inquiries, you are not satisfied on an objective basis that the transactions are legitimate, you must not act.

SCENARIO:**Management of an existing trust that may contain criminal property**

A client went into the trust lawyer's office to terminate a trust established by his deceased mother. The client was the sole beneficiary of the trust. When asked about the source of the funds in the trust, the client was ambiguous and appeared evasive. When pressed, the client informed the legal advisor that he believed his mother may have embezzled the funds over many years from her long-time employer. The client asked the legal advisor for advice regarding the disposition of the assets in the trust and any legal obligations to the former employer.

**RED FLAGS**

- Client is not well known to the lawyer.
- The funds in the trust may be from illegal activity.

What can you do?

If you suspect assets may have been obtained through illegal activity, you have legal and ethical duties to make further inquiries. Facilitating the distribution of the trust assets to the client without making such inquiries and without being satisfied that the funds in the trust account were not obtained illegally would likely result in the breach of the applicable legal and ethical duties. There are no legal or ethical issues with preparing an opinion on the rights of the defrauded employer and the impact of those rights on the trust assets and client's entitlement to them.

SCENARIO: Trust managed to facilitate a fraud⁸

A client retained a legal advisor to set up a trust. After the trust was established and the retainer had ended, the client created a false genealogy for the trust claiming it was a long-standing trust associated with a European monarchy. He then solicited investments for phony loans. The client hired a new legal advisor to manage the trust and publicized the advisor's credentials to legitimize the trust. The client provided the second legal advisor with false documentation about the trust.

The client then instructed the legal advisor to provide guarantees on behalf of the trust, maintain an escrow account into which "investments" could be deposited, and distribute the deposited monies to the client and his third party associates when requested.

RED FLAGS



- Client retained different legal advisors for setting up the trust, and later managing it, to hide the origins of the trust.
- Payments to the trust appear to be advance fees in a potentially fraudulent scheme.
- Client relied on the reputation of the second legal advisor to bolster the trust.
- Client instructed the legal advisor to give guarantees, receive advance fees, and distribute funds out of the trust to the client and third parties.

What can you do?

The legal and ethical obligation on legal professionals to not act for a client if there is reasonable likelihood it will aid or result in the commission of a crime is a very serious one. In this case, there are strong indications that the trust was being used fraudulently. Additional due diligence should be undertaken in such cases, including obtaining and carefully inspecting documents related to the creation and existence of the trust and scrutinizing the transactions that fund the trust.

⁸ Based on *United States v. Anderskow*, 88 F.3d 245 (3d Cir. 1996).

4. MANAGING CLIENT AFFAIRS AND MAKING INTRODUCTIONS

SCENARIO:

Legal advisor fails to respond to money laundering warning signs

A client who owned several residential rental properties contacted a legal advisor for assistance with the purchase of another rental property. He had not yet decided on a property to purchase. He told the legal advisor that he wanted to choose a legal advisor he liked working with and whom he could trust before making his decision on a property. The two had several common interests and got along very well. They met often and became friends, but the client did not provide any immediate work.

One day, the client told the legal advisor that he had found a suitable property but could not proceed due to temporary cash flow difficulties caused by the need to make repairs to one of his rental units. He asked for a short-term loan, which the legal advisor agreed to, lending the money from his personal account. The legal advisor did not advise the client to get independent legal advice. The transaction went ahead and, shortly after closing, the client settled the loan. The client subsequently purchased two more properties, one funded by another loan from the legal advisor; the other funded by payments from a third party account. The client explained that the third party owed him a debt for unpaid rent.

The legal advisor took the client at his word and did not ask for additional information or supporting documents about this debt. Around this time, the legal advisor saw a news report indicating the client was being investigated for involvement with organized crime. The real estate deals closed without issue and the second loan was repaid quickly.



RED FLAGS

- Client is seeking to establish a relationship without specific work identified.
- Source of funds for the transactions are unusual.
- Lack of information on the source of funds for loan repayments.
- Payments from third parties.
- Client has suspected criminal associations.

What can you do?

You should exercise a high degree of caution when a client seeks to establish a relationship without asking you to undertake any specific legal work. Criminals may seek to “groom” you as part of their illegal scheme. The rules of professional conduct prohibit the lending of money to a client unless you explain the conflicting interest and require the client to obtain independent legal advice. Short-term loans of large sums raise red flags and, in circumstances such as these, particularly if discovering suspected links to organized crime, you should not act for the client.

SCENARIO: Lawyer's judgment clouded by relationship with longstanding client

A sole practitioner, with 18 years of estates law practise, was asked by a longstanding client for help in selling his cottage. The legal advisor very rarely did real estate work, but wanted to keep this client's employment law business. She relied on her longstanding relationship with the client and did not take steps to verify the client's identity or otherwise try to learn anything more about the client. The client told her that he wished to sell the property quickly and was willing to list it at almost two-thirds its potential value.

The legal advisor found this odd, but accepted the client's explanation that he was experiencing financial difficulties and could no longer keep up with mortgage payments on his home. The legal advisor had heard a rumour that the police had investigated the client at some point for involvement in drug dealing, but she was not aware of any details. The client was subsequently convicted of drug trafficking. It emerged that he sold the cottage in a hurry as he feared it might be confiscated as part of the criminal proceedings.



RED FLAGS

- Client asked the lawyer to perform work outside her usual scope of practice.
- The instructions to sell the house below value were unusual and could result in a loss to the client.
- Client may be involved in the illegal drug trade.

What can you do?

You should make inquiries if you have information or hear "rumours" indicating the transaction may pose a risk for illegal activity, even with long-standing clients. You should also monitor your clients on an ongoing basis to ensure the information and instructions given are consistent with the purpose of the retainer and that you are not involved in or encouraging dishonesty, fraud, or illegal conduct. In this case, the client's possible criminal activity and his instructions to proceed with an expedited sale of property below market value were indicators that the lawyer might be facilitating criminal activity. In such circumstances, it would not be reasonable to proceed with the transaction.

SCENARIO:

Failure to complete due diligence due to source of referral

A junior partner in a law firm visited an important corporate client to make a pitch on a potential major new file. During a break in the meetings, the CEO for the client introduced the legal advisor to his nephew. The nephew needed help on some commercial matters and the director told the legal advisor that he would be “very grateful” if he would act for his nephew. The legal advisor wanted to please the corporate client and the work sounded straightforward. Urged to say “yes” or “no” right away, the lawyer agreed to act for the new client. Relying on the referral by a respected client and proof that the nephew had accounts with at least two major banks, the legal advisor decided to forgo the full due diligence checks.

Over the next two years, the lawyer acted for the nephew in straightforward commercial matters and significant funds remained in the law firm’s trust account following the transactions. One day, the police contacted the legal advisor and advised that they were investigating the nephew for suspected involvement in a fraud ring. Shortly afterward, the nephew called to ask the lawyer to transfer a large sum of money held in the client trust account to an overseas bank.



RED FLAGS

- Client puts pressure on the lawyer to represent unknown relative of client (in this case leveraging the lawyer’s desire to please another important client).
- Significant funds were being held for the client in the firm’s trust account following completion of transactions.
- Client is being investigated for fraudulent activities.

What can you do?

Always complete your client identification and verification checks, regardless of who the source of the referral. Only funds directly related to legal services are permitted to be held in a lawyer’s trust account. You must disburse funds held in trust for the client as soon as practicable following completion of the related legal services.

SCENARIO: International client and creation of shell corporations

A woman contacted a law firm and met with a legal advisor looking to set up some companies under the *Canada Business Corporations Act*. She presented valid identification and said she is a dual citizen of Canada and a country that poses a geographic risk. She was not employed in Canada, but acted as a director of several corporations in other jurisdictions. She described these other corporations in general terms, stating that most were in the importing and exporting business. The woman gave a similar description for the Canadian companies she wanted to set up. She told the legal advisor that the Canadian companies would initially be funded by the corporations outside the country.

The woman provided documentation and the law firm conducted a search of the corporations, which were verified but appeared to be mainly holding companies. The law firm and the woman entered into engagement retainer agreement. After the legal advisor began setting up the Canadian companies, as instructed, she came across news articles indicating that, even though they had different family names, the client appeared to be the daughter of a former well-known head of state, accused of corruption.

RED FLAGS



- Client is a citizen of a country that poses a geographic risk.
- Client is a director of several corporations in multiple jurisdictions.
- Client can only provide general descriptions of the companies of which she is a director.
- Reason for setting up the new corporations is vague.
- Source of funds is uncertain.
- Funding for the new Canadian corporations is coming exclusively from outside the country.
- Client appears to be a politically exposed person, or have links to one.
- Client's role as director could be an attempt to disguise the real owner or parties to the transaction.

What can you do?

In a situation like this you should make further inquiries about the source of funds and business plan for the companies to be set up in Canada and the client's actual role in these and other corporations. You should also take steps to determine whether the client is a PEP. There are a number of online lists of PEPs. Before acting in such a case, you must be satisfied on reasonable grounds that the matters for which you are being retained are legitimate.

SCENARIO: International politically exposed person investing in Canada

An individual approached a senior lawyer in a law firm to act for him in the purchase of a local sports franchise. The lawyer and the firm were pleased because the firm's sports law work had been declining lately. The potential client was a wealthy individual who made his fortune in the mining industry in a country that poses a geographic risk due to a high level of corruption. The law firm completed its client identification and verification checks and found out that the client was heavily involved in politics in his home country, serving as a member of the national legislature and, at one time, minister of natural resources. These positions made the client a foreign PEP as defined under Canadian anti-money laundering legislation.

The senior lawyer raised the issue of source of funds with the client who responded that the acquisition would be funded out of the proceeds of the sale of one of his former mining businesses. The law firm accepted the engagement. During the course of advising on the proposed investment, a junior lawyer brought to the attention of the senior lawyer a news article reporting that the client had been accused of bribery in obtaining the mining concessions on which his fortune was built. Further, during his time in politics, the client was implicated in an expenses scandal, although a parliamentary investigation found him not guilty of these accusations.

The senior lawyer raised this issue (accusation of bribery) with the client and the client explained that the charges were politically motivated and were made up by an opponent to discredit him. The law firm accepted the client's explanation. A couple of years later, a foreign court convicted the client of bribery and corruption in connection with the mining rights and the parliamentary investigation, which had been conducted by a close associate, and ordered the client's assets frozen.



RED FLAGS

- Client obtained his wealth from a country that poses a geographic risk.
- Mining and natural resource extraction in a country with high corruption may pose a higher risk for money laundering.
- Client is a politically exposed person.
- Client is the subject of allegations of corruption.

What can you do?

You should engage in more thorough risk assessment and due diligence when the client is a PEP or is from a high risk country or region. In this case, the client is both. You should undertake independent research instead of relying on the client's explanation. Before acting or continuing to act for a client in these circumstances, you must be satisfied on an objective basis that you are not facilitating a criminal offence.

SCENARIO:

Multiple high-risk factors relating to an international transaction

An individual attended at the office of a mid-sized law firm without a scheduled appointment seeking legal advice on setting up a business. He told the legal advisor he was an international businessman from a country in Europe and was in the process of moving to Canada. He said that he had secured \$700K in funding for the Canadian business from a company located in a country that poses a geographic risk. When asked for identification, he told the legal advisor he misplaced his passport in the move and had applied to replace it. He produced a photocopy of some temporary travel papers and promised to bring in his new passport as soon as it was issued. He also produced the investment agreement with the company from the high-risk jurisdiction.

The agreement was very basic and did not appear to have been drafted by a lawyer/legal professional. The individual said the funds would be wired by the company from a bank account in a country known for banking secrecy. The legal advisor performed an Internet search on the individual, his other businesses, and the investing company. The search showed that the individual had a very common name in his jurisdiction making it difficult to verify information on him. A Facebook page was found for one of his international companies, but the site had only the company's name, a low resolution logo and a street address with no phone number or email. The legal advisor did not find any information on the investing company.

RED FLAGS



- Client shows up at the law office without an appointment or prior phone or email contact despite the relatively large investment at stake.
- Client and investing company are both located in high-risk countries.
- Client's connection to the jurisdiction is unclear beyond desire to start a business there.
- Client is not able to present valid identification.
- There is little to no information available on the potential client, his business or investing company.
- The purported investment agreement documentation is uncharacteristically simple for the nature of the transaction.
- Funding is arriving from a jurisdiction known for banking secrecy.

What can you do?

You must satisfy the requirements under your regulator's client identification and verification rules. Given the lack of information on the client, his business and the investing company, you should conduct a risk assessment on the client and the other parties to the transaction to find out who they are and determine the source of funds. You should decline to act where there are multiple high-risk factors, as in this case.

SCENARIO:

Failure to consider who controls the client

A corporation retained a law firm in relation to the sale of assets. The corporation “passed” the law firm’s client identification and verification checks and provided documentation on the client’s ownership of the assets. In email communications with the legal advisor, the client copied several other individuals and asked that these individuals be included in future emails from the law firm.

When complications arose on the asset sale, a previously unidentified individual started to attend meetings and appeared to be leading the discussions and decisions for the client. It emerged that this individual had an outstanding warrant for fraud and was making decisions for the client despite holding no formal role with the corporation.



RED FLAGS

- Client is requesting that individuals with no apparent relation to the client be included in communications or meetings.
- Client decisions and instructions appear to be coming from a third party.
- Actual directing party has been charged with fraud.
- There appears to be an attempt to disguise the real owner or parties to the transaction.

What can you do?

You may only take instructions from third parties in very limited circumstances, and only after verifying their identity and obtaining the clear consent of the client. The absence of a logical explanation for the role of the third party is a red flag. The fact that the person who is apparently directing the transaction faces criminal charges for fraud significantly increases the risk of illegal activity. In this scenario, the red flags are sufficient to suggest that the lawyer ought not to continue acting.

SCENARIO: Questionable source of funds

A legal advisor represented a company trying to create an initial public offering (IPO) for an opaque tech start-up. Due to concerns over the company's financial viability and a potentially messy ownership dispute, the company struggled to make the IPO a success. At the last minute, a previously unknown wealthy investor came along and made a substantial bid.

The money offered by the wealthy investor was actually the company's money. Representatives of the company were paying money to the purported investor to promote the investment.



RED FLAGS

- Purpose of the client company is ambiguous.
- Unexplained financing arrangements.
- Appearance of sudden willing investor when previous interest was lacking.

What can you do?

When questionable circumstances arise, such as the unexpected and last minute appearance of a wealthy investor, you should take additional steps, including requesting additional information on the source of funds, inquiring about the reasons for the investor's sudden appearance in the transaction, and/or establishing whether a relationship exists between the investor and the company. Also, when acting on an IPO, the legal advisor must have clear and detailed information on the nature of the corporation and its plans.

SCENARIO: Instructions from an overseas client

A woman who was a UK national, phoned a Canadian legal advisor specializing in estates law seeking representation in relation to the purchase of some high-value properties. The woman told the legal advisor that he came highly recommended by a close friend of hers who was a long-time client and whose opinion she valued highly. The potential client said that she understood that her matter was not in the legal advisor's primary area of practice, but what mattered most to her was that she be able to deal with someone she could trust. The woman did not intend to travel to visit the properties prior to purchasing them.

She asked that the purchases be completed as soon as possible and offered to pay the legal advisor an extra fee if the purchases were completed by a certain date. She assured the legal advisor that financing would not delay the purchase since no loans were required.



RED FLAGS

- Legal advisor being asked to advise on an area of law outside his expertise.
- Client is not planning to visit the properties, despite the high value of the transaction.
- No financing is required for the transactions despite their high value.
- Client promises to pay extra fees for speedily completing transaction.
- Client provides no explanation for an expedited transaction.

What can you do?

You must always verify a client's identity and obtain information about the source of funds when a financial transaction is involved, even for referrals from trusted sources. You should undertake additional inquiries when there are high risk indicators, such as the client not visiting the properties, paying for high value properties without financing, asking you to take on a matter outside your areas of expertise or requesting you to expedite the transaction without a logical explanation. It is good practice to check any referral source. You can ask the client who referred them, and request consent to contact the referral source. If the client says "no", that is an additional red flag. If the client says "yes", you may discover that the source doesn't know the client well or at all, which may also be a red flag.

SCENARIO: Performing due diligence on other parties to a transaction

A Canadian company was a longstanding and major client of a large law firm. The company planned to acquire a construction entity based in a country that poses a geographic risk. The client wanted the entity for its many lucrative government contracts. Very late into the negotiations, it was revealed that the construction entity had made a large number of payments to companies described in the records only as “consulting services”. Establishing the identity of the consultants or the exact nature of the services they provided was difficult. The legal advisors recommended that the client obtain more information about the consultant contracts and the fees paid under those contracts.

On a more detailed analysis, it became apparent that many of the consultants were linked to government officials responsible for awarding public contracts, licenses and permits. No details as to the precise services performed for the construction company were provided. The law firm became concerned that the fees might constitute bribes paid by the construction entity to secure contracts. The legal advisor informed the client that the construction entity it planned to purchase may have obtained its contracts through illegal acts and that the resulting revenue could constitute the proceeds of crime. Since the client was very interested in acquiring the entity, it asked the law firm to proceed with the transaction.



RED FLAGS

- Involvement of a higher-risk jurisdiction.
- Difficulty in obtaining satisfactory information related to services being provided to the target construction company and related to the payments it made.
- Certain assets of the entity being purchased (i.e., construction contracts) appear to have been illegally obtained.

What can you do?

As a legal advisor you have an obligation to satisfy yourself that the transaction with which you are assisting is legal. In this scenario, you would have to inform the client that you could not complete the transaction unless additional information and supporting documentation was obtained to demonstrate the contracts were not illegally acquired. It is important to undertake appropriate risk assessment and due diligence, and to seek additional information when concerns arise. This may occur at any stage of the transaction. In the circumstances of this scenario, seeking further clarification was part of the legal advisor’s duty of care to the client.

SCENARIO:

Third party involvement in an expedited transaction

Legal advisor A is good friends with legal advisor B, whom she has known for years as their practices are similar. B called A and advised that a former client needed assistance with papering a loan that the client was going to make to Company X. B told A that she did not know much about the matter and could not act because she had a trial coming up. A didn't know (and didn't ask) any details about B's relationship with the client, including whether B had complied with the client identification and verification rules. A met with the client, who attended with two other individuals: the person to whom the client had made the loan at issue; and, a third party, introduced only by his first name. No information was provided about the third party's relationship to the lender or the borrower.

The third party did most of the talking during the meeting, explaining that the client lent \$500,000.00 to the borrower a few months ago at an interest rate of 30%. The third party said the proposal was to place a mortgage on the borrower's property for the loan. The third party told A that the borrower was leaving the country shortly on a business trip so they would need to get everything set up and signed immediately. Before anyone asked what A would charge for the retainer, the third party said they could pay her fees with cash or run out to get a bank draft.

RED FLAGS



- No certainty that the client(s)/beneficial owners have been properly identified/verified.
- Involvement of a third party, whose relationship to the client and other parties is not known.
- Both client and other party meet with the lawyer together despite obvious conflict of interest issues.
- Third party appears to be in control of client and other party, and gives instructions.
- Desire to complete the transaction very quickly (i.e. same day).
- Third party offers to pay lawyer's fees in cash or bank draft right away without knowledge of the lawyer's rate.

What can you do?

You should always ensure you know who the client is. Clarify the relationship of any third parties who may appear to be controlling or wanting to give instructions on behalf of the named client. You need the client's clear consent before accepting instructions from a third party and have an obligation to identify and verify the identity of the third party in such circumstances. You should also always assess and communicate any potential conflicts of interest if multiple parties are looking to retain you. It is important to be cautious when faced with a client seeking a transaction within a very short timeline and expressing a willingness to pay your fees immediately in cash without first learning your rate or an estimate of the final bill. You should also avoid entering into a joint retainer with the borrower and lender in private loan agreements.

5. DISPUTES AND LITIGATION

SCENARIO:

Claim for debt recovery with little substantive legal work required

A foreign company retained a legal advisor at a small firm to commence a debt recovery claim against a company located in the firm's jurisdiction. The legal advisor's main area of practice was employment law. At the time, he was busy with several large files. However, the matter appeared straightforward and he decided to take it on. A search verified the identity of the debtor company as a registered corporation, but it was not clear whether it had any assets in the jurisdiction. The legal advisor told the client, but the client did not seem concerned and instructed the legal advisor to proceed with the claim.

After one initial phone call with the legal advisor, the client only communicated via email. The legal advisor asked the client to send him documents to support the debt claim. The client sent a scanned copy of an invoice marked "unpaid" by email. The defendant company did not contest the claim and a default judgment was entered. The legal advisor served the default judgment on the defendant company and a demand letter explaining how to make payment. The defendant company responded by immediately transferring the sum into the law firm's trust account.

RED FLAGS



- Legal services sought by client are beyond the expertise of the legal advisor.
- Foreign company without an obvious connection to the place of litigation.
- Defendant company with no apparent assets in the jurisdiction.
- Limited documentation on the nature of the debt underlying the claim.
- Defendant does not contest default judgment.
- Defendant pays the amount with little debt recovery work required by the legal advisor.

What can you do?

It may be difficult to establish whether one is dealing with fictitious claims, but you must keep an eye out where matters seem to be proceeding too smoothly. You should also be cautious when being asked to take on matters outside your usual area(s) of practise. In this scenario, the legal advisor should have been alerted by the client's lack of concern about the defendant appearing to have no assets in the jurisdiction and the ease with which the litigation was settled. You should always obtain an explanation when asked to provide unused or excess trust funds to a third party since this can increase the risk of money laundering. To avoid this, you should return trust funds to the client or the original payor (if received from someone on behalf of the client).

SCENARIO:

Demand letter and settlement with little substantive legal work

A legal advisor was approached by a new potential client who asked for help regarding a dispute with the owner of ABC Ltd. The client said that the owner of ABC Ltd. convinced her to invest in his company by regaling her with its impressive sales numbers and promising the imminent global launch of ABC's product. The client bought shares in ABC Ltd. for \$100,000 with the expectation that the shares would be worth at least \$600,000 within 12 months. The client said that she now realizes that the owner of ABC Ltd. duped her and that the shares she bought are worthless. Although the legal advisor was busy with several tight deadlines on other files, he agreed to prepare a demand letter. He did not ask her for any documents since he thought the client had told him what he needed and he was only making a demand at this stage.

He sent the demand letter to a Hotmail email address that the client provided for the owner of ABC Ltd. The owner replied within days and agreed to buy-back the client's shares for \$500,000. The client was delighted and asked for the payment to be made by ABC Ltd. into the legal advisor's trust account, and then paid out equally to two separate numbered companies that she controlled. A few days later, the legal advisor received the settlement funds into his trust account by wire transfer from a country known for banking secrecy. The client thanked the legal advisor by giving him a \$5,000 bonus on top of his fees.

RED FLAGS



- Client's loss relates to misleading and potentially fraudulent activity.
- Free online email (i.e., Hotmail) is used to communicate with corporate party.
- Settlement funds are paid very quickly and without explanation following the demand letter, particularly large sums.
- Settlement funds are received from an account located out of the country without explanation.
- Client requests, without explanation, that settlement funds on a personal debt be sent to two corporate accounts with no apparent connection to the dispute.
- Client pays a bonus in addition to fees.

What can you do?

When acting for clients on a claim or demand for recovery of a debt or actionable loss, you should request and review documents supporting the debt or loss. In this scenario, the fact that the client claimed to have lost the money in potentially fraudulent circumstances ought to have reinforced the need for investigation into the nature of the debt. The other red flags, including the quick payment of settlement funds following a simple demand letter and the payment coming from out of the country, suggest this situation is high-risk for money laundering. If a client makes specific unusual requests about how to transfer the funds (e.g., to unrelated corporate accounts) you should make inquiries as to the reason for these instructions.

APPENDIX

RED FLAGS QUICK REFERENCE GUIDE

This appendix provides a list of red flags that indicate potential risks of money laundering and other illegal activity, including fraud. They are arranged by the nature of the risk.⁹ This list is not exhaustive and is intended as a quick reference guide to identify common red flags. Other circumstances may arise suggesting a particular client or transaction poses a money laundering risk.

Identity of the client

- Reluctant to provide or refuses to provide information relating to their identity and/or the identity of a beneficial owner or controlling interest.
- Provides false information or counterfeited documentation in relation to their identity and/or the identity of a beneficial owner or controlling interest.
- Known to have convictions or to be currently under investigation for acquisitive crime, or has known connections with criminals.
- Age or capacity of the client is unusual for the transaction, especially if they are under legal age and there is no logical explanation for their involvement.
- Business entity that has no internet presence at all, cannot be found in corporate registries, and/or is only using an email address from a free web-based email provider (e.g., Hotmail, Gmail, Yahoo, etc.), especially if the client is otherwise secretive or avoids direct contact.
- Business is in cash-intensive industries that are not usually cash-rich but generate substantial amounts of cash (e.g., money-service businesses and casinos).
- Structure of the client organization makes it difficult to identify its beneficial owner or controlling interests (e.g., the unexplained use of legal persons or legal instruments).
- Domestic or international politically exposed person (PEP); i.e. 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.
- Originally from, a resident of, or owner of a company incorporated in a high-risk country as identified by credible sources (e.g., Government of Canada, FINTRAC, FATF, UN) as:
 - o Generally lacking appropriate AML laws, regulations and other measures;
 - o Being in a location from which funds or support are provided to terrorist organisations; or
 - o Having significant levels of corruption or other criminal activity.
- 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.

⁹ This list is based on resources from the Financial Action Task Force, the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe.

APPENDIX

RED FLAGS QUICK REFERENCE GUIDE

Behaviour of the client

- Overly secretive or evasive about:
 - o Their identity
 - o Their address or contact information
 - o Identity of the true client
 - o Identity of the beneficial owner
 - o Where the money is coming from (i.e., source of funds)
 - o Why they are doing the transaction this way
 - o The overall reason for, or purpose of the transaction i
- Chooses a legal advisor who is:
 - o At a distance from the client or the transaction without legitimate or economic reason.
 - o Without experience in a particular specialty or without experience in providing services in complicated or especially large transactions.
- Has changed legal advisor a number of times in a short time or engaged multiple legal advisors without legitimate reason.
- Uses an agent or intermediary without good reason.
- Uses financial intermediaries that are neither subject to adequate anti-money laundering laws nor adequately supervised by authorities.
- Is evasive or actively avoiding personal contact without good reason.
- Is prepared to pay substantially higher fees than usual or bonus for services that would not warrant such a premium or without good reason.
- Demonstrates an excessive desire to expedite the transaction and/or offers an incentive to complete the transaction by a certain date (e.g., higher fee or bonus), without a good reason.
- Changes settlement or execution instructions multiple times or in a short period of time 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.
- Provides false or counterfeited documentation.
- Demonstrates unusual familiarity with the ordinary standards provided for by the law in satisfactory customer identification, data entries and suspicious transaction reporting or asks repeated questions on related procedures.

APPENDIX

RED FLAGS QUICK REFERENCE GUIDE

Source of Funds/ Source of Wealth

- Transaction involves a disproportionate amount of private funding, bearer cheques, bank drafts or an attempt to use cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.
- Source of funds is unusual, e.g.:
 - o Third party funding for the transaction with no apparent connection or legitimate explanation.
 - o Funds received from or sent to a foreign country when there is no apparent connection between the country and the client.
 - o Funds received from or sent to high-risk countries.
- Client is using multiple bank accounts and/or foreign accounts without good reason.
- Client funds provided for a transaction appear to be large relative to the client's income without logical explanation.
- Personal private expenditure is funded by a company, business, or government.
- Collateral being provided for the transaction is currently located in a higher-risk country
- Unusually short repayment period has been set without logical explanation.
- Mortgages are repeatedly repaid well before the initially agreed maturity date, with no logical explanation.
- High value transaction does not require financing.
- Asset is purchased without financing and then rapidly used as collateral for a loan.
- Request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested that are not appropriate for the common practice used for the ordered transaction.
- Financing provided by a lender other than a bank or credit institution with no logical explanation or economic justification.
- 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.
- Increase in capital from a foreign country, which either has no relationship to the company or is high risk.
- Business receives an injection of capital or assets suddenly and/or notably high in comparison to the business, size or market value of the company, with no logical explanation.
- Excessively high or low price attached to the securities transferred.
- No legitimate explanation for 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.

APPENDIX

RED FLAGS QUICK REFERENCE GUIDE

Nature of the retainer or transaction

- Transaction is unusual, e.g.:
 - Type, size, frequency, manner of execution of transaction is unusual for or inconsistent with the size (entity), age, or activity of the client.
 - Remarkable and highly significant differences between the declared price and the approximate or actual values in accordance with any reference that could give an approximate idea of this value or in the judgement of a legal advisor.
 - Non-profit organization requests services for purposes or transactions not compatible or typical with those declared for that body.
- Requested service was refused by another legal advisor or professional or the relationship with another legal advisor or professional was terminated.
- Transaction does not correspond to client's normal professional or business activities.
- Client lacks suitable knowledge of the nature, object or the purpose of professional services requested.
- Client wishes to establish or take over a legal person or entity with a dubious description of the aim, or a description that is not related to client's normal professional or commercial activities or his other activities.
- Client frequently changes legal structures and/or managers without legitimate reason.
- Unexplained changes in instructions, especially at the last minute.
- Client asks for short cuts or unexplained speed in completing the transaction.
- Client requires introduction to financial institutions to help secure banking facilities in the context of the transaction.
- Client instructs the creation of complicated ownership structures when there is no legitimate business or economic reason.
- Involvement of entities in multiple countries where there is no apparent link to the client or transaction, with no legitimate or economic reason.
- Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation.
- Absence of documentation to support client's story, previous transactions, or company activities.
- Several common elements in a number of transactions in a short period of time without logical explanation.
- Back-to-back property transactions, with rapidly increasing value or purchase price.
- Abandoned transactions with no concern for the fee level or after receipt of funds.
- Retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the legal advisor's trust account without the provision of legal services.
- Lack of sensible commercial/financial/tax or legal reason for the transaction.
- Increased complexity in the transaction or the structures used for the transaction that result in higher taxes and fees than apparently necessary.
- Power of attorney is sought for the administration or disposal of assets under conditions that are unusual, where there is no logical explanation.
- Investment in immovable property, without any links to the place where the property is located and/or without any financial advantage from the investment.
- Litigation is settled too easily or quickly, with little to no involvement by the legal advisor retained.
- Includes requests for payments to third parties without substantiating reason and/or corresponding transaction.

APPENDIX

RED FLAGS QUICK REFERENCE GUIDE

Parties

- Originally from, resident or incorporated in a country posing a high risk to money laundering.
- No apparent business reason connecting the parties to the transaction.
- Ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature/reason of the connection.
- Multiple appearances of the same parties in transactions over a short period of time.
- Age or capacity of the executing parties is unusual for the transaction, especially if they are under legal age and there is no logical explanation for their involvement.
- Attempts to disguise the real owner or parties to the transaction.
- Business entities cannot be found and/or have no presence on the internet and/or in corporate registries.
- Person directing the operation is not one of the formal parties to the transaction or the representative.
- Natural person acting as the director or representative does not appear to be a suitable representative.



**Anti-Money Laundering and Terrorist Financing
Working Group**

Risk Advisories for the Legal Profession

**Advisories to Address
the Risks of
Money Laundering
and Terrorist Financing**

December 2019

About These Risk Advisories

The nature of legal practice makes it vulnerable to targeting by criminals seeking to launder the proceeds of crime or facilitate the financing of terrorist activities. Canadian legal professionals assist clients with the purchase and sale of real estate, the creation of corporations and trusts, and the acquisition and sale of businesses. They act as intermediaries for a wide range of financial transactions. Millions of dollars in client funds flow through lawyer trust accounts every year.

Criminals seek out legal professionals because their services may be required to complete certain transactions and 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 involvement of legal professionals can also lend an air of respectability to transactions undertaken by criminals seeking to convert the proceeds of crime into “clean” money.

Members of the legal profession in Canada are subject to a number of rules and regulations designed to mitigate the risks of becoming involved in money laundering and terrorism financing. These include requirements to identify and verify the identity of clients and third parties, manage risks, and understand the client’s financial dealings in relation to the retainer. Lawyers and Quebec notaries also must comply with rules that limit how much cash they may receive, and restrict the use of trust accounts. Members of the legal profession are also prohibited from assisting with or facilitating illegal conduct and have a positive duty to withdraw if continuing to act for a client would breach this rule.

To address the money laundering and terrorism financing vulnerabilities they may face legal professionals need to be aware of the risks that may be inherent in legal practice. Some risks may be related to the clients and their activities; others may arise from the nature or circumstances of a transaction. Some risks may be more likely to arise in specific practice areas, others may arise regardless of the area of practice.

The following advisories address risks arising in five areas: real estate, trusts, private lending, shell corporations, and litigation. They are intended to highlight specific client and transaction risks. While not exhaustive, the lists of risks will assist legal counsel in recognizing situations where additional due diligence may be required. The advisories also remind lawyers and Quebec notaries of the need to be satisfied, on an objective basis, that the transaction or other activity for which a client is seeking assistance is legitimate before acting or continuing to act on the matter.

Risk Advisory for Real Estate	Page 2
Risk Advisory for Shell Corporations	Page 5
Risk Advisory for Private Lending	Page 8
Risk Advisory for Trusts	Page 10
Risk Advisory for Litigation	Page 12

AML Risk Advisory: Real Estate

When does this risk advisory apply?

Real estate is a popular vehicle for those engaged in fraud and money laundering. It is generally an appreciating asset and its sale can lend legitimacy to the appearance of funds.

Consequently, the purchase of real estate is a common outlet for criminal proceeds. Fraudsters and other criminals often go to great lengths to ensure that real estate transactions used to launder funds look legitimate, masking the true intent of the transaction, which could be a purchase, sale or refinancing.

Given the significant role members of the legal profession play in real estate transactions, to avoid assisting or furthering illegal activity, they must be aware of the risks associated with providing legal services in this area. Where there are suspicious circumstances, a legal professional must be satisfied on an objective basis that the transaction is legitimate, prior to acting or continuing to act.

Fraud in real estate generally occurs as:

- Fraud for shelter - to obtain a property for legitimate purposes, but by misrepresenting facts to obtain financing or to mask the identity of the beneficial owner.
- Fraud for profit – to acquiring large sums of money from different parties including a registered owner, a mortgagee or a bona fide purchaser by fraudulent means.

The proceeds of real estate fraud are the proceeds of crime. Laundering of the funds occurs when they are provided for the transaction, often flowing through the trust account of a lawyer or notary, and are disbursed at the direction of the fraudster.

Criminals will also attempt to use funds earned from other illicit activities to purchase and eventually sell real property, converting the illicit funds into legitimate funds. They may also use the property to house illegal activity, or as a vehicle to launder additional funds.

What are risk factors?

While the indicators of fraud and indicators of money laundering activity often overlap, it is important to be aware of the risks of both and develop mitigation strategies. Many of the common risks are identified in the table below, but these lists are not exhaustive. While it is not possible to completely eliminate all of the risks, lawyers and Quebec notaries must conduct proper due diligence. This involves taking into consideration the indicators of fraud and money laundering and relying on prior experience in these types of transactions. Even if not handling the money, a legal professional engaged on a transaction will be aware of the financial details and in many cases will be in a position to ask further questions about the transaction. If satisfied that a transaction is legitimate, lawyers and notaries must comply with all requirements to properly identify and verify the identity of clients, record this information and ensure proper accounting for the transactions.



Client Risks (Real Estate)	Real Estate Fraud	Money Laundering
The company or individual has no e-mail address, physical address, home or business telephone number (disconnected or fake), company logo, contact person.	X	X
The client uses a post office box or general delivery address where other options are available.	X	X
A party to the transaction is a foreign buyer, either an individual or company, notable especially if on a watch list, whose only connection to Canada is the real estate transaction.		X
The client refuses to provide their own name on documents, or uses different names on offers to purchase, closing documents and deposit receipts.	X	X
The legal advisor experiences difficulty obtaining necessary, reliable information to identify the client and verify the client's identity.	X	X
The client insists on choosing the agent where an agent is being used to verify identity.	X	X
The client changes instructions regarding amounts or payees just before closing, or fails to bring in funds as promised.	X	
The client does not care about the property, price, mortgage interest rate, legal and/or brokerage fees, and offers to pay higher than usual legal fees for the legal services for the transaction.	X	X
The client does not appear familiar with property.	X	
The client will not permit contact with a prior legal counsel.	X	
The client is "out of sync" with the property (e.g. occupation, personal wealth, level of sophistication).	X	X
A stranger who appears to control the client attends to sign documents.	X	X
One spouse or business partner is mortgaging equity in a property owned by both.	X	
The client buys and sells often, preferring to deal in cash.	X	
The client contact is only or primarily by email.	X	X
The client has owned vacant, disused or run-down properties for a long time, without activity on title or visible use of land.	X	
Corporate client officers and directors were appointed very recently.	X	
The company purchasing real estate has a complex ownership structure.		X
The head office of a corporate client is or has been recently changed to a non-existent address or one that is highly unusual or lacks credible explanation.	X	X
The client pushes for a fast closing.	X	
The client who has been named in the media as being involved with criminal organizations is purchasing a residential property.	X	X



Transaction Risks (Real Estate)	Real Estate Fraud	Money Laundering
The same legal advisor is acting for all parties, except legitimate vendor.	X	
Funds are directed to parties with no apparent connection to the borrower or the property.	X	X
Repeat activity occurs on a single property or for a single client. The title shows one or more recent transfers, mortgages, or discharges.	X	X
Frequent and quick mortgage discharges occur on the property.	X	
The transaction location is distant from the lawyer's office.	X	X
A buyer of income-generating property has no concern for generating profit by filling vacancies or by adjusting rent/lease rates.		X
The client produces a small deposit relative to price, or pays little or nothing from their own funds.	X	
The sale is presented as a "private agreement" – no agent is involved, or the named agent has no knowledge of the transaction.	X	X
The municipality or utility companies have no knowledge of the client's ownership.	X	
Unusual adjustments are made in favour of the vendor; the transaction involves a large vendor take-back mortgage or an existing mortgage on a purchased property is assumed by another individual without involvement of a financial institution.	X	X
Payments from the client are received by way of counter cheques, bank drafts and/or cash.	X	X
The transaction involves purchase of personal use property through a business.		X
Transactions involve a Power of Attorney or are carried out on behalf of minors, incapacitated persons or others who may not have sufficient economic capacity.	X	X
Behaviour or transactions are unusual compared to other similar clients (e.g. high levels of assets, volume of transactions, nature of business activity).	X	X
The transaction involves 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.		X
Last-minute transfers contemplating "Trustee" arrangements such as "Trustee to beneficial owner" are made at NIL consideration followed immediately by the registration of a mortgage and the advance of mortgage proceeds.	X	
An accelerated repayment of a loan/mortgage occurs shortly after the deal is completed even if penalties are incurred.		X
Transactions 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.		X
The client makes a deposit for a house, reneges on the deal shortly thereafter, then obtains a legitimate cheque from the legal advisor for the value of the deposit. non-existent address or one that is highly unusual or lacks credible explanation.		X

AML Risk Advisory: Shell Corporations

When does this risk advisory apply?

Lawyers and Quebec notaries must be alert to the risks of becoming involved with a client engaged in criminal activity such as money laundering. Vigilance is required because the means for these, and other criminal activities, may be transactions for which lawyers commonly provide services.

Criminals are increasingly turning to shell companies to facilitate money laundering. Anonymous shell companies allow criminals to hide their identities, conceal the origin and flow of money, hide the identities of true beneficiaries or enhance the perception of legitimacy. They are typically used during the “layering phase” of money laundering involving often complex financial transactions designed to hide the illegal source of funds.

Legal advisors must be aware of the risks when dealing with clients looking for assistance with products or transactions that would facilitate anonymity and allow beneficial owners to remain hidden without a reasonable explanation. While client identification and verification rules are essential to ensure that lawyers know their clients, it is imperative that lawyers and notaries also understand the facts relating to their retainers, particularly when a shell corporation is involved.

They must ask probing questions to ensure that they understand the subject-matter and objectives of their retainers, including:

- i) whether there is a legitimate business or legal reason for using a particular corporate structure;
- ii) who are the legal and beneficial owners of the property and business entities;
- iii) who has control of the business entities; and
- iv) where it is unclear, what is the nature and purpose of complex or unusual transactions.

Legal advisors must be satisfied on an objective basis that every transaction is legitimate, prior to acting or continuing to act.

What are risk factors?

To address the risks, lawyers and Quebec notaries should be on the lookout for suspicious circumstances, including the following when setting up or representing shell corporations:



Description of Risk (Shell Corporations)	Client Risks	Transaction Risks
The retainer involves a non-face-to-face transaction where the legal advisor has not previously met the client seeking to establish a shell corporation or the agent of the corporation in person.	X	
The client or corporation's reasons for selecting the lawyer are unclear given the lawyer's geographic location or practice area.	X	
The lawyer is not asked to provide any legal services other than assisting with the creation of the shell corporation.	X	
The corporation is transacting with a party that has a suspected or known history of drug trafficking, money laundering, actions resulting in civil forfeiture, loansharking, fraud, high-stakes gambling or similar activity.	X	
The lawyer experiences difficulty obtaining necessary, reliable information to identify an agent of the corporation or verify the agent's identity.	X	
Insufficient information is provided by the client to identify the beneficial owners of the corporation.	X	
Third parties or intermediaries are involved, including in providing instructions.	X	
The corporation has been refused counsel or changed counsel recently or several times without apparent good reason.	X	
The corporation has no or nominal assets, or assets consisting solely of cash and cash equivalents.	X	
The corporation was incorporated in a jurisdiction that might enable anonymity.	X	
The corporation's financial transactions occur in a jurisdiction that minimizes transparency or provides an environment more amenable to money laundering.	X	
Gaps or red flags in the corporation's online presence are evident. One spouse or business partner is mortgaging equity in a property owned by both.	X	
Inconsistent information exists relating to the corporation; e.g. a corporation doing business in one jurisdiction has an address and contact information in one or more other jurisdictions.	X	
The lawyer encounters contact concealment, e.g. a generic email address, no physical address, etc.	X	
The client offers to pay an unusually high fee for the legal services.	X	
The lawyer is not asked to provide any substantial legal services in connection with the transaction.		X
The lawyer cannot obtain information necessary to identify the originator or beneficiary of a transaction.		X
The corporation's transactions appear inconsistent with the corporation's or the other party's profile/circumstances (e.g. age, income, geographic location or occupation).		X



Description of Risk (Shell Corporations)	Client Risks	Transaction Risks
The corporation transacts through a foreign bank and exceeds the anticipated volume projected in its client profile for wire transfers in a given time period, or the corporation exhibits a high level of sporadic activity that is inconsistent with normal business patterns.		X
A corporation makes payments that have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.		X
The goods or services of the company do not match the company's profile based on information provided by the client.		X
The corporation transacts with businesses sharing the same address.		X
The client's business discloses the frequent involvement of beneficiaries located in high-risk, offshore financial centers.		X
Multiple high-value payments or transfers are made or instructed between shell companies with no apparent legitimate business purpose.		X
The client attempts cash transactions with an inability to explain the source of funds/wealth.		X
The client uses partial signatures on contracts and/or invoices		X
The lawyer is retained to complete a transaction after funds have already been advanced or after a loan agreement or a security agreement has been signed.		X
Transaction documents are unusual or inconsistent with the client's explanation of the transaction.		X
The corporation transacts from an offshore jurisdiction that is known to be secretive or restrictive.		X

AML Risk Advisory: Private Lending

When does this risk advisory apply?

Criminals may attempt to use private lending transactions to launder the proceeds of crime, and may engage the services of lawyers for the transactions.

Members of the legal profession must know their clients and properly understand the facts relevant to their retainers. Where there are suspicious circumstances, a legal professional must be satisfied on an objective basis that the transaction is legitimate, prior to acting or continuing to act.

All lawyers and Quebec notaries should be alert to and appropriately consider risk factors associated with illegal activity when retained to do any of the following:

- Drafting, reviewing or advising on a loan agreement, promissory note, guarantee, mortgage, security agreement or other loan documents;
- Registering a security agreement for a private loan; or
- Taking any steps to assist with the advance or recovery of funds related to a private loan.

What are risk factors?

In addressing the risks, legal counsel should be on the lookout for suspicious circumstances, including the following for private lending transactions:

Description of Risk	Client Risks	Transaction Risks
The retainer involves a non-face-to-face transaction where the legal advisor has not previously met the client in-person.	X	
The client's reasons for selecting the lawyer or Quebec notary are unclear given the geographic location or practice area.	X	
A party to the transaction (or a family member or close associate) has an alleged or known history of drug trafficking, money laundering, civil forfeiture, loansharking, fraud, high-stakes gambling or similar activity.	X	
The lawyer or notary experiences difficulty obtaining necessary, reliable information to identify the client and verify the client's identity. Conversely, the client appears unusually familiar with client identification and verification requirements.	X	
The transactions involves third parties or intermediaries, including in providing instructions.	X	



Description of Risk (Private Lending)	Client Risks	Transaction Risks
The client has been refused counsel or changed counsel recently or several times without apparent good reason.	X	
The client offers to pay an unusually high fee for the services.	X	
The client's instructions change unexpectedly and for no logical reason.	X	
There is no clear or plausible reason for the borrower not borrowing from a commercial lender.		X
The loan seems inconsistent with the client's or the other party's profile/ circumstances (e.g. age, income, geographic location or occupation).		X
The lawyer or notary is not asked to provide any substantial legal services in connection with the transaction.		X
Funds are exchanged between the parties in cash but the parties are unable to explain the source of funds/wealth.		X
The borrower named in the loan documents is not the actual recipient of the funds.		X
There is no security registered for the loan, without explanation, or the security is a subsequent mortgage or charge on a fully or near-fully encumbered property.		X
The actual or agreed-to repayment period is unusually short.		X
The legal professional is retained after the funds have already been advanced or after the loan agreement or security agreements have been signed.		X
The loan documents are unusual or inconsistent with the client's explanation of the transaction.		X
The interest rate exceeds the criminal rate or is substantially above/below market rates.		X
The funds are received from or paid out to an offshore jurisdiction that is known to be secretive or restrictive.		X
The entity providing the loan proceeds (or receiving the loan payout) is not the party named in the loan documentation and the relationship between the entity and the named party is not apparent.		X

AML Risk Advisory: Trusts

When does this risk advisory apply?

While there are many legitimate uses of trusts for matters such as estate planning and asset management, members of the legal profession must be on guard against clients who wish to use such instruments for an improper or fraudulent purpose. Some criminals see trusts as potentially useful vehicles to hide the origin and ownership of assets.

Disguising the real owners and parties to a transaction is a necessary requirement for money laundering to be successful, and although there may be legitimate reasons for hiding ownership, it should be considered a red flag.

The use of trusts to purchase real property poses an increased risk that the trust will be used to obscure ownership and launder the proceeds of crime. Legal counsel who are asked to become involved in the management of a trust should be extremely wary, as this is a technique used by criminals to provide respectability and legitimacy to their activities.

Lawyers and Quebec notaries must strictly comply with client identification rules including the requirement to know their client and the source of the client's funds, and to understand the nature and scope of the retainer. Legal counsel must be satisfied on an objective basis that every transaction is legitimate, prior to acting or continuing to act.

What are risk factors?

To address the risks, lawyers should be on the lookout for suspicious circumstances, including the following when asked to create or be involved in the management of trusts:

Description of Risk	Client Risks	Transaction Risks
The retainer involves a non-face-to-face transaction where the legal advisor has not previously met the client in-person.	X	
The client's reasons for selecting the legal advisor are unclear given the geographic location or practice area.	X	
The client offers to pay an unusually high fee for the services or to provide a substantial retainer that is excessive considering the scope of the retainer.	X	
The client or a party in the matter (or a family member or close associate) has a suspected or known history of drug trafficking, money laundering, actions resulting in civil forfeiture, loansharking, fraud, high-stakes gambling or similar activity.	X	
The legal advisor experiences difficulty obtaining necessary, reliable information to identify the client and verify the client's identity, or the client appears unusually familiar with the client identification and verification requirements.	X	



Description of Risk (Trusts)	Client Risks	Transaction Risks
Third parties or intermediaries are involved, including in providing instructions, without good reason.	X	
The client has been refused counsel or changed counsel recently or several times without apparent good reason.	X	
A complicated ownership structure is created when there is no legitimate or economic reason for it.		X
There is no sensible reason for the transaction.		X
The client changes instructions without explanation, especially at the last minute.		X
The legal advisor is not asked to provide any substantial legal services in connection with the transaction.		X
The proposed retainer relates to keeping documents or other goods, holding large deposits of money or otherwise using the trust account of the lawyer or notary without the provision of legal services.		X
An existing trust agreement contains minimal details regarding the arrangement or is poorly drafted.		X
Beneficiaries are difficult to identify; beneficiaries are minors.		X
The relationship between individual people named in the trust agreement suggests that there may be no legitimate purpose to the transaction.		X
The transfer of funds is not consistent with the known legitimate income of the client.		X
The client is evasive about the source of funds for the trust.		X

AML Risk Advisory: Litigation

When does this risk advisory apply?

To avoid assisting or furthering illegal activity, lawyers must be aware of the risks associated with providing certain types of legal services. Litigation, particularly debt recovery actions, may pose risks. Criminals may attempt to launder proceeds of crime by filing and recovering on civil claims. This could, for example, involve using fabricated documents to misrepresent transactions or claim an interest in property. A lawyer should not assist a client in enforcing a contract that may be based on criminal activity.

Lawyers must know their clients and properly understand the facts relevant to their retainers. Where there are suspicious circumstances, a lawyer must be satisfied on an objective basis that the transaction is legitimate, prior to acting or continuing to act.

Lawyers should be alert to and appropriately consider risk factors when retained to assist with the recovery of funds including:

- a private loan (secured or unsecured);
- a builder's lien claim;
- a claim for recovery of capital investment;
- a claim for defective goods, including intellectual property; or
- a claim for unpaid commercial invoices.

What are risk factors?

In addressing the risks, legal counsel should be on the lookout for suspicious circumstances, including the following for private lending transactions:

Description of Risk	Client Risks	Transaction Risks
The retainer involves a non-face-to-face transaction where the legal advisor has not previously met the client in-person.	X	
The client's reasons for selecting the lawyer or Quebec notary are unclear given the geographic location or practice area.	X	
The client or a party in the matter (or a family member or close associate) has a suspected or known history of drug trafficking, money laundering, actions resulting in civil forfeiture, loansharking, fraud, high-stakes gambling or similar activity.	X	
The lawyer experiences difficulty obtaining necessary, reliable information to identify the client and verify the client's identity. Conversely, the client appears unusually familiar with client identification and verification requirements.	X	



Description of Risk (Litigation)	Client Risks	Transaction Risks
The transactions involve third parties or intermediaries, including in providing instructions.	X	
The client has been refused counsel or changed counsel recently or several times without apparent good reason.	X	
The client offers to pay an unusually high fee for the services or to provide a substantial retainer that is excessive considering the scope of the retainer.	X	
Client instructions change unexpectedly and for no logical reason.	X	
The claim settles quickly with little or no work being done by the lawyer. The defendant does not contest the claim, resulting in default judgment with the claim paid immediately.		X
The debt relates to a contract based on criminal activity.		X
The claim seems inconsistent with the client's or the other party's profile/ circumstances (e.g. age, income, geographic location or occupation).		X
The claim asserts that funds were exchanged between the parties but the client is unable to satisfactorily explain the source of funds/wealth..		X
The claim is against an individual/entity that is not the actual recipient of the funds in question.		X
The documents supporting the claim are unusual or inconsistent with the client's explanation of the transaction or with other documents.		X
No security is registered for the loan, without explanation, or the security is a subsequent mortgage or charge on a fully or near-fully encumbered property.		X
The actual or agreed-to repayment period for the debt is unusually short.		X
The interest rate for the loan exceeds the criminal rate or is substantially above/below market rates.		X
The funds to settle the claim are received from or paid out to a third party whose relationship to the parties is unknown, or to an offshore jurisdiction that is known to be secretive or restrictive.		X



GUIDANCE FOR A RISK-BASED APPROACH

ACCOUNTING PROFESSION

JUNE 2019





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 (2019), *Risk-based Approach for the Accounting Profession*, FATF, Paris,
www.fatf-gafi.org/publications/documents/rba-accounting-profession.html

© 2019 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredits coverphoto ©Getty Images

Table of contents

Acronyms	3
Executive Summary	5
Section I - Introduction and key concepts.....	7
Background and context	7
Purpose of the Guidance	8
Target audience, status and content of the Guidance.....	8
Scope of the Guidance and key features of the accountancy profession	9
Scope and Terminology	9
Key features	10
Vulnerabilities of accounting services	11
FATF Recommendations applicable to accountants.....	13
Section II – The RBA to AML/CFT.....	14
What is the risk-based approach?	14
The rationale for the new approach	15
Application of the risk-based approach	15
Challenges.....	16
Allocating responsibility under a RBA.....	19
Identifying ML/TF risk.....	19
Assessing ML/TF risk.....	20
Mitigating and managing ML/TF risk	20
Developing a common understanding of the RBA	21
Section III: Guidance for accountants on implementing a risk-based approach.....	22
Risk identification and assessment	22
Country/Geographic risk	24
Client risk	25
Transaction/Service and associated delivery channel risk	29
Variables that may impact on a RBA and on risk	32
Documentation of risk assessments.....	33
Risk mitigation.....	33
Initial and ongoing CDD (R.10 and 22).....	34
Politically exposed persons (PEP) (R.12 and R.22).....	38
Ongoing monitoring of clients and specified activities (R.10 and 22).....	39
Suspicious activity/transaction reporting, tipping-off, internal controls and higher-risk countries (R.23)	40
Section IV – Guidance for supervisors	44
Risk-based approach to supervision.....	44

Supervisors and SRBs' role in supervision and monitoring.....	44
Understanding ML/TF risk.....	45
Mitigating and managing ML/TF risk.....	46
Supervision of the RBA.....	48
Licensing or registration.....	48
Monitoring and supervision	50
Enforcement	51
Guidance	52
Training	52
Endorsements	53
Information exchange.....	53
Supervision of Beneficial Ownership requirements and source of funds/wealth requirements	54
Nominee arrangements	56
Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom an accountant provides services	58
Annex 2: Glossary of terminology.....	63
Annex 3: Supervisory practices for implementation of the RBA.....	66
Annex 4: Members of the RBA Drafting Group	69

Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client ¹ due diligence
DNFBP	Designated non-financial businesses and professions
FATF	Financial Action Task Force
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
NRA	National Risk Assessment
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

¹ In some jurisdictions or professions, the term “customer” is used, which has the same meaning as “client” for the purposes of this document.

Executive Summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that supervisors, financial institutions, and professional accountants in public practice (also referred to as “accountants” or “accountancy profession” for the purpose of this Guidance) identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.
2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a [general presentation](#) of the RBA and provides [specific guidance](#) for the accountancy profession and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the industry.
3. The development of the ML/TF risk assessment is a key starting point for the application of the RBA. It should be commensurate with the nature, size and complexity of the business. The most commonly used risk criteria are country or geographic risk, client risk, service/transaction risk. The Guidance provides [examples of risk factors](#) under these risk categories.
4. The Guidance highlights that it is the responsibility of the senior management of accountants to foster and promote a culture of compliance as a core business value. They should ensure that accountants are committed to manage ML/TF risks when establishing or maintaining business relationships.
5. The Guidance highlights that accountants should design their policies and procedures so that the level of initial and ongoing client due diligence measures addresses the ML/TF risks they are exposed to. In this regard, the Guidance explains the obligations for accountants regarding identification and verification of [beneficial ownership information](#) and provides [examples](#) of standard, simplified and enhanced CDD measures based on ML/TF risk.
6. The Guidance has a [section for supervisors](#) of the accountancy profession and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the risk-based approach to supervision as well as supervision of the risk-based approach by providing specific guidance on licensing or registration requirements for the accountancy profession, mechanisms for on-site and off-site supervision, enforcement, guidance, training and value of information-exchange between the public and private sector.
7. The Guidance also highlights the importance of [supervision of beneficial ownership](#) requirements and nominee arrangements. It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained by the accountants and made available in a timely manner to competent authorities when required.

Section I - Introduction and key concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org.

- a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the Glossary.
- b) Other relevant FATF Guidance documents such as:
 - The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
 - FATF Guidance on Transparency and Beneficial Ownership (October 2014)
 - FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs) (June 2019)
 - FATF Guidance on the Risk-Based Approach for legal professionals (June 2019)
- c) Other relevant FATF Reports such as the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018).

Background and context

8. The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012². The FATF has reviewed its 2009 RBA Guidance for accountants, in order to bring it in line with the new FATF requirements³ and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to professional accountants in public practice (hereinafter also referred to as “accountants” or “accountancy profession”- see paragraph 16 below). Accountants should also refer to the RBA Guidance for trust and company service providers, when they provide TCSP services.

9. The RBA Guidance for accountants was drafted by a project group comprising FATF members and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 4.

10. The FATF adopted this updated RBA Guidance for accountants at its June 2019 Plenary.

² [FATF \(2012\)](#).

³ The FATF Standards are comprised of the [FATF Recommendations](#), their Interpretive Notes and applicable definitions from the Glossary.

Purpose of the Guidance

11. The purpose of this Guidance is to:
- a) Support a common understanding of a RBA for the accountancy profession, financial institutions and designated non-financial businesses and professions (DNFPBs)⁴ that maintain relationships with accountants, competent authorities and self-regulatory bodies (SRBs)⁵ responsible for monitoring the compliance of accountants with their AML/CFT obligations;
 - b) Assist countries, competent authorities and accountants in the design and implementation of a RBA to AML/CFT by providing guidelines and examples of current practice, with a particular focus on providing advice to sole practitioners and small firms;
 - c) Recognise the difference in the RBA for different accountants providing diverse services such as statutory audit, financial and tax advice, insolvency related services, among others;
 - d) Outline the key elements involved in applying a RBA to AML/CFT related to accountants;
 - e) Highlight that financial institutions that have accountants as clients should identify, assess and manage the ML/TF risk associated with accountants and their services;
 - f) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to accountants, particularly Recommendations 22, 23 and 28;
 - g) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;
 - h) Support the effective implementation of action plans of NRAs conducted by countries; and
 - i) Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

Target audience, status and content of the Guidance

12. This Guidance is aimed at the following audience:
- a) Practitioners in the accountancy profession;
 - b) Countries and their competent authorities, including AML/CFT supervisors of accountants, SRBs, AML/CFT supervisors of banks that rely on the CDD performed by accountants, and Financial Intelligence Units (FIU); and
 - c) Practitioners in the banking sector, other financial services sectors and DNFPBs that rely on the CDD performed by accountants.
13. The Guidance consists of four sections. Section I sets out introduction and key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific guidance to accountants (Section III) and guidance to

⁴ See definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary.

⁵ See definition of the term 'Self-regulatory body' in the FATF Glossary

supervisors of accountants on the effective implementation of a RBA (Section IV). There are four annexes:

- a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom an accountant provides services (Annex 1);
- b) Glossary of terminology (Annex 2);
- c) Supervisory practices for implementation of the RBA (Annex 3); and
- d) Members of the RBA Drafting Group (Annex 4).

14. This Guidance recognises that an effective RBA will take into account the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile of a country's accountancy profession and the risk profile of individual accountants operating in the sector. The Guidance sets out different elements that countries and accountants could consider when designing and implementing an effective RBA.

15. This Guidance is non-binding and does not overrule the purview of national authorities⁶, including on their local assessment and categorisation of the accountancy profession based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and accountants to implement applicable FATF Recommendations effectively. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. DNFPBs should also refer to relevant legislation and sector guidance for the country in which an accountant is based.

Scope of the Guidance and key features of the accountancy profession

Scope and Terminology

16. This Guidance is for professional accountants in public practice⁷ and is aimed to help them comply with the FATF Recommendations that apply to them. Professional accountant in public practice refers to professional accountants, irrespective of functional classification (for example, audit, tax, advisory or consulting) in a firm or individual practitioners that provide professional services. The nature of services provided (e.g. statutory audit as against other professional services such as financial advice, company services) will determine the scope and depth of due diligence and risk assessment. Professional accountants should also consider their ethical obligations as set out under the Code of Ethics issued by the International Federation of Accountants (IFAC)⁸ where relevant.

17. This Guidance is not meant to apply to professional accountants in business, which includes professional accountants employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not-for-profit sector, regulatory bodies or professional bodies. Such

⁶ National authorities should however take the Guidance into account when carrying out their supervisory functions.

⁷ The term 'accountant' is used interchangeably with 'professional accountant in public practice' throughout this guidance.

⁸ [Handbook of the International Code of Ethics for Professional Accountants issued in 2018.](#)

accountants should refer to their professional code of conduct or other alternative sources of Guidance, on the appropriate action to take in relation to suspected illegal activity by their employer or a third party.

Key features

18. Accountants provide a range of services and activities that vastly differ (e.g. in their methods of delivery and in the depth and duration of the relationships formed with clients, and the size of their operation). This Guidance is written at a high-level to cater for all, and the different levels and forms of supervision or monitoring that may apply. Each country and its national authorities should aim to establish a partnership with its designated non-financial businesses and professions (DNFBP) sector that will be mutually beneficial to combating ML/TF.

19. The roles, and therefore risks, of the different DNFBP and/or professional constituents, including accountants frequently differ. However, in some areas, there are inter-relationships between different DNFBP and/or professional sectors, and between the DNFBPs and financial institutions. For example, businesses or professionals within other DNFBP and/or professional sectors or by financial institutions that may instruct accountants. In some jurisdictions, accountants may also provide trust and company services covered by the FATF Recommendations. For such activities, accountants should refer to the guidance on the risk-based approach for Trust and Company Service Providers (TCSPs).

20. Professional accountants in public practice may provide a wide range of services, to a diverse range of clients. The actual services delivered by accountants may vary between jurisdictions and the examples provided here may not be applicable in every jurisdiction. Services may include (but are not limited to) the following, though not necessarily to the same client. The FATF recommendations apply to specified activities in R.22 (see paragraph 31).

- a) Audit and assurance services (including reporting accountant work in initial public offerings);
- b) Book-keeping and the preparation of annual and periodic accounts;
- c) Tax compliance work;
- d) Tax advice;
- e) Trust and company services;
- f) Internal audit (as a professional service), and advice on internal control and risk management;
- g) Regulatory and compliance services, including outsourced regulatory examinations and remediation services;
- h) Company liquidation/insolvency/receiver-managers/bankruptcy related services;
- i) Advice on the structuring of transactions;
- j) Due diligence in relation to mergers and acquisitions
- k) Succession advice;
- l) Advice on investments and custody of client money; and
- m) Forensic accounting.

21. In many countries, accountants are the professionals frequently consulted by many small businesses and individuals when seeking general business advice and a wide range of regulatory and compliance advice. Subject to the codes of professional conduct in the relevant jurisdiction, where services are not within their competence or risk appetite or comfort zone, accountants should refuse the engagement. However, they may advise on an alternate professional advisor (such as a legal professional, notary or trust and company service provider, or another professional accountant).

Vulnerabilities of accounting services

22. Some of the functions performed by accountants that are the most susceptible to the potential launderer include:

- a) Financial and tax advice – criminals may pose as individuals seeking financial or tax advice to place assets out of reach in order to avoid future liabilities.
- b) Company and trust formation – criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements (trusts, for example).
- c) Buying or selling of property – criminals may use property transfers to serve as either the cover for transfers of illegal funds (layering stage) or else the final investment of these proceeds after their having passed through the laundering process (integration stage).
- d) Performing financial transactions – criminals may use accountants to carry out or facilitate various financial operations on their behalf (e.g. 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.).
- e) Gaining introductions to financial institutions- criminals may use accountants as introducers or intermediaries. This can occur both ways as criminals may use financial institutions to gain introductions to accountants as well.

23. Further, maintenance of incomplete records by clients as revealed during the accounting/bookkeeping services provided by accountants can be an area of higher risk. Also, preparation, review and auditing of financial statements may be susceptible to misuse by criminals where there is a lack of professional body oversight or required use of accounting and auditing standards.

24. Many aspects of this Guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply the RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. Accountants may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this guidance, accountants and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.

25. Services relating to the formation and management of companies and trusts are seen as being a particular area of vulnerability.

Formation of companies and trusts⁹

26. In some countries, accountants are involved in the formation of a company. While in other countries members of the public are able to register a company themselves directly with the company registry, an accountant's advice is sometimes sought at least in relation to initial corporate, tax and administrative matters.

27. Criminals may 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 often trusts and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies¹⁰, which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies¹¹, which can be formed by accountants, by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of corporate structures, further concealing the underlying beneficial ownership information.

Management of companies and trusts

28. In some cases, criminals will seek to have accountants involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude an accountant from acting as a trustee or as a company director, or require a disclosure of directorship positions to ensure independence and transparency is maintained. This will affect whether any funds relating to activities by the company or trust can go through the relevant accountant's client account.

Acting as nominee

29. Individuals may sometimes have accountants or other persons hold their shares as a nominee, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. In some countries, accountants are not permitted to hold shares in entities for whom they provide advice, while in other countries accountants regularly act as nominees. Accountants should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where accountants are asked to act as a nominee, they should understand the reason for this request and ensure they are able

⁹ The illustrations could also apply to other legal persons and arrangements.

¹⁰ A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

¹¹ A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

to verify the identity of the beneficial owner of the shares and that the purpose appears to be legitimate.

Accountancy services for falsified accounts and tax evasion, misuse of client accounts and of insolvency services

30. Criminals may abuse services provided by accountants to provide a sense of legitimacy to falsified accounts in order to conceal the source of funds. For example, accountants may review and sign off such accounts for businesses engaged in criminality, thereby facilitating the laundering of the proceeds. Accountants may also perform high value financial transactions allowing criminals to misuse accountants' client accounts. Insolvency practice, which may be conducted by certain accountancy professionals also pose a risk of criminals concealing the audit trail of money laundered through a company and transferring the proceeds of crime. Accountancy services may also be used to facilitate tax evasion and VAT fraud.

FATF Recommendations applicable to accountants

31. The basic intent behind the FATF Recommendations as it relates to accounting professionals is consistent with their ethical obligations as professionals, namely to avoid assisting criminals or facilitating criminal activity. The requirements of R.22 regarding customer due diligence, record-keeping, PEPs, new technologies and reliance on third parties set out in R. 10, 11, 12, 15 and 17 apply to accountants in certain circumstances. Specifically, the requirements of R.22 applies to accountants when they prepare for or carry out transactions for their clients concerning the following activities:

- a) Buying and selling of real estate;
- b) Managing of client money, securities or other assets;
- c) Management of bank, savings or securities accounts;
- d) Organisation of contributions for the creation, operation or management of companies; and
- e) Creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

32. R.23 requires that R.18, 19, 20 and 21 provisions regarding internal AML/CFT controls, measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, reporting of suspicious activity and associated prohibitions on tipping-off and confidentiality apply to accountants when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in R.22 above. Section III provides further guidance on the application of R.22 and R.23 obligations to accountants.

33. Countries should establish the most appropriate regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for accountants.

Section II – The RBA to AML/CFT

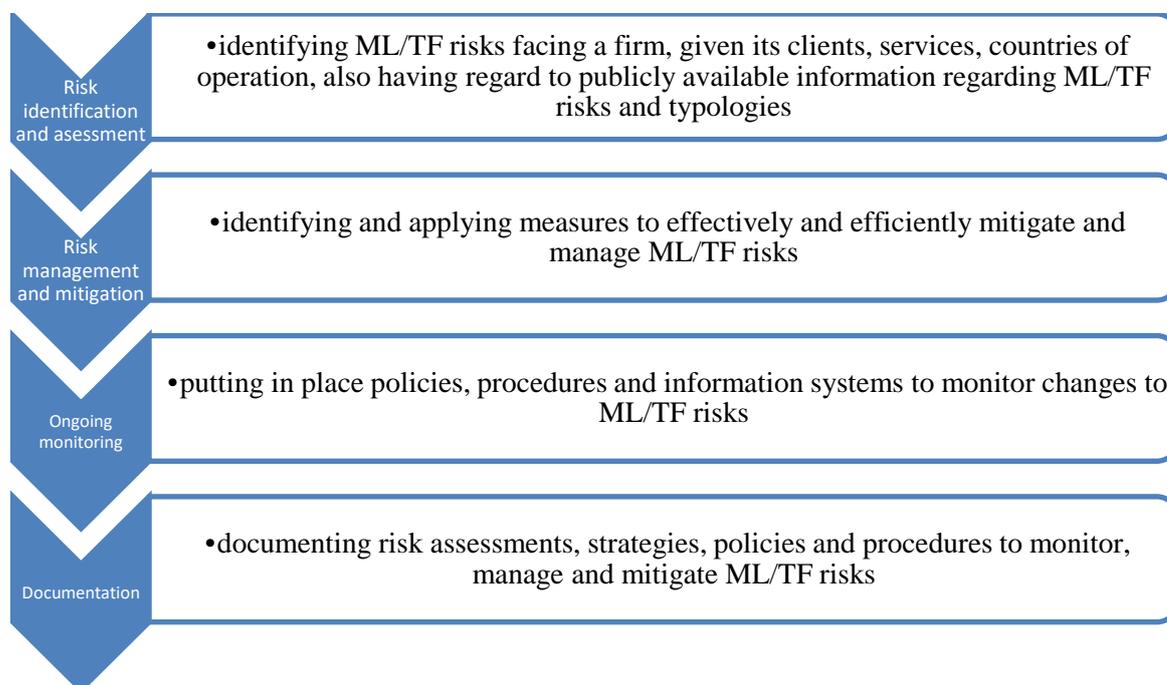
What is the risk-based approach?

34. The RBA to AML/CFT means that countries, competent authorities, DNFBPs, including accountants¹² should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

35. For accountants, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions in which they operate and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision, and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

36. The RBA is not a “zero failure” approach; there may be occasions where an accountancy practice has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that accountants must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

37. Key elements of a RBA can be summarised as follows:



¹² Including both legal and natural persons, see definition of Designated Non-Financial Businesses and Professions in the FATF Glossary.

The rationale for the new approach

38. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

39. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.¹³

40. The RBA allows countries, within the framework of the FATF requirements, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are commensurate with the nature of risks.

41. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and accountants.¹⁴

Application of the risk-based approach

42. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors, including, services, products, clients, geography and the strength of an entity's compliance program.

43. R.1 sets out the scope of application of the RBA as follows:

- a) **Who should be subject to a country's AML/CFT regime?** In addition to the sectors and activities already included in the scope of the FATF Recommendations¹⁵, countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.¹⁶

¹³ R.1.

¹⁴ The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take into account the risks and the flexibility allowed by the RBA when determining whether there are deficiencies in a country's AML/CFT measures, and their importance (*FATF, 2013f*).

¹⁵ See Glossary, definitions of "Designated non-financial businesses and professions" and "Financial institutions".

¹⁶ See INR.1.

- b) **How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime?** Supervisors should ensure that accountants are implementing their obligations under R.1. AML/CFT supervisors should consider an accountant's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.
- c) **How should those subject to the AML/CFT regime be required to comply?** The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. Accountants are required to apply each of the CDD measures under (a) to (d) below¹⁷: (a) identification and verification of the client's identity; (b) identification and taking reasonable measures to verify the identity of the beneficial owner; (c) understanding the purpose and nature of the business relationship; and (d) on-going monitoring of the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.
- d) **Consideration of the engagement in client relationships:** Accountants are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all accountants and all their clients or services pose a higher risk when taking into account the risk mitigating measures that have been put in place.
- e) **Importance of accountancy services to the overall economy:** Accountants often play significant roles in the legal and economic life of a country. The role of accountants in providing objective assurance regarding the financial status and activity of a business is vital. The risks associated with any type of client group is not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium, medium, medium-high or high risk (see section III below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

44. Implementing a RBA can present a number of challenges for accountants in identifying what necessary measures they need to take. A RBA requires resources and expertise, both at a country and sector level, to gather and interpret information on risks, to develop policies and procedures and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing such policies and procedures. It will also lead to a diversity in practice, although this can result in innovative solutions to address areas of higher risk. On the other hand, accountants may be uncertain as to how to comply with the regulatory

¹⁷ See R.10

framework itself and the accountancy profession may find it difficult to apply an informed approach to RBA.

45. Accountants need to have a good understanding of the risks and should be able to exercise sound judgement. This requires the profession, and the individuals within it, to build expertise through practice and training. If accountants attempt to adopt a RBA without sufficient expertise, or understanding and knowledge of the risks faced by the sector, they may make flawed judgements. Accountants may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, and thereby creating vulnerabilities.

46. Accountants may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. It may also encourage a 'tick-box' approach to risk assessment.

47. Developing sound judgement needs good information, and intelligence sharing by designated competent authorities and SRBs. The existence of good practice guidance, training, industry studies and other available information and materials will also assist the accountants to develop methods to analyse the information in order to obtain risk based criteria. Accountants must be able to access this information and guidance easily so that they have the best possible knowledge on which to base their judgements.

48. The services and products accountants provide to their clients vary and are not wholly of financial nature. The FATF Recommendations apply equally to accountants when they are engaged in a specified activity (see paragraph 31), including obligations related to customer due diligence, reporting of suspicious transactions and associated prohibitions on tipping off, record-keeping, identification and risk management related to politically exposed persons or new technologies, and reliance on other third-party financial institutions and DNFBPs.

Box 1. Particular RBA challenges for accountants

Culture of compliance and adequate resources. Implementing a RBA requires that accountants have a sound understanding of the risks and are able to exercise good professional judgement. Above all, management should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation, appropriate to the size, scale and activities of the organisation. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will benefit from information sharing by relevant competent authorities, supervisors and SRBs. The provision of good practice guidance by competent authorities, supervisors and SRBs is also valuable.

Significant variation in services and clients. Accountants may vary substantially in the breadth and nature of services provided and the clients

they serve, as well as the size, focus, and sophistication of the firm and its employees. In implementing the RBA, accounting (and related auditing) professionals should make reasonable judgements for their particular services and activities. Supervisors and SRBs should acknowledge that in a risk-based regime, not all accountants will adopt identical AML/CFT controls. Appropriate mitigation measures will also depend on the nature of the professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those that are engaged for distinct purposes. Where these services involve tax laws and regulations, accounting professionals also have additional considerations related to a country or jurisdiction's permissible means to structure transactions and entities or operations to legally avoid taxes.

Transparency of beneficial ownership on legal persons and arrangements¹⁸. Accountants may be involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person also may be able to conduct these activities. Where professionals do play this "gatekeeper" role, they may be challenged in obtaining and keeping current and accurate beneficial ownership information depending upon the nature and activities of their clientele. Other challenges may arise when taking on new clients with minimal economic activity associated with the legal entity and/or its owners or beneficial owners - such as start-up firms. Finally, whether the source is a public registry or the clientele, there is always potential risk in the correctness of the information, in particular where the underlying information has been self-reported (accountants should refer to the RBA Guidance for TCSPs in this respect). Those risks notwithstanding, from the outset the accountant should seek answers from the immediate client in determining beneficial ownership (having first determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company). The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the accountant is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

Risk of criminality. Because of their crucial role in providing a legally required window into the financial health and operations of a firm, accountants should be particularly alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of a substantive offence of ML/TF. Accounting (and related auditing) firms must protect themselves from misuse by criminals and terrorists.

¹⁸ Reference should also be made to the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

Allocating responsibility under a RBA

49. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Accountants should identify and assess their own ML/TF risk taking account of the NRAs in line with R.1, as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. Accountants are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.¹⁹ Where ML/TF risks are higher, accountants should always apply enhanced CDD, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

50. Strategies adopted by accountants to mitigate ML/TF risks has to take account of the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which accountants can decide how to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise how accountants manage ML/TF risks and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that accountants are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until understanding and experience of the sector is strengthened.²⁰

51. Accountants should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resources on higher risk entities.

Identifying ML/TF risk

52. Access to accurate, timely and objective information on ML/TF risks is a prerequisite for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, SRBs, financial institutions and accountants. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information on ML/TF risks and threats, or where access to information is restricted by censorship, it will be difficult for accountants to correctly identify ML/TF risk.

53. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines

¹⁹ R.1 and IN.1.

²⁰ This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP.

and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

Assessing ML/TF risk

54. Assessing ML/TF risk requires countries, competent authorities, including supervisors, SRBs and accountants to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the impact that these would have, on the individual accountants, the entire sector and on the national economy. As a starting step, ML/TF risks are often classified as low, medium-low, medium, medium-high and high. Assessing ML/TF risk therefore goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.²¹

55. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. Accounting firms/accountants that are required to routinely conduct a high volume of enquiries when on-boarding clients, e.g. because of the size and geographic footprint of the firm may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such accounting firms are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist accountants in this regard.

56. Accounting firms should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. Accounting firms should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

57. The FATF Recommendations require that, when applying a RBA, accountants, countries, competent authorities and supervisors decide on the most appropriate and effective way to mitigate and manage the ML/TF risk they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied.²²

- a) Countries may decide not to apply some of the FATF Recommendations requiring accountants to take certain actions, provided (i) 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 accountants or (ii) a financial activity is carried out by a natural or legal person

²¹ [FATF \(2013a\)](#), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

²² Subject to the national legal framework providing for Simplified Due Diligence.

on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6 are met.

- b) Countries and accountants looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of clients or services targeted, establish a threshold for the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.²³

Developing a common understanding of the RBA

58. The effectiveness of a RBA depends on a common understanding by competent authorities and accountants of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, accountants should deal with the risks they identify. Competent authorities should issue guidance to accountants on meeting their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and the sector is essential.

59. Competent authorities should acknowledge that not all accountants will adopt identical AML/CFT controls in a risk-based regime. On the other hand, accountants should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls with a RBA.

²³ For example, R.22 on Customer Due Diligence.

Section III: Guidance for accountants on implementing a risk-based approach

Risk identification and assessment

60. Accountants should take appropriate steps to identify and assess the risk firm-wide, given their particular client base, that they could be used for ML/TF. This is usually performed as part of the overall client and engagement acceptance processes. They should document those assessments, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and supervisors.²⁴ The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

61. ML/TF risks can be organised into three categories: (a) country/geographic risk, (b) client risk and (c) transaction/service and associated delivery channel risk²⁵. The risks and red flags listed in each category are not exhaustive but provide a starting point for accountants to use when designing their RBA.

62. When assessing risk, accountants should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in accounting services/sector, risk reports in other jurisdictions where the accountant based in, and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Accountants may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profile are also important. Competent authorities should consider how they can best alert accountants to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to an accounting practice in the relevant country.

63. Due to the nature of services that an accountant generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most accountants. There may be some scope to use artificial intelligence and analytical tools in an audit context to spot unusual transactions. The accountant's knowledge of the client and its business will develop throughout the duration of a longer term and interactive professional relationship (in some cases, such relationships may exist for short term clients as well, e.g. for property transactions). However, although individual accountants are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationship. Accountants will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily

²⁴ Paragraph 8 of INR.1

²⁵ Including products, transactions or delivery channels.

be low risk (e.g. one-off client relationship). Accountants should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

64. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow accountants to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the accountant's role and involvement. Circumstances may vary considerably between professionals who represent clients on a single transaction and those involved in a long term advisory relationship.

65. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. An accountant may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring accountant).

66. Accountants may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling accountants, where required, to subject each client to reasonable and proportionate risk assessment.

67. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the accountant and/or firm. These criteria, however, should be considered holistically and not in isolation. Accountants, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

68. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. providing company management services may entail greater risk than other services).

69. Criminals use a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. Accountants may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

70. A practical starting point for accounting firms (especially smaller firms) and accountants (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

- a) Client acceptance and know your client policies: identify the client (and its beneficial owners where appropriate) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of

wealth²⁶ of the client, where required, its owners and the purpose of the transaction.

- b) Engagement acceptance policies: Understand the nature of the work. Accountants should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where an accountant does not have the requisite expertise, the accountant should not undertake the work.
- c) Understand the commercial or personal rationale for the work: Accountants need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Accountants however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.
- d) Be attentive to red flag indicators: exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion.
- e) Then consider what action, if any, needs to be taken.
- f) The outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).
- g) Accountants should adequately document and record steps taken under a) to e).

Country/Geographic risk

71. A client may be higher risk when features of their business are connected to a higher risk country as regards:

- a) the origin, or current location of the source of wealth or funds;
- b) where the services are provided;

²⁶ The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

- c) the client's country of incorporation or domicile;
- d) the location of the client's major operations;
- e) the beneficial owner's country of domicile; or
- f) target company's country of incorporation and location of major operations (for potential acquisitions).

72. There is no universally agreed definition of a higher risk country or geographic area but accountants should pay attention to those countries that are:

- a) Countries/areas identified by credible sources²⁷ as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
- b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
- c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.
- d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.
- e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

Client risk

73. The key risk factors that accountants should consider are:

- a) The firm's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
- b) The firm's clients include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients (Please refer to the FATF Guidance (2013) on politically-exposed persons for further guidance on how to identify PEPs).

²⁷ "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

Box 2. Particular considerations for PEPs and source of funds and wealth

If an accountant is advising a PEP client, or where a PEP is the beneficial owner of assets in a transaction, appropriate enhanced CDD is required if a specified activity under R.22 is involved. Such measures include, obtaining senior management (e.g. senior partner, managing partner or CEO) approval before establishing a business relationship, taking reasonable measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs, and conducting enhanced ongoing monitoring on that relationship.

The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust). Source of funds relates directly to the literal origin of funds to be used in a transaction. This is likely to be a bank account. Generally, this would be evidenced by bank statements or similar. Source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). Source of wealth is the origin of the accrued body of wealth of an individual. Understanding source of wealth is about taking reasonable steps to be satisfied that the funds to be used in a transaction are not the proceeds of crime.

While source of funds and wealth may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

Relevant factors that influence the extent and nature of CDD include the particular circumstances of a PEP, PEPs separate business interests and the time those interests prevailed in relation to the public position, whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts, the PEP's home country, the type of activity that the PEP is instructing the accountant to perform, whether the PEP is domestic or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

- c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).
- d) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling

interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

- i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.
 - ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
 - iii. Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the accountants' understanding of the client's business and economic purpose.
- e) Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- f) Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks. These may include, for example:
- i. Money or Value Transfer Services (MVTs) businesses (e.g. remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities);
 - ii. Operators, brokers and others providing services in virtual assets;
 - iii. Casinos, betting houses and other gambling related institutions and activities;
 - iv. Dealers in precious metals and stones
- g) Businesses that while not normally cash intensive appear to have substantial amounts of cash.
- h) Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- i) Clients using financial intermediaries, financial institutions or DNFBPs that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SRBs.
- j) Clients who appear to be acting on somebody else's instructions without disclosure.
- k) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are

otherwise evasive or very difficult to reach, when this would not normally be expected.

- l) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the accountants to perform a proper risk assessment.
- m) Clients with previous convictions for crimes that generated proceeds, who instruct accountants (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.
- n) Clients who have no address, or multiple addresses without legitimate reasons.
- o) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).
- p) Clients who change their settlement or execution instructions without appropriate explanation.
- q) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.
- r) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.
- s) Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where accountants may receive a significant premium for a successful provision of their services, should not be considered a risk factor.
- t) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.
- u) Where there are certain transactions, structures, geographical location, international activities or other factors that are not consistent with the accountants' understanding of the client's business or economic situation.
- v) The accountants' client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
- w) Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.
- x) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

- y) The relationship between employee numbers/structure and nature of the business is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets used compared to similar businesses).
 - z) Sudden activity from a previously dormant client without any clear explanation.
 - aa) Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enters into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.
 - bb) Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
 - cc) Reason for client choosing the accountant is unclear, given the firm's size, location or specialisation.
 - dd) Frequent or unexplained change of client's professional adviser(s) or members of management.
 - ee) Client is reluctant to provide all the relevant information or accountants have reasonable grounds to suspect that the information provided is incorrect or insufficient.
 - ff) Clients seeking to obtain residents rights or citizenship in the country of establishment of the accountants in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.
74. The clients referred to above may be individuals that are, for example, trying to obscure their own business interests and assets or the clients may be representatives of a company's senior management who are, for example, trying to obscure the ownership structure.

Transaction/Service and associated delivery channel risk

75. Services which may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:
- a) Use of pooled client accounts or safe custody of client money or assets without justification.
 - b) Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

- c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting as trustees of such a trust.
- d) Services where accountants may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.
- e) Services that are capable of concealing beneficial ownership from competent authorities.
- f) Services requested by the client for which the accountant does not have expertise except where the accountant is referring the request to an appropriately trained professional for advice.
- g) Non-cash wire transfers through the use of many inter-company transfers within the group to disguise the audit trail.
- h) Services that rely heavily on new technologies (e.g. in relation to initial coin offerings or virtual assets) that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.
- i) Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- j) Transactions where it is readily apparent to the accountant that there is inadequate consideration, where the client does not provide legitimate reasons for the transaction.
- k) Administrative arrangements concerning estates where the deceased was known to the accountant as being a person who had been convicted of proceeds generating crimes.
- l) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the accountant.
- m) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.
- n) Transactions using unusual means of payment (e.g. precious metals or stones).
- o) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.
- p) Unexplained establishment of unusual conditions/clauses in credit arrangements that do not reflect the commercial position between the parties and may require accountants to be aware of risks. Arrangements that may be abused in this way might include unusually short/long amortisation periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.
- q) Transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for

the type of clients, transaction, or with accountant's normal course of business such as a transfer to a corporate entity, or generally without any appropriate explanation.

- r) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.
- s) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.
- t) Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.
- u) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.
- v) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner) with no apparent legal, tax, business, economic or other legitimate reason.
- w) 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.
- x) Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.
- y) Existence of suspicions regarding fraudulent transactions, or transactions that are improperly accounted for. These might include:
 - i. Over or under invoicing of goods/services.
 - ii. Multiple invoicing of the same goods/services.
 - iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).
 - iv. Multiple trading of goods/services.

76. In relation to the areas of risk identified above, accountants may also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240) and the examples of conditions and events that may indicate risks of material misstatement in International Standard of Auditing 315: Identifying and assessing risks of material misstatement through understanding the entity and its environment (ISA315). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.

Variables that may impact on a RBA and on risk

77. While all accountants should follow robust standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst accountants, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating a RBA that complies with the existing obligations of accountants.

78. Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large law firms. Accountants in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

79. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular accountant. This factor must always be considered in the context of the accountant's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice. An accountant's RBA methodology may thus take account of risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause an accountant to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, accountants should always adhere to the minimum requirements as set out in national legislation. These variables may increase or decrease the perceived risk posed by a particular client or type of work. While the presence of the specific factors referred to in paragraphs 71-76 may tend to increase risk, there are more general client/ engagement-related variables that may add to or mitigate that risk.

80. Examples of factors that may increase risk are:

- a) Unexplained urgency of assistance required.
- b) Unusual sophistication of client, including complexity of control environment.
- c) Unusual sophistication of transaction/scheme.
- d) The irregularity or duration of the client relationship. One-off engagements involving limited client contact throughout the relationship may present higher risk.

81. Examples of factors that may decrease risk are:

- a) Involvement of adequately regulated financial institutions or other DNFBP professionals.
- b) Similar country location of accountants and client.
- c) Role or oversight of a regulator or multiple regulators.
- d) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact and easy flow of information throughout the relationship may present less risk.
- e) Private companies that are transparent and well-known in the public domain.
- f) Accountant's familiarity with a particular country, including knowledge of and compliance with local laws and regulations as well as the structure and extent of regulatory oversight.

Documentation of risk assessments

82. Accountants must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement. However, 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.

83. Accountants may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner has become more important.

84. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment, and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

85. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.

Risk mitigation

86. Accountants should have policies, controls and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. 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 supervisors. Measures and controls may include:

- a) General training on ML/TF methods and risks relevant to accountants.
- b) Targeted training for increased awareness by the accountants providing specified activities to higher risk clients or to accountants undertaking higher risk work.
- c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.
- d) Periodic review of the services offered by the accountant, and the periodic evaluation of the AML/CFT framework applicable to the accountant and the accountant's own AML/CFT procedures, to determine whether the ML/TF risk has increased.
- e) Reviewing client relationships from time to time to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

87. Accountants should design CDD procedures to enable them to establish with reasonable certainty the true identity of each client and, with an appropriate degree of confidence, know the types of business and transactions the client is likely to undertake. Accountants should have procedures to:

- a) Identify the client and verify that client's identity using reliable, independent source documents, data or information.
- b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that accountants are satisfied that they knows who the beneficial owner is. This should include accountants' understanding of the ownership and control structure of the client. This is articulated in the following box

**Box 3. Beneficial ownership information obligations
(see R.10, R.22 and INR.10)**

R.10 sets out the instances where accountants will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the

risks. Accountants should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. Accountants should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. Accountants can verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. Accountants can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the accountant is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client, and may include conducting public searches as well as by seeking information directly from the client.

Accountants will likely need to obtain the following information for a client that is a legal entity:

- a) the name of the company;
- b) the company registration number;
- c) the registered address and/ or principal place of business (if different);
- d) the identity of shareholders and their percentage ownership;
- e) names of the board of directors or senior individuals responsible for the company's operations;
- f) the law to which the company is subject and its constitution; and
- g) the types of activities and transactions in which the company engages.

To verify the information listed above, accountants may use sources such as the following:

- a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
- b) details from company registers;
- c) shareholder agreements or other agreements between shareholders concerning control of the legal person; and
- d) filed audited accounts.

Accountants should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

- c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
- d) Conduct ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to respond to requests for information from an FIU and the law enforcement agencies.

88. Accountants should design their policies and procedures so that the level of client due diligence addresses the risk of being used for ML/TF by the client. In accordance with the national AML/CFT framework, accountants should design a 'standard' level of CDD for normal risk clients and a reduced or simplified CDD process for low risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that are assessed as high risk. These activities may be carried out in conjunction with firms' normal client acceptance procedures and should take account of any specific jurisdictional requirements for CDD.

89. In the normal course of their work, accountants are likely to learn more about some aspects of their client, such as their client's business or occupation and/or their level and source of income, than other advisors. This information is likely to help them reassess the ML/TF risk.

90. A RBA means that accountants should perform varying levels of work according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or natural persons exercising effective control; and an indication of the purpose of the trust. Accountants will need to obtain a reasonable level of comfort that the declared purpose of the trust is in fact its true purpose.

91. Changes in ownership or control of clients should lead to review or repeat of client identification and verification procedures. This may be carried out in conjunction with any professional requirements for client continuation processes.

92. Public information sources may assist with this ongoing review (scrutinising transactions undertaken throughout the course of that relationship). The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominees and complex structures.

93. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

**Box 4. Examples of Standard/Simplified/Enhanced CDD measures
(see also INR.10)**

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the accountant is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- 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 business and risk profile the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of client and beneficial owner
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data or information, which is perceived to be unreliable)
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained
- 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 client's name with a bank subject to similar CDD standards
- Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of engagement teams responsible for the client.
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Politically exposed persons (PEP) (R.12 and R.22)

94. Accountants should take reasonable measures to identify whether a client is a PEP or a family member or close associate of a PEP. Accountants should also refer to the 2013 FATF Guidance on politically-exposed persons for further guidance on how to identify PEPs.

95. If the client or the beneficial owner is a PEP or a family member or close associate of a PEP, accountants should perform the following additional procedures:

- a) obtain senior management approval for establishing (or continuing, for existing clients) such business relationships;
- b) take reasonable measures to establish the source of wealth and source of funds²⁸; and
- c) conduct enhanced ongoing monitoring of the business relationship.

96. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's role in a particular government/government agency, whether the PEP has access to official funds, the PEP's home country, the type of work the PEP is instructing the accountant to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

97. The nature of the risk should be considered in light of all relevant circumstances, such as:

- a) The nature of the relationship between the client and the PEP. If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.
- b) The nature of the client (e.g. where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is

²⁸ See INR 28.1.

subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

- c) The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration.

Ongoing monitoring of clients and specified activities (R.10 and 22)

98. Accountants are not expected to scrutinise every transaction that goes through their clients' books and some accounting services are provided only on a one-off basis, without a continuing relationship with the client and without the accountant having access to client's books and/or bank records. However, many of the professional services provided by accountants put them in a relatively good position to encounter and recognise suspicious activities (or transactions) carried out by their clients through their inside knowledge of, and access, to the client's records and management processes and operations, as well as through close working relationships with senior managers and owners. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements and corporate filings) would also enable the relevant accountants to develop a better understanding of the activities of their clients.

99. Accountants need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgement in the forming of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional accountancy functions and relationships.

100. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that accountants are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information. As discussed below, ongoing monitoring may also give rise to filing a STR.

101. Accountants should also consider reassessing CDD on an engagement/assignment basis for each client. Well-known, reputable, long-standing clients may suddenly request a new type of service that is not in line with the previous relationship between the client and accountant. Such an assignment may suggest a greater level of risk.

102. Accountants should not conduct investigations into suspected ML/TF on their own but instead file a STR or if the behaviour is egregious they should contact the FIU or law enforcement or supervisors, as appropriate, for guidance. Within the scope of engagement, an accountant should be mindful of the prohibition on "tipping off" the client where a suspicion has been formed. Carrying out additional investigations, which are not within the scope of the engagement should also be considered against the risk alerting a money launderer.

103. When deciding whether or not an activity or transaction is suspicious, accountants may need to make additional enquiries (within the normal scope of the assignment or business relationship) of the client or their records this could typically be done as part of the accountant's CDD process. Normal commercial enquiries, being

made to fulfil duties to clients, may assist in understanding an activity or transaction to determine whether or not it is suspicious.

Suspicious activity/transaction reporting, tipping-off, internal controls and higher-risk countries (R.23)

104. R.23 sets out obligations for accountants on reporting and tipping-off, internal controls and higher-risk countries as set out in R.20, R.21, R.18 and R.19.

Suspicious transaction reporting and tipping-off (R.20, 21 and 23)

105. R.23 requires accountants to report suspicious transactions set out in R.20. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly. The requirement to file a STR is not subject to a RBA, but must be made whenever required in the country concerned.

106. Accountants may be required to report suspicious activities, as well as specific suspicious transaction, and so may make reports on a number of scenarios including suspicious business structures or management profiles which have no legitimate economic rationale and suspicious transactions, such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business. As specified under INR.23, where accountants seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

107. However, it should be noted that a RBA is appropriate for the purpose of identifying a suspicious activity or transaction, by directing additional resources at those areas that have been identified as higher risk. The designated competent authorities or SRBs may provide information to accountants, which can inform their approach for identifying suspicious activity or transactions, as part of a RBA. Accountant should also periodically assess the adequacy of their system for identifying and reporting suspicious activity or transactions.

108. Accountants should review CDD if they have a suspicion of ML/TF.

Internal controls and compliance (R.18 and 23)

109. In order for accountants to have effective RBA, the risk-based process must be imbedded within the internal controls of the firm and they must be appropriate for the size and complexity of the firm.

Internal controls and governance

110. Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the RBA. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

111. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

- a) designating an individual or individuals, at management level responsible for managing AML/CFT compliance;
- b) designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate, and include risk-based CDD policies, procedures and processes;
- c) ensuring that adequate controls are in place before new services are offered; and
- d) ensuring adequate controls for accepting higher risk clients or providing higher risk services, such as management approval.

112. These policies and procedures should be implemented across the firm and include:

- a) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;
- b) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;
- c) providing senior management with a regular report of compliance initiatives, identifying compliance deficiencies, corrective action taken, and STRs filed;
- d) planning for changes in management, staff or firm structure so that there is compliance continuity;
- e) focusing on meeting all regulatory record-keeping and reporting requirements, recommendations for AML/CFT compliance and providing for timely updates in response to changes in regulations;
- f) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;
- g) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;
- h) providing for appropriate training to be given to all relevant staff;
- i) having appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP or a person subject to applicable financial sanctions;
- j) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, evidencing the source of wealth and funds of a client and escalation to senior management, or additional review and/or consultation);
- k) providing increased focus on the accountant/accounting firm's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;
- l) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the accountant/accounting firm operates and the services it provides; and

- m) providing for an AML/CFT compliance function and review programme, as appropriate, given the scale of the organisation and the nature of the accountant's practice.

113. The firm should perform a firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures.

114. Accountants should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of accountants as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.

115. Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole practitioners, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

Internal mechanisms to ensure compliance

116. Accountants (at the senior management level) should monitor the effectiveness of internal controls. If accountants identify any weaknesses in those internal controls, improved procedures should be designed.

117. The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member that has a good working knowledge of the firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.

118. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the firm is acting on those recommendations.

119. Accountants should review/update firm-wide risk assessments regularly and ensure that policies and procedures continue to target those areas where the ML/TF risks are highest.

Vetting and recruitment

120. Accountants should consider the skills, knowledge and experience of staff both before they are appointed to their role and on an ongoing basis. The level of

assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

121. R.18 requires that accounting firms/ accountants provide their staff with AML/CFT training. For accountants, and those in smaller firms in particular, such training may also assist with raising awareness of monitoring obligations. The accounting firm's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant staff with at least general information on AML/CFT laws, regulations and internal policies.

122. Firms should provide targeted training for increased awareness by the accountant providing specified activities to higher-risk clients and to accountants undertaking higher- risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted towards the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

123. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in accountant's own practice. In addition, competent authorities, SRBs and representative bodies should work with educational institutions to ensure that the relevant curricula address ML/TF risks. The same training should also be made available for students taking courses to train to become accountants.

124. Firms must provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, accountants may take account of any AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without a professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

125. The overall risk-based approach and the various methods available for training and education gives accountants flexibility regarding the frequency, delivery mechanisms and focus of such training. Accountants should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

- a) tailored to the relevant staff responsibility (e.g. client contact or administration);
- b) at the appropriate level of detail (e.g. considering the nature of services provided by the accountants);
- c) at a frequency suitable to the risk level of the type of work undertaken by the accountants; and

- d) used to test to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

126. Consistent with R.19, accountants should apply enhanced due diligence measures (also see paragraph 72 above), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV – Guidance for supervisors

127. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs must ensure that accountants are implementing their obligations under R.1.

Risk-based approach to supervision

128. A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resource to areas of higher ML/TF risk. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of accountants, any relevant supervisors and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.

Supervisors and SRBs' role in supervision and monitoring

129. According to R.28, countries can designate a competent authority or SRB to ensure that accountants are subject to effective oversight, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

130. A SRB is body representing a profession (e.g. accountants, legal professionals, notaries, other independent legal professionals or TCSPs) made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practise in the profession. A SRB also performs supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

131. Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanctions), and adequate financial, human and technical resources. Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on accountants on the basis of their understanding of the ML/TF risks, and taking into consideration the characteristics of the accountants, in particular their diversity and number.

132. Countries should ensure that supervisors and SRBs are as equipped as a competent authorities in identifying and sanctioning non-compliance by its members.

Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

133. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant persons should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

134. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas

Understanding ML/TF risk

135. The extent to which a national framework allows accountants to apply a RBA should also reflect the nature, diversity and maturity of the sector and its risk profile as well the ML/TF risks associated with individual accountants.

136. Access to information about ML/TF risks is essential for an effective risk-based approach. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information available for AML/CFT risk assessments conducted by accountants and the jurisdictions' national risk assessment. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and accountants. In situations where some accountants have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

137. Supervisors and SRBs should, as applicable, draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supranational risk assessments, domestic or international typologies, supervisory expertise and FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

138. These sources can also be helpful in determining the extent to which an accountant is able to effectively manage ML/TF risk. Information-sharing and collaboration should take place among AML/CFT supervisors across all sectors (legal professionals, accountants and TCSPs).

139. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which accountants operate in the country and the nature of services provided by them.

140. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the accountant. Supervisors and SRBs should also consider the type of services the accountant is providing as well as its size and business model (e.g. whether it is a sole practitioner), corporate

governance arrangements, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation. Supervisors and SRBs should also consider the controls accountants have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements).

141. Supervisors and SRBs should seek to ensure their supervised populations are fully aware of, and compliant with, measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues that affect several aspects of AML/CFT.

142. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers and typologies published by international bodies.²⁹ Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

143. Supervisors and SRBs should review their assessment of accountants' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the profession.

Mitigating and managing ML/TF risk

144. Supervisors and SRBs should take proportionate measures to mitigate and manage ML/TF risk. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the inherent ML/TF risks. Supervisors and SRBs should consider the characteristics of accountants, particularly where they act as professional intermediaries, in particular their diversity and number. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of accountant and their clients, products and services.

145. Supervisors and SRBs should take account of the risk profile of accountants when assessing the adequacy of internal controls, policies and procedures.

146. Supervisors and SRBs should develop a means of identifying which accountants are at the greatest risk of being used by criminals. This involves considering the probability and impact of ML/TF risk.

147. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by accountants and the environment in which they operate. The risk can also increase or decrease depending on other factors:

- a) service and product risk (the likelihood that services or products can be used for ML/TF);
- b) client risk (the likelihood that clients' funds may have criminal origins);
- c) the nature of transactions (e.g. frequency, volume, counterparties);

²⁹ Such as the FATF, the OECD, the WB, the IMF and the UNODC

- d) geographical risk (whether the accountant, its clients or other offices trade in riskier locations); and
- e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the accountant as well as information on its compliance history, complaints about the accountant or about the quality of its internal controls, and intelligence from law enforcement agencies on suspected involvement in financial crimes (including unwitting facilitation). Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports from credible media particularly those related to predicate offences for ML/TF or to financial crimes.

148. In adopting a RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of an accountant within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the accountant from the grouping.

149. Supervisors and SRBs should also consider the impact, i.e. the potential harm caused if ML/TF is facilitated by the accountant or group of accountants. A small number of accountants may cause a high level of harm. This can depend on:

- a) size (i.e. turnover), number and type of clients, number of premises, value of transactions etc.); and
- b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

150. The risk assessment should be updated by supervisors and SRBs on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of accountants.

151. Supervisors or SRBs should consider whether accountants meet the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and propriety. This will include whether the accountant meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

152. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate between categories of accountants based on factors such as their client base, countries they deal with and applicable AML/CFT controls etc.

153. Supervisors and SRBs should acknowledge that in a risk-based regime, not all accountants will adopt identical AML/CFT controls and that an isolated incident where the accountant is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of the accountant's AML/CFT controls. At the same time, accountants should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

154. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

Supervision of the RBA

Licensing or registration

155. R.28 requires a country to ensure that accountants are subject to regulatory and supervisory measures to ensure compliance by the profession with AML/CFT requirements.

156. R.28 requires the supervisor or SRB to 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 in an accountancy practice. This can be achieved through the evaluation of these persons through a “fit and proper” test.

157. A licensing or registration mechanism is one of the means to identify accountants to whom the regulatory and supervisory measures, including the “fit and proper” test should be applied. It also enables the identification of the number of accountants for the purposes of assessing and understanding the ML/TF risks for the country, and the action that should be taken to mitigate them in accordance with R.1.

158. Licensing or registration provides a supervisor or SRB with the means to fulfil a “gatekeeper” role over who can undertake the activities specified in R.22. Licensing or registration should ensure that upon qualification, accountants are subject to AML/CFT compliance monitoring.

159. The supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry or tax authority), information from financial institutions and DNFBPs, complaints by the public, open source information from advertisements and business and commercial registries, or any other sources which indicate that there are unsupervised individuals or businesses providing the activities specified in R.22.

160. Licensing or registration frameworks should define the activities that are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing “bad actors”.

161. The terms “licensing” or “registration” are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential, conduct as well as ML/TF risks on an on-going basis. Some jurisdictions have adopted similar licensing regimes for accountants, generally where accountants carry out trust and corporate services, to encompass aspects of prudential and conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

162. A jurisdiction may have a registration framework over the entire DNFBP sector, including accountants or have a specific registration framework for each constituent of a DNFBP. Generally, a supervisor or SRB carries out the registration function.

163. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interests of its members. If so, the SRB should ensure that registration decisions are taken separately and independently from its activities regarding member representation.

Fit and proper tests

164. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a management function in an accountancy practice.

165. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in an accountancy practice. However, the decisions on an individual's fitness and propriety may also be based upon a range of factors concerning the individual's competency, probity and judgement as well as integrity.

166. In some jurisdictions, a "fit and proper test" forms a fundamental part of determining whether to license or register the applicant and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that position.

167. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. The questionnaire could gather personal identification information, residential and employment history, and require disclosure by the applicant of any convictions or adverse judgements, including pending prosecutions and convictions relating to the applicant. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors, or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

168. The supervisor or SRB should also ensure on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function. The supervisor or SRB should consider re-assessing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against “brass-plate” operations

169. The supervisor or SRB should ensure that its licensing or registration requirements require the applicant to have a meaningful physical presence in the jurisdiction. This usually means that the applicant should have its place of business in the jurisdiction. Where the applicant is a legal person, those individuals who form its mind and management, should also be resident in the jurisdiction and be actively involved in the business. A business with only staff who do not possess the professional requirements of an accountant should not be licensed or registered.

170. A supervisor or SRB should consider the ownership and control structure of the applicant to determine that sufficient control over its operation will reside within the business, which it is considering licensing or registering. Factors to take account of could include consideration of where the beneficial owners and controllers reside, the number and type of management functions the applicant is proposing to have in the country, such as directors and managers, including compliance managers, and the calibre of the individuals who will be occupying those roles.

171. The supervisor or SRB should also consider whether the ownership and control structure of accountants unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

172. Supervisors and SRBs should take measures to effectively monitor accountants through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected risk-based approach. Supervisors and SRBs may choose to adjust:

- a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.
- b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of accountants. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer other relevant and staff, considering gatekeeper’s own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients and other matters, which may be

observed in the course of an onsite visit and, where appropriate, sample testing of reporting obligations.

- c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from accountants' inclusion in thematic review samples).
- d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of accountants' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include; detailed testing of systems and files to verify the implementation and adequacy of the accountant's risk assessment, CDD, reporting and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

173. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

174. Record keeping and quality assurance are important, so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

175. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by accountants. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFPBs, to include accountants when providing the services outlined in R.22(d). Sanctions should be available for the directors and senior management of the firm when an accountant fails to comply with requirements.

176. Supervisors and SRBs should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, reprimand and censure to punitive measures (including disbarment and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic

breakdowns or significantly inadequate controls will result in more severe supervisory response.

177. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

178. Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement with relevant stakeholders, including accountants. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to accountants should also discuss ML/TF risk within their sector and outline ML/TF indicators to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

179. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the accountancy profession, which may cover operational and practical issues, and be more detailed and explanatory in nature. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to the accountancy profession and be consistent with all other legal requirements and obligations.

180. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions accountants will consider that separate guidance targeted at their profession will be the most appropriate and effective form.

181. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

Training

182. Training is important for supervisory staff, and other relevant employees, to understand the accountancy profession and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness

and efficiency of AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension.

183. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by accountants and the adequacy and proportionality of AML/CFT controls of accountants. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

184. Supervisors should avoid mandating the use of AML systems, tools or software of any third party commercial providers to avoid conflicts of interest in the effective supervision of firms.

Information exchange

185. Information exchange between the public and private sector and within private sector (e.g. between financial institutions and accountants) is important to combat ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial Intelligence Units and law enforcement) should be robust, secure and subject to compliance with national legal requirements.

186. The type of information that could be shared between the public and private sectors include:

- a) ML/TF risk assessments;
- b) Typologies (i.e. case studies) of how money launderers or terrorist financiers have misused accountants;
- c) feedback on STRs and other relevant reports;
- d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with accountants as a class or individually; and
- e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

187. Domestic co-operation and information exchange between FIU and supervisors of the accountancy profession and among competent authorities including law enforcement, intelligence, FIU, tax authorities, supervisors and SRBs is also vital for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged. When sharing information, protocols and safeguards should be implemented in order to protect personal data.

188. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the accountancy profession, taking account of the multi-jurisdictional reach of many accounting firms.

Supervision of Beneficial Ownership requirements and source of funds/wealth requirements

189. The FATF Recommendations require competent authorities to have access to adequate, accurate and timely information on the beneficial ownership and control of legal persons (R.24). In addition, countries must take measures to prevent the misuse of legal arrangements for ML/TF, in particular ensuring that there is adequate, accurate and timely information on express trusts (R.25). Implementation of the FATF Recommendations on beneficial ownership has proven challenging. As a result, the FATF developed a Guidance on Transparency and Beneficial Ownership (2014) to assist countries in their implementation of R.24 and R.25, as well as R.1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

190. R.24 and R.25 require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). Accountants must, however, be cautious in blindly relying on the information contained in registries. It is important for there to be some form of ongoing monitoring during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership as registries are unlikely to provide such information on a dynamic basis.

191. Those responsible for company formation and the creation of legal arrangements fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements or in their management and administration.

192. As DNFBPs, accountants are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In a number of countries an accountant may be required as part of the process of registering the legal person and will be responsible for providing basic and/or beneficial ownership information to the registry.

193. In their capacity as company directors, trustees or foundation officials etc. of these legal persons and legal arrangement, accountants often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing banking or audit services to these types of client.

194. These financial institutions and other DNFBPs may request the CDD information collected and maintained by accountants, who because of their role as director or trustee, will be their principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owners of the legal person or legal arrangement.

195. Under R.28, countries are to ensure that accountants are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify

them. R.24 and R.25, which deal with transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up-to-date information on these legal entities is available on a timely basis.

196. In accordance with R.28, accountants should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The supervisor or SRB should have a supervisory framework, which can help in ascertaining that accurate and current basic and beneficial ownership information on legal person and legal arrangements is maintained and will be available on a timely basis to competent authorities.

197. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which accountants have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client records on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

198. During onsite and offsite inspections, the supervisor or SRB should examine the policies, procedures and controls that are in place for taking on new clients to establish what information and documentation is required where the client is a natural person or legal person or arrangement. The supervisor or SRB should verify the adequacy of these procedures and controls to identify beneficial owners to understand the ownership and control structure of these legal persons and arrangements and to ascertain the business activity. For example, self-declaration on beneficial ownership provided by the client without any other mechanism to verify the information will not be adequate in all cases.

199. Sample testing of records will assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the records selected should reflect the profile of the client base and include both new and existing clients.

200. The supervisor or SRB should consider the measures the accountants have put in place for monitoring changes in the beneficial ownership of legal person and legal arrangements to whom they provide services to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

201. During examinations, the supervisor or SRB should consider whether to verify the beneficial ownership information available on the records of accountants with that held by the relevant registry, if any. The supervisor or SRB may also consider information from other competent authorities such as FIUs, public reports and information from other financial institutions or DNFBNs, to verify the efficacy of accountants' controls.

202. Accountants should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly

evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and controls that accountants have established to identify and record sources of wealth in arrangements.

Nominee arrangements

203. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner.

204. A nominee shareholder is a natural or legal person who is officially recorded in the register of members and shareholders of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement.

205. In a number of countries, accountants act or arrange for other persons (either individuals or corporate) to act as directors. Accountants also act or arrange for other persons (either individuals or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, one of the mechanisms to ensure that nominee shareholders and directors are not misused, is by subjecting these accountants to licensing and recording their status in company registries. Countries may rely on a combination of measures in this respect.

206. There are legitimate reasons for accountants to act as or provide directors to a legal person or act or provide nominee shareholders. These may include the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. However, nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of the person from whom they will take instructions or whom they represent. They are sometimes referred to as “strawmen”.

207. Nominee directors and nominee shareholders can create obstacles to identifying the true beneficial owner of a legal person, particularly where the status is not disclosed. This is because it will be the identity of the nominee that is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in various countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

208. The supervisor or SRB should be aware that undisclosed nominee arrangements may exist. They should consider whether undisclosed nominee arrangements would be identified and addressed during their onsite and offsite inspections and examination of the policies, procedures, controls and client records of the accountant, including the CDD process and ongoing monitoring by the accountant.

209. An undisclosed nominee arrangement may exist where there are the following (non-exhaustive) indicators:

- a) the profile of a director or shareholder is inconsistent with the activities of the company;
- b) the individual holds numerous appointments to unconnected companies;
- c) a director's or shareholder's source of wealth is inconsistent with the value and nature of the assets within the company;
- d) funds into and out of the company are sent to, or received from unidentified third party/ies;
- e) the directors or shareholders are accustomed to acting on instruction of another person; and
- f) requests or instructions are subject to minimal or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the director/s.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom an accountant provides services

1. Taking a RBA, the amount of information that should be obtained by an accountant will depend on whether an accountant is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, an accountant will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. An accountant who is providing other services (e.g. acting as registered office) to a trust, company or other legal entity will be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. An accountant that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by other accountants, legal professionals or TCSPs providing services to the trust or relevant extracts from the trust deed itself to enable the accountant to identify the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. An accountant should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that an accountant's policies should enable it to disregard source documents, data or information which are perceived to be unreliable):

- i. the settlor;
- ii. the protector;
- iii. the trustee(s), where the accountant is not acting as trustee;
- iv. the beneficiaries or class of beneficiaries; and
- v. any other natural person actually exercising effective control over the trust.

Settlor

- a) A settlor is generally any person (or persons) by whom the trust is made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).
- b) A settlor may or may not be named in the trust deed. Accountants should have policies and procedures in place to identify and verify the identity of the real economic settlor.
- c) An accountant establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or

director of a trust, company or other legal entity should have policies and procedures in place (using a RBA) to identify the source of funds in the trust, company or other legal entity.

- d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift or letter of wishes.
- e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

- a) An accountant should have policies and procedures in place, adopting a RBA to enable it to form a reasonable belief that it knows the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that an accountant is satisfied that it knows who the beneficiaries are. This does not require an accountant to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the accountant should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).
- b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), an accountant should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).
- c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although an accountant should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed) the accountant is not obliged to obtain additional information to identify the individual beneficiaries referred to in the class unless or until the trustees make a distribution to such beneficiary.
- d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, an accountant is not required to obtain additional information to identify such contingent beneficiaries unless or until the contingency is satisfied or until the trustees make a distribution to such beneficiary.
- e) An accountant who administers the trust or company or other legal entity owned by a trust or otherwise provides or acts as trustee or director to the trust, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the information has been provided, or there are other changes to the class of beneficiaries.

- f) An accountant is not obliged to obtain other information about beneficiaries other than to enable an accountant to satisfy itself that it knows who the beneficiaries are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

- a) An accountant providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.
- b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:
 - i. dispose of or invest (other than as an investment manager or adviser) trust property;
 - ii. make or approve trust distributions;
 - iii. vary or terminate the trust;
 - iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and or;
 - v. appoint or remove trustees.
- c) An accountant who administers the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

4. These examples are subject to the more general guidance on what information should be obtained by an accountant to enable it to identify settlors and beneficiaries. It is not intended to suggest that an accountant must obtain more information about a beneficiary that is an entity where it would not need to obtain such information if the beneficiary is an individual.
- a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, an accountant should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.
 - b) In the case of a settlor that is a legal entity, an accountant should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, an accountant should take steps to satisfy itself as to the economic settlor of the trust (i.e. the person who has provided funds to the legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor

retains powers over the trust (e.g. a power of revocation), an accountant should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

- c) In the case of a beneficiary that is an entity (e.g. a charitable trust or company), an accountant should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, an accountant should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

- a) Where an accountant is not itself acting as trustee, it is necessary for an accountant to obtain information to enable it to identify and verify the identity of the trustee (s) and, where the trustee is a corporate trustee, identify the corporate entity, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.
- b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, an accountant should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. An accountant can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body that regulates the trustee and of the regulated trustee itself).
- c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence that enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, an accountant should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, an accountant does not need to obtain detailed information to identify the directors or controlling persons of that entity that acts as shareholder of the private trust company.

Individual and Corporate protector

- a) Where an accountant is not itself acting as a protector and a protector has been appointed, the accountant should obtain information to identify and verify the identity of the protector.
- b) Where the protector is a legal entity, an accountant should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

- c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, an accountant should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. An accountant can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the web-site of the body that regulates the protector and of the regulated protector itself).

Annex 2: Glossary of terminology

Beneficial Owner

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.

Competent Authorities

Competent authorities refers to all public authorities 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 and bearer negotiable instruments (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.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

- a) Casinos (which also includes internet and ship based casinos).
- 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, 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 the 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.

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 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).'

FATF Recommendations

Refers to the FATF Forty Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with an accountant or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term "*Legal professional*" refers to legal professionals, civil law notaries, common law notaries, and other independent legal professionals.

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.

Red Flags

Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A "*red flag*" may be used as a short hand for any indicator of risk which puts an investigating accountant on notice that further checks or other appropriate safeguarding actions will be required.

Self-regulatory bodies (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, 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.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions (“financial supervisors”) 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.

Annex 3: Supervisory practices for implementation of the RBA

China

People's Bank of China ("PBC") Conducts Risk Assessment on Accounting Firms in Jiangsu Province. In November 2017, the PBC Suzhou Branch conducted Money Laundering Risk Assessment on nine accounting firms. The assessments revealed that, for the inherent risk of the accounting firms, there are risks of the Certified Public Accountants utilizing the professional nature of their occupation and confidentiality privilege to assist customers in money laundering; failing to identify illicit funds being injected into the corporate's normal business activities when providing services, and providing services to customers on the monitoring lists or from sensitive jurisdiction. In respect of risk control areas, deficiencies were noted among the accounting firms including the unsound internal control system, weak AML awareness of practitioners, lack of capability, unsatisfactory mechanisms for sanction screening and lack of practical cases of suspicious transaction reports. However, as substantial business practitioners and the target clients of the auditing services are mainly corporates (and mostly being the listed companies and foreign enterprises), the overall money laundering risk of accounting firms was not considered high.

Malaysia

AML/CFT Supervisory Practices of Accountants in Malaysia

A. Fit and Proper Requirements – Self-Regulatory Body (SRB)

The accounting profession in Malaysia is regulated by the Malaysian Institute of Accountants (MIA), as the self-regulated body (SRB) under the Accountants Act (AA) 1967. Prior to their admission as MIA members and issuance of Practising Certificates, they are subject to appropriate market entry controls in which they are required to fulfil the "fit and proper" requirements under the legislation.

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated competent authority for the AML/CFT supervision of the Designated Non-Financial Businesses and Professions (DNFBPs) & Other Financial Institutions in Malaysia, including accountants.

BNM adopts a risk-based approach supervision on accountants, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia's third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness had stipulated the accountants' net ML and TF risks as "**MEDIUM HIGH**" and "**MEDIUM**" level, respectively, as exacerbated by the sector's marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

ii. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on accountants are guided accordingly to include a range of supervisory tools, as follows:

- **On-site Examination**

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management. In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions.

- **Off-site Monitoring and Supervisory Outreach Activities**

Apart from on-site examinations, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by the accountants. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for accountants is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of Data and Compliance Reports and internal audit reports. In addition, BNM and the relevant SRBs conduct periodic nationwide AML/CFT outreach and awareness programmes.

Monaco

Monaco completed its first NRA (National Risk Assessment) in 2017 and the accountants were included in the scope (see public NRA report in www.siccfm.mc/en/The-National-Risk-Assessment-NRA). The assessed risk

regarding accountants was rated ML (moderate low) so the accountants were not included in the priority professionals to be inspected on-site. However, since 2016, they are being inspected and about two third of the number of accountants has already been assessed. They are planned to have all been assessed by the end of 2021, the most prominent professional having already been inspected (including the Big four companies).

Considering the small number of accountants in Monaco, no real RBA was used for their supervision and these inspections are aimed to be comprehensive.

Annex 4: Members of the RBA Drafting Group

FATF members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors(GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD
Member	Accountants Office	Institution
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants
Member	Legal professionals and Notaries Office	Institution
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón Alexander Winkler	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

Member	TCSPs Office	Institution
John Riches (Co-chair) Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland



GUIDANCE FOR A RISK-BASED APPROACH ACCOUNTING PROFESSION

The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012.

This guidance highlights the need for a sound assessment of the money laundering and terrorist financing risks that accountants face so that the policies, procedures and ongoing customer due diligence measures mitigate these risks.

The FATF developed this guidance with significant input from the profession itself, to ensure that it reflects the experience gained by public authorities and the private sector over the years.

www.fatf-gafi.org | June 2019





CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

Guide to Comply with Canada's Anti-Money Laundering (AML) Legislation





CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

Guide to Comply with Canada's Anti-Money Laundering (AML) Legislation

Prepared by MNP LLP

DISCLAIMER

This publication was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Library and Archives Canada Cataloguing in Publication

McGuire, Matthew, author

Guide to comply with Canada's anti-money laundering (AML) legislation / Matthew McGuire, MAcc, CPA, CA, DIFA, CAMS, AMLP.

Also available in French.

ISBN 978-1-55385-877-5 (pbk.)

1. Money laundering--Canada--Prevention. 2. Money--Law and legislation--Canada--Criminal provisions. 3. Accounting--Law and legislation--Canada. I. Chartered Professional Accountants of Canada II. Title.

KE1024.R42M34 2014

345.71'0268

C2014-905959-0

KF1030.R3 M34 2014

© 2014 Chartered Professional Accountants of Canada

All rights reserved. This publication is protected by copyright and written permission is required to reproduce, store in a retrieval system or transmit in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise).

For information regarding permission, please contact permissions@cpacanada.ca

Preface

The Anti-Money Laundering Committee (AML Committee) of the Chartered Professional Accountants of Canada (CPA Canada) has commissioned this publication *Guide to Comply with Canada's Anti-Money Laundering (AML) Legislation* to help CPA Canada members and Accounting Firms deal with recent changes in AML regulatory requirements. Accountants and Accounting Firms are reporting entities under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* with specific regulatory requirements when they engage in certain activities.

This *Guide* sets out recent changes to Canada's AML Legislation and provides practical guidance for AML compliance that is relevant to Accountants and Accounting Firms.

Accountants and Accounting Firms are at risk of penalties (both monetary and criminal) for non-compliance with the AML Legislation in the event of, for example, failure to report suspicious transactions. An effective AML compliance program is key to mitigating this risk.

This publication aids Accountants and Accounting Firms by addressing comprehensive topics including:

- AML standards and regime
- who and what activities fall within the AML obligations
- money laundering risk assessment
- development of a compliance regime
- AML and privacy obligations
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) examinations
- ongoing monitoring of business relationships

Throughout the *Guide* there are questionnaires and checklists to help Accountants and Accounting Firms ask the right questions, FINTRAC forms, and practical guidance on how to complete the forms.

CPA Canada thanks the author, Matthew McGuire of MNP LLP, and acknowledges the contribution of the CPA Canada AML Committee. Particular gratitude is extended to Mr. McGuire's colleague at MNP LLP, Iain Kenny, who provided valuable input and assistance throughout the project.



Gordon Beal, CPA, CA, M.Ed.
Vice-President
Research, Guidance & Support
CPA Canada

Anti-Money Laundering Committee

Matthew McGuire, MAcc, CPA, CA, DIFA, CAMS, AMLP, *Chair*
Michael Ecclestone, LL.B., CAMS
Monica Stark, CA, CAMS

Author

Matthew McGuire, MAcc, CPA, CA, DIFA, CAMS, AMLP

Project Direction, CPA Canada

Gigi Dawe, LL.M.
Principal, Research, Guidance & Support
Leader, Corporate Oversight & Governance

Rayna Shienfield, J.D.
Principal, Research, Guidance & Support
Corporate Oversight & Governance

Marial Stirling, CPA, CA, LL.B.
Principal, Research, Guidance & Support
Corporate Oversight & Governance

Gordon Beal, CPA, CA, M.Ed.
Vice-President, Research, Guidance & Support

Table of Contents

Preface	iii
CHAPTER 1	
Motivation for the Guide	1
CHAPTER 2	
Determining if the Obligations Are Applicable	3
2.1 Definition of Accountant and Accounting Firm	3
2.2 Definition of Triggering Activities	4
2.2.1 Giving Instructions Versus Giving Advice	5
2.2.2 Specified Exemptions and Considerations	6
2.2.2.1 Employment Relationship	6
2.2.2.2 Assurance Related Activities	6
2.2.2.3 Trustee in Bankruptcy Services	7
2.2.2.4 Implications of Organizational Structure	7
2.2.2.5 A Note on Client Fees	8
2.3 Questionnaires to Assist in Determining Applicability	8
2.3.1 Do I Have Obligations as an Accountant?	8
2.3.2 Do We Have Obligations as an Accounting Firm?	10
2.4 Determination of Triggering Activities in Larger Firms	11
CHAPTER 3	
What to Do if the Obligations Are Applicable	13
3.1 Required Tasks When Engaged in Triggering Activities	13
3.1.1 Receiving Funds of \$3,000 or More	14
3.1.1.1 Exemptions	14
3.1.1.2 Receipt of Funds Record	15
3.1.1.3 Client Identification	15

3.1.2	Receiving Funds of \$10,000 or More in Cash	17
3.1.2.1	Exemptions	17
3.1.2.2	Client Identification	17
3.1.2.3	Third Party Determination	19
3.1.2.4	Large Cash Transaction Record and Report	19
3.1.3	Suspicious Transaction or Activity	20
3.1.3.1	Establishing Reasonable Grounds for Suspicion	20
3.1.3.2	How Money is Laundered	21
3.1.3.2.1	Concealment within Business Structures	22
3.1.3.2.2	Misuse of Legitimate Businesses	23
3.1.3.2.3	Use of False Identities, Documents, or Straw Men	23
3.1.3.2.4	Exploiting International Jurisdictional Issues	23
3.1.3.2.5	Use of Anonymous Asset Types	23
3.1.3.3	Indicators of Money Laundering and Terrorist Financing	23
3.1.3.4	Tipping Off	24
3.1.3.5	Client Identification	25
3.1.3.6	Completing the Suspicious Transaction Record and Report	26
3.1.4	Knowledge of Terrorist Property	27
3.1.4.1	Terrorists, Terrorist Groups, and Designated Persons	27
3.1.4.2	Definition of Property	27
3.1.4.3	Filing a Terrorist Property Report	28
3.1.4.4	Advising the RCMP and CSIS	28
3.2	Ongoing Monitoring of Triggering Activity Business Relationships	28
3.2.1	Defining the Purpose and Intended Nature of a Business Relationship	29
3.2.2	Ongoing Monitoring: Detecting Suspicious Transactions and Assessing Consistency of Transactions with Client Knowledge and Risk	29
3.2.3	Ongoing Monitoring: Keeping Client Identification Information Up-To-Date	30
3.2.4	Ongoing Monitoring: Reassessing Client Risk Levels	30
3.3	Implementing and Maintaining a Program to Ensure Performance of Compliance Tasks	31
3.3.1	Designated Compliance Officer	31
3.3.1.1	Sample Role Description of a Compliance Officer	31
3.3.1.2	Sample Qualifications of a Compliance Officer	32
3.3.2	Risk Assessment and Mitigation	32
3.3.2.1	Accountants and Accounting Firms' Risk of Money Laundering/ Terrorist Financing	32
3.3.2.2	Requirement for a Risk Assessment	33
3.3.2.3	Risk Assessment Process	33

3.3.2.4	Risk Assessment	34
3.3.2.4.1	Clients and business relationships	34
3.3.2.4.2	Products and delivery channels	35
3.3.2.4.3	Geographic location of the activities	35
3.3.2.4.4	Any other relevant factor	36
3.3.2.4.5	Risk Mitigation	36
3.3.3	Enhanced Due Diligence and Ongoing Monitoring	36
3.3.4	Policies and Procedures	38
3.3.4.1	Minimum Policies	38
3.3.4.1.1	General Policies	39
3.3.4.1.2	Reporting	39
3.3.4.1.3	Record Keeping	39
3.3.4.1.4	Ascertaining Identification	39
3.3.4.1.5	Third Party Determination	40
3.3.4.2	Sample List of Policies and Procedure Headings	40
3.3.5	Ongoing Training Program	41
3.3.5.1	Who Must Take the AML Training?	41
3.3.5.2	What Should Be Included in the Ongoing Training Program?	42
3.3.5.3	Sample Training Schedule	42
3.3.6	Effectiveness Review	43
3.3.6.1	What Does the Effectiveness Review Cover?	43
3.3.6.2	Sample Scope	45

CHAPTER 4

AML and Privacy Obligations **47**

4.1	Summary of KYC/CDD Requirements	47
4.2	Where AML and Privacy Get Complicated	47
4.3	What Does the AML Legislation Say About EDD Measures?	48
4.4	What Is Required for EDD Measures?	48
4.5	What Information Should Be Documented?	48

CHAPTER 5

Interactions with Other Reporting Entities **49**

CHAPTER 6	
FINTRAC Examinations	51
6.1 FINTRAC's Powers	51
6.2 How to Prepare	51
6.3 What to Expect	52
6.4 Follow Up	53
6.5 Compliance Assessment Report	54
CHAPTER 7	
Appendix A—Canada's AML Legislation	55
7.1 Provenance	55
7.2 Purpose	55
7.3 Players	56
7.4 Penalties and Criminal Fines for Non-Compliance	57
CHAPTER 8	
Appendix B—Links to FINTRAC Guidance	59
CHAPTER 9	
Appendix C—Summary of Changes Effective February 1, 2014	61
CHAPTER 10	
Appendix D—FINTRAC Interpretation Notice No. 2	63
CHAPTER 11	
Appendix E—FINTRAC Interpretation Notice No. 7	65
CHAPTER 12	
Appendix F—Sample Receipt of Funds Record	67

CHAPTER 13	
Appendix G—Identification of Individuals in Person: Method and Form	69
13.1 Requirements	69
13.2 Method	69
13.3 Form	71
CHAPTER 14	
Appendix H—Identification of Individuals Non-Face-to-Face: Methods	73
14.1 Requirements	73
14.2 Methods	73
CHAPTER 15	
Appendix I—Identification of Individuals by Third Parties: Methods	75
15.1 Requirements	75
15.2 Methods	75
CHAPTER 16	
Appendix J—Confirming the Existence of an Entity	77
16.1 Requirements	77
16.2 Method	77
16.3 Form	78
CHAPTER 17	
Appendix K—Large Cash Transaction Report Form	79
CHAPTER 18	
Appendix L—Suspicious Transaction Report Form	99
CHAPTER 19	
Appendix M—Terrorist Property Form	119

CHAPTER 20	
Appendix N—Self-Review Checklist	139
Part A: Compliance Framework Evaluation	139
Part B: Operational Compliance Evaluation	143
About the Author	145

CHAPTER 1

Motivation for the Guide

Since 2000, professional accountants in Canada have been an official part of the country's fight against money laundering and terrorist financing.¹ Our part in the fight generally involves keeping specified records about transactions and identifying clients from which we receive funds² in case that information should be needed for investigations; collecting, retaining and reporting large cash transactions;³ as well as reporting attempted and completed suspicious transactions⁴ and terrorist property⁵ to add to the national money laundering intelligence database. AML Legislation was recently amended with changes to obligations effective February 1, 2014.⁶ Those amendments also require Accountants and Accounting Firms to conduct ongoing monitoring of the relationships with clients involved in Triggering Activities.⁷

Canada codified obligations for Accountants and Accounting Firms in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its Regulations (collectively referred to in this document as "AML Legislation"). The regulator responsible for ensuring adherence to that legislation is the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC issues its own guidance to assist individuals and entities to comply with their obligations.⁸

1 Details about the offences of money laundering and terrorist financing, and Canada's anti-money laundering and counter terrorist financing initiatives and their history are included in Appendix A—Canada's AML Legislation.

2 See section 3.1.1 for details.

3 See section 3.1.2 for details.

4 See section 3.1.3 for details.

5 See section 3.1.4 for details.

6 Those changes are incorporated into this guidance, and summarized in Appendix C—Summary of Changes Effective February 1, 2014.

7 See section 3.2 for details.

8 A listing of links to FINTRAC guidance relevant to Accountants and Accounting Firms is included in Appendix B—Links to FINTRAC Guidance.

The obligations only apply to Accountants and Accounting Firms in certain circumstances, generally instances where they are dealing with assets on behalf of their clients.⁹ Once it is determined that they do apply, fulfilling the obligations may seem complex. Failing to comply with applicable AML Legislation in the prescribed circumstances can result in significant fines, penalties and jail time for Accountants and Accounting Firms.¹⁰

CPA Canada and its members are mandated to maintain the reputation of our profession. The profession's reputation can be tainted by non-compliance with legislation designed to combat crime, and worse, by association with activities that enable crime.

With that in mind, this *Guide* has three main purposes:

1. To help Accountants and Accounting Firms determine if AML obligations are applicable to their activities.
2. To guide Accountants and Accounting Firms to which AML Legislation applies in the development of a program to comply with their obligations.
3. To educate Accountants and Accounting Firms about the enforcement methods by the regulator FINTRAC and risks of non-compliance.

This *Guide* itself does not constitute an AML program. Each Accountant and Accounting Firm must develop its own policies and procedures, risk assessment and training program, as applicable.

⁹ These circumstances are described in section 2.2.

¹⁰ See section 7.4 for details.

CHAPTER 2

Determining if the Obligations Are Applicable

AML Legislation is applicable to Accountants and Accounting Firms engaging in Triggering Activities (described in section 2.2). Accountants and Accounting Firms have ongoing obligations to identify the performance of Triggering Activities and to perform all prescribed measures within specified timelines. As a practical matter, Accounting Firms are advised to perform annual training to make their organization aware of Triggering Activities in order that those in their firm are equipped to self-identify those circumstances. As a safeguard, Accounting Firms are advised to conduct an annual self-assessment to determine whether individuals in their organizations are involved in Triggering Activities, and to evaluate conformance of the related documentation to AML standards. Questionnaires aimed at assisting that determination are included in section 2.3.

2.1 Definition of Accountant and Accounting Firm

An “Accountant” is defined by AML Legislation as being a Chartered Accountant (CA), Certified General Accountant (CGA), or a Certified Management Accountant (CMA).¹¹ We expect that AML Legislation may be amended to include the new Chartered Professional Accountant (CPA) designation. This *Guide* has been prepared as though CPAs are covered.

¹¹ Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) subsection 1(2).

An “Accounting Firm” is defined by AML Legislation as being an entity that is engaged in the business of providing accounting services¹² to the public and has at least one partner, employee or administrator that is an accountant.¹³

The definition of Accountant does not require the professional to be engaged in providing professional accounting services to the public to be covered by the AML Legislation, only that they are a designated Accountant that performs, however infrequently, Triggering Activities.

An Accountant is not subject to AML Legislation if they only perform Triggering Activities on behalf of their employer.¹⁴ That employer could be an Accounting Firm, or any other entity. An Accountant performing any Triggering Activities for any client in addition to, or outside of their regular employment relationship would still be subject to AML Legislation, in respect of those outside activities.

2.2 Definition of Triggering Activities

Generally, Triggering Activities involve dealing with client assets on their behalf. Dealing with client assets might involve actually conducting transactions on their behalf, or giving instructions to a party to conduct the transactions.¹⁵ Exceptions and other considerations are explained in section 2.2.2.

There are three categories of Triggering Activities which are listed below with illustrative examples. These examples do not represent an exhaustive list of all possible Triggering Activity scenarios.

1. Receiving, Paying or Transferring Funds^{16,17}
 - a. Your Accounting Firm performs bookkeeping services and has signing authority over the account of a not-for-profit organization client and pays invoices from that account on its behalf.

12 “Accounting services” is not defined in the PCMLTFR. In Alberta, the *Regulated Accounting Profession Act* paragraph 1(oo) defines “public accounting practice” to include the providing or offering to provide one or more of the following services to the public: (i) an assurance engagement; (ii) a specified auditing procedures engagement; (iii) a compilation engagement; (iv) accounting services; (v) forensic accounting, financial investigation or financial litigation support services; (vi) advice about or interpretation of taxation matters; (vii) preparation of a tax return or other statutory information filing, if prepared in conjunction with any service referred to in subclauses (i) to (vi).

13 PCMLTFR subsection 1(2).

14 PCMLTFR subsection 34(2).

15 The concept of “giving instructions” is explained in more detail in section 2.2.1.

16 PCMLTFR paragraphs 34(1)(a)(i)(iii).

17 “Funds” are defined in the PCMLTFR 1(2) as meaning “cash, currency or securities, or negotiable instruments or other financial instruments, in any form, that indicate a person’s or an entity’s title or interest in them”.

- b. A client issues a cheque to you as a sole practitioner Accountant in an amount equal to their income tax payable and your accounting fees. You then deposit the cheque and wire the income tax payable to the Canada Revenue Agency from your account.
 - c. A client instructs their vendor to settle their invoice by remitting funds to your Accounting Firm and then asks that your firm issues a cheque for the difference between the value of the wire and your outstanding fees.
 - d. A client requests assistance in transferring funds from a sanctioned country into Canada, in respect of which an Accountant arranges for Canadian accounts and wire transfers through intermediate countries.
 2. Purchasing or Selling Real Property, Business Assets, or Entities¹⁸
 - a. The leader of the corporate finance group of your Accounting Firm travels to the U.S. to finalize the purchase of a business on behalf of their client.
 - b. Acting as the trustee for an estate, an Accountant instructs a real estate broker to sell a piece of land owned by the estate.
 3. Purchasing, Transferring or Selling Securities¹⁹
 - a. An Accountant within your Accounting Firm has been engaged by the lawyer of a client without capacity to manage their investments, and exercises discretionary authority to buy and sell securities on their behalf.
 - b. As part of a tax restructuring engagement, an Accountant opens investment accounts in other countries on behalf of their clients and orders domestically-held securities transferred there.
 - c. In connection with a corporate reorganization, an Accountant documents and executes share transfers in a minute book on behalf of their client.

2.2.1 Giving Instructions Versus Giving Advice

An interpretation notice from FINTRAC²⁰ distinguishes the concept of “giving instructions”, which would constitute a Triggering Activity in respect of any of the three categories, from “giving advice”, which would not constitute a Triggering Activity. Giving instructions is synonymous with “ordering” a specific transaction in this context (e.g. “Based on my client’s instructions, I request that you transfer \$600 from my client’s account 12345 to his other

18 PCMLTFR 34(1)(a)(ii)(iii).

19 *Ibid.*

20 See the Interpretation Notice No. 2 at Appendix D—FINTRAC Interpretation Notice No. 2.

account 67890”). Giving advice involves a recommendation to the client or their advisors rather than giving instructions to take action with respect to their assets (e.g. “For tax purposes, we recommend that you transfer your money into long-term investments”).

2.2.2 Specified Exemptions and Considerations

Once it has been determined that you are an Accountant or an Accounting Firm that engages in Triggering Activities, AML Legislation is applicable unless one of three exemptions apply:

1. In the case of an Accountant, when all Triggering Activities are performed on behalf of an employer.
2. In the case of an Accountant or an Accounting firm, where all Triggering Activities are performed in respect of an audit, review or compilation engagement.
3. In the case of an Accountant or Accounting firm acting solely in the capacity of a Trustee in Bankruptcy.

Additionally, for risk and other legislative reasons, some Accounting Firms have incorporated a separate entity through which they conduct Triggering Activities. Those entities are typically subject to other provisions of the same AML Legislation.

2.2.2.1 *Employment Relationship*

As mentioned earlier, an Accountant who performs Triggering Activities only for their employer is not subject to the AML Legislation. Triggering Activities performed by an Accountant outside of their employment relationship would not be exempted by this provision. An Accountant who both worked as full-time employee controller *and* maintained bookkeeping clients on whose behalf they transferred funds, would be covered by AML Legislation because of the latter activity, and only in respect of that latter activity.

2.2.2.2 *Assurance Related Activities*

AML Legislation holds that what would otherwise constitute Triggering Activities do not subject an Accountant or an Accounting Firm to its obligations in cases where those activities are performed in respect of “audit, review or compilation engagements carried out in accordance with the recommendations set out in the CICA Handbook”.²¹ Given the nature and standards governing those types of engagements, it is unlikely in any event that any Triggering Activities would be performed in connection with them.

21 PCMLTFR subsection 34(3). Also refer to Footnote 51.

2.2.2.3 *Trustee in Bankruptcy Services*

FINTRAC issued an interpretation notice²² advising that Accountants and Accounting Firms appointed by a Court, or acting solely as a trustee in bankruptcy, are not considered to be acting on behalf of any other individual or entity, and therefore, are not engaged in Triggering Activities.

Additionally, FINTRAC advised in the notice that practices that only provide the services listed below are not considered to be “providing accounting services to the public”, and therefore would not be considered to be an Accounting Firm subject to AML Legislation:

1. As a receiver, pursuant to the provisions of a Court order or by way of a private letter appointment pursuant to the terms of a security interest.
2. A trustee in bankruptcy.
3. As monitor under the provisions of the *Companies' Creditors Arrangement Act* or any other proceeding that results in the dissolution or restructuring of an enterprise or individual and to which the firm, individual or insolvency practitioner serves as an officer of the Court or agent to one or more creditors or the debtor.

Notwithstanding, a firm which provides any accounting services to the public outside of the scope of those three listed services will be deemed to be an Accounting Firm. An insolvency practice may, for instance, also perform restructuring and interim controller services outside of the context of an appointment which would bring their firm into the definition of an Accounting Firm. In that case, Triggering Activities performed by that practice, such as the sale of real property in the capacity of an interim controller, would subject them to the obligations of prevailing AML Legislation.

2.2.2.4 *Implications of Organizational Structure*

For risk management purposes and to comply with other legislation, it is common practice for Accounting Firms to incorporate separate entities—such as a corporate finance division—for activities that relate to purchasing or selling real property, business assets, entities or securities. If these entities do not offer accounting services to the public, then they would not be considered to be Accounting Firms and therefore not subject to AML Legislation on that basis. However, other obligations arise from AML Legislation for entities that are considered to be “securities dealers”²³ or real estate brokers. Firms that

22 See Interpretation Notice No. 7 at Appendix E—FINTRAC Interpretation Notice No. 7.

23 PCMLTFR subsection 1(2) defines “securities dealers” as being: a person or entity that is authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services.

organize separate entities should comply with laws relevant to their activities, and take care not to provide or offer accounting services to the public from those entities.

2.2.2.5 A Note on Client Fees

For clarity, Triggering Activities give rise to the obligations of AML Legislation whether or not professional fees are received for those activities.

Receiving payment for client fees does not in itself constitute a Triggering Activity as the funds are not received on behalf of a client—they are received on behalf of the firm itself. However, payments from clients where the amount is comprised of both fees and value for further payment to a third party, such as the Canada Revenue Agency, would be considered a Triggering Activity.

2.3 Questionnaires to Assist in Determining Applicability

2.3.1 Do I Have Obligations as an Accountant?

Question	Response	Comment/Direction
1. Are you a professionally designated Accountant (CPA, CA, CMA, CGA)?	Yes	Designated professional Accountants have responsibilities if they perform Triggering Activities. Proceed to Question 2.
	No	Non-designated accountants do not have responsibilities to AML Legislation by virtue of being accountants. 
2. Do you perform transactions or give instructions for transactions that involve any of these Triggering Activities on behalf of a client (on a compensated or non-compensated basis)? a. Receiving, Paying or Transferring Funds b. Purchasing or Selling Real Property, Business Assets, or Entities c. Purchasing, Transferring or Selling Securities	Yes	Performing Triggering Activities gives rise to obligations defined in AML Legislation, unless exceptions apply. Proceed to Question 3.
	No	If no Triggering Activities are performed or offered, no obligations arise from AML Legislation by virtue of being an Accountant. 

Question	Response	Comment/Direction
<p>3. Are all Triggering Activities you perform or offer done so as part of your employment?</p>	Yes	<p>If all Triggering Activities are performed in the course of an employment relationship, the obligations defined by AML Legislation are not applicable.</p> 
	No	<p>If any one Triggering Activity is performed outside of an employment relationship, obligations set out in AML Legislation are applicable, unless other exemptions apply.</p> <p>Proceed to Question 4.</p>
<p>4. Are all Triggering Activities performed in connection with assurance engagements or as part of trustee in bankruptcy appointments?</p>	Yes	<p>If all Triggering Activities are performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by AML Legislation are not applicable.</p> 
	No	<p>If any one Triggering Activity is conducted that is not performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by AML Legislation are applicable.</p> 

2.3.2 Do We Have Obligations as an Accounting Firm?

Question	Response	Comment/Direction
<p>1. Does your firm provide accounting services to the public?</p>	<p>Yes</p>	<p>An entity that provides any accounting services to the public may be considered an Accounting Firm if it has at least one partner, employee or administrator that is an Accountant. Note that insolvency related engagements that involve appointments as: receiver, trustee in bankruptcy, or as monitor under the provisions of the <i>Companies' Creditors Arrangement Act</i> are not considered to constitute accounting services.</p> <p>Proceed to Question 2.</p>
	<p>No</p>	<p>An entity that does not provide any accounting services to the public is not considered to be an Accounting Firm, and therefore would not have obligations pursuant to AML Legislation on that basis.</p> 
<p>2. Is at least one of your entity's partners, employees or administrators a professionally designated Accountant (CPA, CA, CMA, CGA)?</p>	<p>Yes</p>	<p>Any entity that offers accounting services to the public and has at least one designated professional Accountant as a partner, employee or administrator is considered to be an Accounting Firm, and would have responsibilities if they perform Triggering Activities.</p> <p>Proceed to Question 3.</p>
	<p>No</p>	<p>Any entity that offers accounting services to the public, but has no designated Accountant partners, employees or administrators, is not considered to be an Accounting Firm, and therefore would not be subject to AML Legislation obligations on that basis.</p>

Question	Response	Comment/Direction
3. Does your firm perform transactions or give instructions for transactions that involve any of these Triggering Activities on behalf of a client (on a compensated or non-compensated basis)? a. Receiving, Paying or Transferring Funds b. Purchasing or Selling Real Property, Business Assets, or Entities c. Purchasing, Transferring or Selling Securities	Yes	Performing any Triggering Activity, for any fees or no fees, gives rise to obligations defined in AML Legislation, unless exceptions apply. Receiving client fees does not itself constitute a Triggering Activity. Proceed to Question 4.
	No	If the firm performs no Triggering Activity, no obligations arise from AML Legislation by virtue of being an Accounting Firm. 
4. Are all Triggering Activities performed in connection with assurance engagements or as part of trustee in bankruptcy appointments?	Yes	If all Triggering Activities are performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by AML Legislation are not applicable. 
	No	If any one Triggering Activity is conducted that is not performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by AML Legislation are applicable. 

2.4 Determination of Triggering Activities in Larger Firms

Once it is determined that you are an Accountant or an Accounting Firm, there is an ongoing risk that you or your firm conducts a Triggering Activity (even if it is determined at a point in time that no Triggering Activity has occurred in the past or is not expected in the future). The engagement in one single Triggering Activity gives rise to the full scope of obligations under AML Legislation applicable to Accountants and Accounting firms, including training obligations, policies and procedures, risk assessments, etc. AML Legislation does not address the issue of how long obligations apply following an Accountant's or Accounting Firm's engagement in a single Triggering Activity.

Given the extent of effort required to maintain a Compliance Regime, and the significance of consequences for non-compliance, it is advisable that Accounting Firms direct resources to the determination of engagement in Triggering Activities across their firm at a point in time and then annually thereafter. A sole-practitioner Accountant may just complete the questionnaire provided above annually. At an Accounting Firm with less than ten partners, that determination may be limited to adding the item to the annual partner meeting agenda for discussion and declaration. At larger firms, education coupled with questionnaires, engagement checklists, and internal audit procedures may be more appropriate.

Some Accounting Firms have adopted a policy to prohibit engagement of Triggering Activities because of the risk and resource they entail, or to conduct them by authorized exception only. To satisfy examiners, those firms may wish to engage in an annual and documented self-assessment exercise to assess adherence to that prohibition policy. Even Accounting Firms that prohibit Triggering Activities or believe that they do not engage in such activities adopt a program to comply with AML Legislation in case Triggering Activities are inadvertently performed.

CHAPTER 3

What to Do if the Obligations Are Applicable

Accountants and Accounting Firms that engage in Triggering Activities are subject to the obligations of AML Legislation. Those obligations include the requirement to perform certain tasks when engaging in Triggering Activities that are associated with certain types of transactions, and to implement and maintain a program to ensure that those tasks are performed.

3.1 Required Tasks When Engaged in Triggering Activities

Being engaged in a Triggering Activity by itself does not trigger any required transaction-related tasks.²⁴ Certain tasks must be performed if engaged in a Triggering Activity **and** one or more of the following situations (or “Special Cases”) arise in connection with the Triggering Activity: the receipt of C\$3,000 or more;²⁵ the receipt of C\$10,000 or more in cash; reasonable grounds to suspect money laundering or terrorist financing; and, knowledge of terrorist property. The following table summarizes those situations and the associated task obligations.

24 Notwithstanding, engaging in any Triggering Activity gives rise to the obligation to implement and maintain a compliance program.

25 All amounts are expressed in Canadian dollars. Amounts received in foreign currencies must be translated to Canadian dollar equivalents using the official conversion rate of the Bank of Canada for that currency as published in the Bank of Canada’s Daily Memorandum of Exchange Rates that is in effect at the time of the transaction to assess whether applicable thresholds have been met (PCMLTFR paragraph 2(a)).

Special Case	Receipt of Funds Record	Client Identification	Large Cash Transaction Report	Third Party Determination	Suspicious Transaction Report	Terrorist Property Report
Receiving funds of C\$3,000 or more (section 3.1.1)	•	•				
Receiving C\$10,000 or more in cash (section 3.1.2)	•	•	•	•		
Suspicious activity or transaction (section 3.1.3)		•			•	
Knowledge of terrorist property (section 3.1.4)						•

3.1.1 Receiving Funds of \$3,000 or More

If funds²⁶ of C\$3,000 or more are received by an Accountant or Accounting Firm in a single transaction in connection with a Triggering Activity, two task obligations are triggered:

1. Keep a receipt of funds record.
2. Identify the client from whom the funds are received.

Those funds might be received in respect of fees, or for any other reason connected with the Triggering Activity. AML legislation does not specify that the funds must be received from the client for which the Triggering Activity is being performed.

3.1.1.1 Exemptions

The obligations noted do not apply if the funds are received from a client that is a financial entity²⁷ or a public body.²⁸

26 “Funds” are defined in the PCMLTFR 1(2) as meaning “cash, currency or securities, or negotiable instruments or other financial instruments, in any form, that indicate a person’s or an entity’s title or interest in them.”

27 “Financial Entity” means an authorized foreign bank, as defined in section 2 of the *Bank Act*, in respect of its business in Canada or a bank to which that Act applies, a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial Act, an association that is regulated by the *Cooperative Credit Associations Act*, a financial services cooperative, a credit union central, a company to which the *Trust and Loan Companies Act* applies and a trust company or loan company regulated by a provincial Act. It includes a department or agent of Her Majesty in right of Canada or of a province when the department or agent is carrying out an activity referred to in section 45.

28 “Public Body” means (a) any department or agent of Her Majesty in right of Canada or of a province; (b) an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body or an agent of any of them; and (c) an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the *Excise Tax Act*, or any agent of such an organization.

If the funds received involve C\$10,000 or more in cash, a Large Cash Transaction Report should be completed, retained and filed with FINTRAC instead of producing a receipt of funds record (see section 3.1.2—Receiving funds of \$10,000 or More in Cash).

3.1.1.2 *Receipt of Funds Record*

A sample receipt of funds record is shown in Appendix F—Sample Receipt of Funds Record. All fields on that form are mandatory. An Accountant or Accounting Firm may choose to maintain the information required in a receipt of funds record as part of its regular records (on paper or electronically in order that a paper copy can be readily produced from it),²⁹ as long as all information can be produced to FINTRAC within 30 days of a request.³⁰ The receipt of funds record must be retained for five years following the date of its creation. Receipt of funds records should not be filed with FINTRAC, however, their details might be subsequently referenced as necessary in Large Cash Transaction Reports (see section 3.1.2.4) or Suspicious Transaction Reports (section 3.1.3).

3.1.1.3 *Client Identification*

Client identification must occur at or before the time of the transaction to which the receipt relates, although it should occur as soon as practical after being engaged to conduct a Triggering Activity. In instances where funds are received unexpectedly and without the client present, and where the client had not been previously identified, the Accountant or Accounting Firm should identify the client prior to processing or returning the funds (both to meet regulatory obligations and to establish ownership over the property).

The purpose of client identification is to verify the identity of the person (name, address and date of birth) with whom you are dealing, in the case of a natural person, and, in the case of an entity, to verify the existence of the entity with which you are dealing and to verify the identity of the individual who is dealing on its behalf (with reference to corporate/other entity documentation).

29 PCMLTFR subsection 68(a).

30 PCMLTFR section 70.

AML Legislation permits client identification to occur in the following ways:

1. For individuals (natural persons):
 - a. Face-to-face: If the client is met in person, AML Legislation permits Accountants and Accounting Firms to verify their identity with reference to one piece of original government-issued valid and unexpired identification. See Appendix G—Identification of Individuals in Person: Method and Form.
 - b. Non-Face-to-Face: When a client is identified remotely (i.e., they are not physically present when you inspect their original, valid, and unexpired piece of government-issued identification), AML Legislation permits reference to a combination of one necessary and one sufficient identification method. The necessary methods include reference to credit checks or an attestation by a limited class of professionals, and the acceptable sufficient identification methods generally include confirmation against a Canadian deposit account. See Appendix H—Identification of Individuals Non-Face-to-Face: Methods.
 - c. Using an Agent or Mandatary: It is possible to contract a third party to conduct face-to-face identification measures on your behalf (i.e. have a third party pre-contracted to verify the identity of a client with reference to one piece of original government-issued valid and unexpired identification. While the task can be delegated to an agent, the responsibility for client identification rests with the Accountant/Accounting Firm. See Appendix I—Identification of Individuals by Third Parties: Methods.

Individual client information records must be maintained for five years following the date on which they were created. It may be prudent to retain those records for a longer period in case of the need for subsequent reliance in other identification scenarios, and on account of other obligations and uses, while respecting privacy obligations.

2. For entities: Where an entity is the client for Triggering Activities, the Accountant or Accounting Firm must confirm the existence of the entity with reference to its incorporation records, organizing agreements, and retain a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation. See

Appendix J— Confirming the Existence of an Entity. Information collected in respect of this obligation must be maintained for five years following the date the last business transaction is conducted.

Successful client identification need not be repeated for subsequent transactions if the Accountant/Accounting Firm recognizes the client.³¹

3.1.2 Receiving Funds of \$10,000 or More in Cash

When you receive an amount of C\$10,000 or more in cash³² over one or more transactions over 24 consecutive hours, in respect of a Triggering Activity, by, or on behalf of the same person or entity, you must (a) keep a large cash transaction record; (b) file a large cash transaction report with FINTRAC within 15 days; and (c) take reasonable measures to determine whether there is third party involvement.

While an Accountant or Accounting Firm might prohibit the acceptance of cash by policy or practice, cash may still be received inadvertently (by mail or otherwise). As a consequence, it is advisable to adopt a policy and procedure to deal with that eventuality. Some firms have adopted a policy whereby the sender will be invited to identify themselves to the firm in person and retrieve the funds intact within a certain number of days following receipt, and notified that the funds will be returned intact otherwise by the same method by which they were received. Depositing the funds into the Accountant's or Accounting Firm's account and then remitting them back to the sender may assist in achieving money laundering objectives, given the apparent legitimacy of payments received from an Accountant/Accounting Firm. It has been the administrative practice of FINTRAC that obligations described below still apply if the funds are returned, since the cash has been received.

3.1.2.1 Exemptions

The noted obligations do not apply if the funds are received from a client that is a financial entity or a public body.

3.1.2.2 Client Identification

Client identification must occur at or before the time the funds are received, although it should occur as soon as practical after being engaged to conduct a Triggering Activity. In instances where funds are received unexpectedly and without the client present, the Accountant or Accounting Firm should identify the client prior to processing or returning the funds (both to meet regulatory obligations and to establish ownership over the property).

31 FINTRAC's administrative position is that "recognizing the client" involves recognizing the face or voice of an individual.

32 "Cash" means coins or notes issued by the Bank of Canada or coins or bank notes of countries other than Canada.

The purpose of client identification is to verify the identity of the person (name, address and date of birth) with whom you are dealing, in the case of a natural person, and, in the case of an entity, to verify the existence of the entity with which you are dealing and to verify the identity of the individual who is dealing on its behalf (with reference to corporate/other entity documentation).

AML Legislation permits client identification to occur in the following ways:

1. For individuals (natural persons):
 - a. Face-to-face: If the client is met in person, AML Legislation permits Accountants and Accounting Firms to verify their identity with reference to one piece of original government-issued valid and unexpired identification. See Appendix G—Identification of Individuals in Person: Method and Form.
 - b. Non-Face-to-Face: When a client is identified remotely (i.e., they are not physically present when you inspect their original, valid, and unexpired piece of government-issued identification), AML Legislation permits reference to a combination of one necessary and one sufficient identification method. The necessary methods include reference to credit checks or an attestation by a limited class of professionals, and the acceptable sufficient identification methods generally include confirmation against a Canadian deposit account. See Appendix H—Identification of Individuals Non-Face-to-Face: Methods.
 - c. Using an Agent or Mandatary: It is possible to contract a third party to conduct face-to-face identification measures on your behalf (i.e., have a third party pre-contracted to verify the identity of a client with reference to one piece of original government-issued valid and unexpired identification). See Appendix I—Identification of Individuals by Third Parties: Methods.

Individual client information records must be maintained for five years following the date on which they were created.

2. For entities: Where an entity is the client for Triggering Activities, the Accountant or Accounting Firm must confirm the existence of the entity with reference to its incorporation records, organizing agreements, and retain a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation. See

Appendix J—Confirming the Existence of an Entity. Information collected in respect of this obligation must be maintained for five years following the date the last business transaction is conducted.

Successful client identification need not be repeated for subsequent transactions if the Accountant/Accounting Firm recognizes the client.³³

3.1.2.3 Third Party Determination

Third party determination involves taking measures to confirm whether or not the person from whom the cash is received is acting on someone else's instructions, and then collecting details about that instructing party. The instructing party may be an individual or an entity. The required details include:

- name, address and principle business or occupation of the third party
- if the third party is an individual, their date of birth
- if the third party is a corporation, the incorporation number and place of incorporation
- the nature of the relationship between the third party and the individual who gives you the cash

This information can be recorded on the Large Cash Transaction Record, and must be maintained for five years following the transaction.

An employee is not considered to be a third party with respect to their employer.

3.1.2.4 Large Cash Transaction Record and Report

AML Legislation requires that Accountants and Accounting Firms create a Large Cash Transaction Record and retain it for five years following the transaction, and also that they file a Large Cash Transaction Report with FINTRAC on paper or electronically within 15 days following the transaction. Client identification and third party determination should precede the completion of the record and report to obtain all necessary details (as long as those steps can be completed and the report filed within the 15 day timeline).

A sample of the Large Cash Transaction Report form is included in Appendix K—Large Cash Transaction Report Form.³⁴ All fields marked with an asterisk are mandatory fields. All other fields are “reasonable efforts” fields, which mean that they must be completed if the information is available to the Accountant or Accounting Firm. Maintaining a copy of the Large Cash

33 FINTRAC's administrative position is that “recognizing the client” involves recognizing the face or voice of an individual.

34 An electronic version can be obtained from FINTRAC's website by following this link: www.fintrac.gc.ca/publications/LCTR-2008-eng.pdf.

Transaction Report can serve as a Large Cash Transaction Record, since the mandatory fields of the report cover all the requirements of the record. Field-by-field guidance on completing the report is included after the sample in Appendix K—Large Cash Transaction Report Form.

A suspicious transaction report (explained in section 3.1.3) may also be filed in respect of the transactions reported as large cash transactions if circumstances warrant.

3.1.3 Suspicious Transaction or Activity

Within 30 days of the detection of facts first giving rise to suspicion, Accountants and Accounting Firms must report electronically or on paper attempted and completed suspicious transactions which relate to Triggering Activities to FINTRAC using the prescribed forms. A sample form is included at Appendix L—Suspicious Transaction Report Form.³⁵ The occurrence of a suspicious transaction also gives rise to an obligation to take reasonable measures to ascertain the identity of a person that attempts or conducts the suspicious transaction unless that person had been previously identified according to the AML Legislation standards, or if conducting the identification would make the person aware that a report was being filed (known as “Tipping Off”).

3.1.3.1 Establishing Reasonable Grounds for Suspicion

According to AML Legislation, Accountants and Accounting Firms are required to report to FINTRAC, using the prescribed form, every financial transaction that occurs or is attempted in the course of Triggering Activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or the attempted commission of (a) a money laundering offence; or (b) terrorist activity financing offence.³⁶

The offence of money laundering in Canada broadly involves a person who deals with property or proceeds of any property they know or believe was derived directly or indirectly as a result of a designated offence committed in Canada or elsewhere, with the intent to conceal or convert³⁷ that property or those proceeds.³⁸ Designated offences include all manner of offences that can generate proceeds and could result in jail sentences of two years or more (even murder for hire). Particularly, they include offences related to:

35 An electronic version can be obtained from FINTRAC's website by following this link: www.fintrac.gc.ca/publications/STR-2008-eng.pdf.

36 PCMLTFA section 7.

37 Convert means to change or transform, and does not require an element of concealment (R. v. Daoust, [2004] 1 SCR 217, 2004 SCC 6).

38 Criminal Code of Canada subsection 462.31.

drugs, fraud, theft, robbery, tax evasion, copyright, as well as break and enter. According to FINTRAC, the person reporting the transaction need not have knowledge or suspicion of the specific offence that gave rise to the proceeds, only reasonable grounds to suspect that reported transactions are related to money laundering or terrorist financing.³⁹

The offence of terrorist financing generally involves providing or collecting property intending or knowing that it will be used in whole or in part to carry out a terrorist activity. Terrorist activity includes such things as acts committed for a political, religious, ideological purpose with the intention of intimidating the public with regard to economic or physical security, or compelling any person, government or international organization to do or to refrain from doing any act, and that intentionally causes or endangers health, property, services, facilities or systems.⁴⁰ The government maintains a list of entities they have reasonable grounds to believe have knowingly carried out, attempted to carry out, participated in or facilitated terrorist activity; or knowingly acting on behalf of such an entity.⁴¹

Research has found that the methods employed for money laundering and terrorist financing are similar.

Reasonable grounds to suspect has been held to be equivalent to a “sufficient reasonable articulable suspicion,”⁴² which must rely on a “constellation of objectively discernible facts”.⁴³ A “hunch based on intuition gained by experience”⁴⁴ is not sufficient. The discernible facts can consist of information collected about the client, their historical and expected transaction behaviour, and research conducted. One way of identifying potentially suspicious transactions is to be vigilant about indicators of money laundering (see section 3.1.3.3) at the time of the transaction. Another is through the conduct of ongoing monitoring and enhanced due diligence of clients and their activities (discussed in section 3.2).

3.1.3.2 How Money is Laundered

Money laundering methods are often described in three stages: placement, layering and integration. A money launderer’s first problem is typically placing cash into the financial system. The placement stage attracts the most

39 FINTRAC Frequently Asked Questions: www.fintrac.gc.ca/questions/FAQ/2-eng.asp?ans=65.

40 Criminal Code of Canada section 2.

41 www.publicsafety.gc.ca/cnt/ntnl-scrtr/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx

42 R. v. Mann, [2004] 3 SCR 59, 2004 SCC 52.

43 R. v. Simpson (1993), 12 O.R. (3d) 182.

44 R. v. Mann, [2004] 3 SCR 59, 2004 SCC 52.

attention, and is the one at which most money laundering laws and risk mitigation tools are directed, and is therefore one of the hardest stages. Even if just this one stage is accomplished, money is laundered—since the proceeds of crime have been converted. Placement is so critical to money laundering because once nefariously generated funds are in the system, it becomes difficult to distinguish a good dollar from a bad dollar. Placement is sometimes accomplished by simply depositing illicitly generated funds at a financial institution, while others involve converting cash into commodities like gold and diamonds before selling them into the financial system.

More sophisticated schemes also try to create further distance and obscurity between that original transaction and the ultimate use of the money—ideally severing the audit trail, a process called layering. Layering might involve changing the domicile of money, or transferring it in ways that obscures the origin or destination of the funds. Integration is commonly known as the final stage of money laundering—it is the stage during which the proceeds of crime are used to buy assets or pay for further criminal operations. For a money launderer, it is ideal that the assets and payments funded by criminal activities have an alternative legitimate explanation for their origin.

The methods and techniques employed at any of those stages vary in complexity and sophistication and will depend on the jurisdiction, the origins and amount of money that needs to be cleaned. A report issued by the Egmont Group,⁴⁵ a worldwide association of Financial Intelligence Units, suggests five general categories of means by which money is laundered (known as “typologies”): Concealment within Business Structures; Misuse of Legitimate Businesses; Use of False Identities, Documents, or Straw Men; Exploiting International Jurisdictional Issues; and the Use of Anonymous Asset Types.

3.1.3.2.1 *Concealment within Business Structures*

Money laundering schemes can involve concealing illicit proceeds of crime within the structure of an existing business owned or controlled by the criminal organization. The funds can be intermingled with legitimate transactions of the business and moved throughout the financial system. Detecting this type of activity is difficult as it may take great amounts of analysis to distinguish between legitimate business transactions and those above and beyond which would be from criminal activities. False invoices and receipts can be utilized to demonstrate to their financial institution that the transactions have in fact “occurred”. However, the funds being deposited are in fact proceeds of crime disguised as legitimate business profits.

45 FIU's in Action: 100 cases from the Egmont Group.

3.1.3.2.2 *Misuse of Legitimate Businesses*

A similar scheme is through legitimate businesses which are not controlled by the criminal organization. One advantage over the previous scheme is that this method provides additional separation for the criminal organization as the criminal funds would be linked to the legitimate business and not the criminals misusing the business. For instance, illicit funds may be deposited with a financial institution and transferred to an account held at a foreign financial institution.

3.1.3.2.3 *Use of False Identities, Documents, or Straw Men*

False identities, documents and “straw men” are another common method utilized to launder proceeds of crime. This involves separating the assets from a criminal and associating the funds with an individual who had no involvement with the initial criminal activity. For instance, false documents and identities can be used to open bank accounts and create a buffer between the criminal and the illicit funds. Even if the criminal is prosecuted and has all assets under their name seized, the assets held under a false identity will be available.

3.1.3.2.4 *Exploiting International Jurisdictional Issues*

On a larger scale, international jurisdictions are exploited for the benefit of laundering money. Criminals will take advantage of differing legislation in foreign jurisdictions to successfully launder illicit proceeds of crime. For instance, identification requirements, disclosure requirements, company formation laws and secrecy laws all provide avenues that are exploited for the benefit of disguising and laundering funds. In favourable jurisdictions, criminals can open bank accounts, form corporations and send funds with ease and secrecy and, therefore, distort the true source and ownership of the illicit funds.

3.1.3.2.5 *Use of Anonymous Asset Types*

Similarly, the use of anonymous asset types allows criminals to separate the ownership of the assets from themselves and any law enforcement actions related to those assets. Cash, jewellery and precious metals are all anonymous asset types favoured by criminals. This explains the prevalence of conducting drug trafficking in cash as opposed to other payment methods which can be traced back to the criminal.

3.1.3.3 *Indicators of Money Laundering and Terrorist Financing*

In its Guideline 2 in respect to suspicious transaction reports, FINTRAC provides a number of indicators about which Accountants and Accounting Firms should be vigilant.⁴⁶ The presence of an indicator is one factor which may lead to the consideration of a suspicious transaction report, but by itself is

46 www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp

not definitive. Contextual information about the client, the transaction(s) and historical behaviour will assist in determining whether there are sufficient grounds to suspect the transactions are relevant to a money laundering or terrorist financing offence.

- Client appears to be living beyond his or her means.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company 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.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

3.1.3.4 Tipping Off

It is an offence to disclose that a suspicious transaction report has been filed, or to disclose the content of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.⁴⁷ However, it is common practice in other industries for reporting entities to request clarifying information about transactions for the purpose of enhanced due diligence, without reference to suspicious transaction reporting obligations.

47 PCMLTFA section 8.

3.1.3.5 *Client Identification*

The occurrence of a suspicious transaction gives rise to an obligation to take reasonable measures to ascertain the identity of a person that attempts or conducts the suspicious transaction unless that person has been previously identified according to the AML Legislation standards. Identification should not be attempted if that attempt risks tipping off the client to the consideration or filing of a report. The policy of conducting identification at the engagement stage for a Triggering Activity helps to alleviate both the need to identify following a suspicious transaction and the risk that doing so will tip off a client to the filing of a report.

The purpose of client identification is to verify the identity of the person (name, address and date of birth) with whom you are dealing, in the case of a natural person, and, in the case of an entity, to verify the existence of the entity with which you are dealing and to verify the identity of the individual who is dealing on its behalf (with reference to corporate/other entity documentation).

AML Legislation permits client identification to occur in the following ways:

1. For individuals (natural persons):
 - a. Face-to-face: If the client is met in person, AML Legislation permits Accountants and Accounting Firms to verify their identity with reference to one piece of original government-issued valid and unexpired identification. See Appendix G—Identification of Individuals in Person: Method and Form.
 - b. Non-Face-to-Face: When a client is identified remotely (i.e., they are not physically present when you inspect their original, valid, and unexpired piece of government-issued identification), AML Legislation permits reference to a combination of one necessary and one sufficient identification method. The necessary methods include reference to credit checks or an attestation by a limited class of professionals, and the acceptable sufficient identification methods generally include confirmation against a Canadian deposit account. See Appendix H—Identification of Individuals Non-Face-to-Face: Methods.
 - c. Using an Agent or Mandatary: It is possible to contract a third party to conduct face-to-face identification measures on your behalf (i.e., have a third party pre-contracted to verify the identity of a client with

reference to one piece of original government-issued valid and unexpired identification). See Appendix I—Identification of Individuals by Third Parties: Methods.

Individual client information records must be maintained for five years following the date on which they were created.

2. For entities: Where an entity is the client for Triggering Activities, the Accountant or Accounting Firm must confirm the existence of the entity with reference to its incorporation records, organizing agreements, and retain a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation. See Appendix J—Confirming the Existence of an Entity. Information collected in respect of this obligation must be maintained for five years following the date the last business transaction is conducted.

3.1.3.6 *Completing the Suspicious Transaction Record and Report*

Completed and attempted suspicious transactions can be reported to FINTRAC either electronically, if the Accountant/Accounting Firm has the technical capability to do so, or, otherwise, in paper format. A copy of the paper form is attached in Appendix L—Suspicious Transaction Report Form along with field-by-field guidance on completing the report. A copy must be retained for five years following the transaction(s), and filed with FINTRAC within 30 days of the detection of facts first giving rise to suspicion. All fields marked with an asterisk are mandatory fields. All other fields are “reasonable efforts” fields, which mean that they must be completed if the information is available to the Accountant or Accounting Firm.

Maintaining a copy of the Suspicious Transaction Report can serve as a Suspicious Transaction Record, since the mandatory fields of the report cover all the requirements of the record.

Client identification, if possible, should precede the completion of the record and report to obtain all necessary details (so long as those steps can be completed and the report filed within the 30 day timeline).

FINTRAC has identified the suspicious transaction narrative portion of the report (known as section G) as being the most critical to their intelligence objectives. In addition to detailing reasons for suspicion, FINTRAC desires these information elements in the narrative: the names of individuals and entities involved in transactions; directorships and signing authorities for business entities; account numbers and other key identifiers (e.g., date of birth,

government-issued ID, addresses, telephone numbers); the flow of funds; historical transaction activity; and associated entities and individuals and relationships between them (e.g., family members, business associates).⁴⁸

3.1.4 Knowledge of Terrorist Property

In the context of performing Triggering Activities, Accountants and Accounting Firms are required to report to FINTRAC using the prescribed paper form without delay when they know they are in possession or control of property that is owned or controlled on behalf of a terrorist or terrorist group, and when they believe they are in possession or control of property that is owned or controlled by or on behalf of a designated person. It is an offence to deal with such property, and imperative that it be reported without delay to the RCMP and the Canadian Security Intelligence Service (CSIS). AML Legislation does not impose a duty on Accountants or Accounting Firms to screen the names of their Triggering Activities clients against terrorist lists. An Accountant or Accounting Firm may, for example, become aware of such a situation because of research conducted during engagement acceptance procedures, through press clippings, or based on the advice of law enforcement.

If the Accountant or Accounting Firm is not sure that the property is owned or controlled on behalf of a terrorist, terrorist group or designated person, FINTRAC encourages the filing of a suspicious transaction report (see section 3.1.3) instead of a terrorist property report.

3.1.4.1 Terrorists, Terrorist Groups, and Designated Persons

Canada's listings of terrorists, terrorist groups, and designated persons are available on the Public Safety Canada website (www.publicsafety.gc.ca/cnt/ntnl-scr/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx) and from the Office of the Superintendent of Financial Institutions' website (www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/atf-fat/Pages/default.aspx).

3.1.4.2 Definition of Property

Property means any type of real or personal property which includes any deed or instrument giving title or right to property, or giving right to money or goods (for example, cash, bank accounts, insurance policies, money orders, real estate, securities, precious metals and stones, and traveler's cheques).

48 FINTRAC Feedback on Suspicious Transaction Reporting.

3.1.4.3 Filing a Terrorist Property Report

The Terrorist Property Form included as Appendix M—Terrorist Property Form⁴⁹ must be filed with FINTRAC without delay by faxing it to 1.866.226.2346. A copy must be retained for five years following the transaction, and it is advisable to maintain a record of successful transmission of the fax. Instructions to complete the form are included on the pages following the form. All fields marked with an asterisk are mandatory fields. All other fields are “reasonable efforts” fields, which mean that they must be completed if the information is available to the Accountant or Accounting Firm.

3.1.4.4 Advising the RCMP and CSIS

Concurrent with the filing of a terrorist property report, the Accountant or Accounting Firm must send the information to the RCMP and CSIS without delay. That may be accomplished by faxing the completed terrorist property report to the RCMP Anti-Terrorist Financing Team at 613.949.3113 and to the CSIS Financing Unit at 613.231.0266. It is advisable to maintain a record of the successful transmission of both faxes.

3.2 Ongoing Monitoring of Triggering Activity Business Relationships

Pursuant to regulatory amendments known as SOR/2013-15, Accountants and Accounting Firms must recognize the establishment of a “business relationship” with any client for which two or more Triggering Activities are performed and client identification is required after January 31, 2014, within any rolling five year period. That is, a business relationship is established for every client for which two or more transactions occur involving the creation of a receipt of funds record and a large cash or suspicious transaction report is filed within any rolling five year period. The establishment of a business relationship gives rise to the immediate obligation to keep a record that sets out the “purpose and intended nature of the business relationship”, and then the ongoing obligations to periodically monitor the business relationship, on a risk-sensitive basis, for the purpose of:

1. Detecting any reportable suspicious transactions or attempted suspicious transactions.
2. Keeping client identification information up-to-date.
3. Reassessing the level of risk associated with the client's transactions and activities.

⁴⁹ An electronic version can be obtained from FINTRAC's website by following this link: www.fintrac.gc.ca/publications/TPR-2008-eng.pdf.

4. Determining whether transactions or activities are consistent with the information obtained about the client, including the risk assessment of the client.

All of the measures and the definition of purpose and intended nature of the business relationship are with reference only to Triggering Activities. Non-Triggering Activities (such as the performance of an audit engagement) are to be excluded from the analysis.

Measures undertaken to conduct ongoing monitoring, as well as findings and outcomes, must be documented. Ideally, all ongoing monitoring for any given client is conducted on the same cycle to achieve efficiencies.

3.2.1 Defining the Purpose and Intended Nature of a Business Relationship

In FINTRAC's Guideline 6D, a non-exhaustive list of three potential "Purpose and Intended Nature of Business Relationship" descriptions is suggested:

- transferring funds or securities
- paying or receiving funds on behalf of a client
- purchasing or selling assets or entities

The Purpose and Intended Nature of Business Relationship must be recorded in a Business Relationship Record created at the inception of the business relationship. FINTRAC guidance suggests that the information recorded is meant to assist in understanding the client's activities over time, and that a determination could be achieved through a combination of information on hand and inquiries of the client. In professional accounting scenarios, the engagement letter typically documents the client's objectives (purpose of the business relationship) and services to be offered (nature of the business relationship). It is critical that policies and procedures reflect the adoption of that information source for the determination if that is the approach taken by the Accountant or Accounting Firm.

3.2.2 Ongoing Monitoring: Detecting Suspicious Transactions and Assessing Consistency of Transactions with Client Knowledge and Risk

An ongoing monitoring exercise to detect suspicious transactions for a client with which an Accountant or Accounting Firm has established a business relationship for Triggering Activities would generally involve a historical review of Triggering Activities conducted in the period under the review. The review frequency and scope would depend on the assessment of the client's risk, and should be documented. Triggering Activity transactions would generally

be compared against expectations and in view of suspicious transaction indicators, for a perspective that might not have arisen for consideration of each Triggering Activity transaction in isolation.

3.2.3 Ongoing Monitoring: Keeping Client Identification Information Up-To-Date

Keeping client identification up-to-date for clients with which the Accountant or Accounting Firm has established a business relationship must occur with a frequency commensurate with the client's money laundering risk. Updating client information does not involve re-identifying the client—re-identification should generally occur only when the veracity of identification is in question, or when a client is not recognized in the course of a transaction attempt. Client information updates, rather, involve re-confirming and updating information regarding client identification which might change over time, such as legal name, address and occupation. The measures taken and outcomes must be documented contemporaneously.

3.2.4 Ongoing Monitoring: Reassessing Client Risk Levels

As explained in the section titled 3.3.2 *Risk Assessment and Mitigation*, client risk levels are determined with reference to their characteristics, products and services, relevant geographies and other relevant factors. Through ongoing monitoring with a frequency determined by the pre-existing risk level, client risk is re-evaluated against risk factors established by the Accountant or Accounting Firm. Based upon a review of the client's activities and transactions and the updated client information, it may result in a higher or lower risk assessment for the client. For instance, if the client has reduced the amount of activity and their transactions have become less frequent, all else being equal, their risk level may be reduced to low from medium. The opposite is also true where based on a change in client information and activity, the level of risk can be raised from low to medium or high. The rationale for changes to the risk level should reflect the risk assessment methodology established when the risk assessment documentation was created.

3.3 Implementing and Maintaining a Program to Ensure Performance of Compliance Tasks

AML Legislation requires that Accountants and Accounting Firms implement and keep an up-to-date program to achieve compliance with required tasks. The Compliance Regime is comprised of five mandatory components:

1. a designated compliance officer
2. an inherent risk assessment and risk mitigation plan
3. policies and procedures
4. an ongoing training program
5. an effectiveness review

3.3.1 Designated Compliance Officer

As part of the Compliance Regime, you are required to appoint a person who is responsible for the implementation of the Compliance Regime. The Compliance Officer has an overall accountability for the Compliance Regime. The person that is appointed the role of the Compliance Officer should be adequately qualified and maintain relevant anti-money laundering and counter terrorist financing knowledge.

3.3.1.1 *Sample Role Description of a Compliance Officer*

- The Compliance Officer is to ensure that the AML policies and procedures are kept up-to-date and that all changes are approved by Senior Management and the Board of Directors.
- The Compliance Officer is to ensure that the risk-based training program is documented and tailored to meet the AML roles and responsibilities of different staff.
- The Compliance Officer is to ensure that the effectiveness review of the organization's Compliance Regime will be conducted at least every two years.
- The Compliance Officer is to conduct an assessment of the inherent risk of money laundering and terrorist financing on an ongoing basis.
- The Compliance Officer should understand and monitor the effectiveness of the technology used to enable AML compliance to ensure that transactional alerts and regulatory reports generated are accurate, complete and reflect the actual operations of the organization.

3.3.1.2 Sample Qualifications of a Compliance Officer

The person that is appointed the role of the Compliance Officer should be adequately qualified and maintain relevant anti-money laundering and counter terrorist financing knowledge. The Compliance Officer should have the following:

- Thorough working knowledge of money laundering and counter terrorist financing risks and controls of the organization.
- Knowledge of the anti-money laundering and counter terrorist financing regulatory requirements.
- Broad knowledge of the operations of the organization.
- Appropriate professional qualifications, experience and strong leadership skills.

The appointment of the Compliance Officer, and any changes to that appointment, should be formally documented.

3.3.2 Risk Assessment and Mitigation

3.3.2.1 Accountants and Accounting Firms' Risk of Money Laundering/Terrorist Financing

Accountants are considered “gatekeepers” of the financial system. Gatekeepers, as defined by the Financial Action Task Force (FATF), are individuals that protect the gates to the financial system through which potential users of the system, including launderers, must pass in order to be successful.

According to studies conducted by international organizations, accountants are highly susceptible to money laundering risk and have been exploited by money launderers, with and without the accountant's knowledge of the illicit operations or objectives. Money launderers increasingly rely on the advice or services of specialized professionals to help facilitate their financial operations. Accountants have specific skills and expertise and can provide specialized services, advice and access to industry insiders.

Accountants provide a wide range of services that are most useful to potential money launderers. These services include:

- buying and selling real estate
- management of client money, securities or other assets
- management of bank, savings or securities accounts
- organization of contributions for the creating, operation or management of companies
- creation, operation or management of legal person or arrangements, and buying and selling of business entities

According to the *Global Money Laundering and Terrorist Financing Threat Assessment* published by the FATF in 2010, the most significant cases involved sophisticated schemes that were only possible with the assistance of skilled professionals that were able to set up corporate structures to disguise the source and ownership of the money.

3.3.2.2 Requirement for a Risk Assessment

Accountants and Accounting Firms are obligated to include in their Compliance Regimes the conduct and documentation of a money laundering and terrorist financing risk assessment, and to adopt measures which mitigate identified risks.

Risk assessment requirements are prescribed at subsection 9.6(2) of the PCMLTFA, and paragraph 71(1)(c) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* (PCMLTFR). Those provisions require that Accountants and Accounting Firms assess and document the risk (likelihood and significance) of money laundering or terrorist financing activity occurring in the course of their activities. It must take into account the organization's:

1. clients and business relationships
2. products and delivery channels
3. geographic location of activities
4. other relevant factors

Neither the FATF nor FINTRAC advocate a particular method or format for risk assessments, but expect that the risk-based approach will lead to greater diversity in practice which can lead to innovation and improved compliance.

The PCMLTFA at subsection 9.6(3) and the PCMLTFR at section 71.1 require that prescribed special measures be taken for higher risk activities, including policies and procedures for periodic client identification updates, ongoing monitoring for the purpose of detecting suspicious transactions, and others that mitigate identified risks.

Ultimately, risk assessments should lead to controls designed to make it more difficult for criminal elements to use Accountants and Accounting Firms to launder their illicit proceeds.

3.3.2.3 Risk Assessment Process

The risk assessment process is a consultative process throughout the organization which allows for a thorough understanding of the business structure along with all areas of risk. The first step in the risk assessment process is identifying where within your organization Triggering Activities are being

conducted and classifying those activities into the correct category. For instance, the business consulting team at an Accounting Firm may purchase and sell businesses on behalf of their clients. To determine what activities are being conducted can involve interviews with partners or service line leads to obtain an adequate understanding of the business to determine if Qualifying Activities are being conducted or could be conducted in the future. A questionnaire can be used if the organization is large with offices across the country. Once it has been determined where the activities are being conducted and which specific ones they are, a risk rating can be completed on each specific Qualifying Activity.

FINTRAC guidance provides assistance with the risk rating process and allows for objective classification using established criteria. For instance, services that allow for client anonymity are recommended to be rated as high risk services. This criterion can be applied to Triggering Activities because it is not a requirement to identify a client unless they have provided funds of \$3,000 and above, conducted a large cash transaction or conducted/attempted a suspicious transaction. Therefore, any Triggering Activity that does not involve a trigger for ascertaining identification may be classified as high risk. This example is meant as a guide and, in practice, many other factors can be considered in the risk rating process of all products and services.

Regardless of the risk rating, it is important to provide rationale for the rating and to ensure that the reasons provided are reasonable. The level of risk associated to each Triggering Activity will determine if any additional enhanced due diligence needs to be taken. For activities deemed to be low or medium risk, it is not a requirement to have enhanced due diligence measures, but if the risk of the activity is high, enhanced due diligence measures are mandatory. In the example above, if the transaction is conducted without requiring identification and it is deemed high risk, additional enhanced due diligence measures should be documented and conducted.

3.3.2.4 Risk Assessment

The Compliance Regime is to include a documented risk assessment of the risk of money laundering and the terrorist financing offence. The risk assessment involves assessing and documenting the risks, taking into consideration the following risk categories:

3.3.2.4.1 Clients and business relationships

This factor should fully explain all clients that you are dealing with and it should consider the nature of the relationship with the clients. It is about understanding your clients and the types of activities and transactions that

they normally conduct. The nature of the relationships should consider things such as the length of the relationship and how the client was acquired or introduced. Certain client industries are considered a higher risk of money laundering and/or terrorist financing such as cash-intensive businesses, and these elements should be considered within the risk of each client. For instance, the risk level of a client with a convoluted legal structure based in a known client offshore secrecy jurisdiction would, all else being equal, be a higher risk client than an individual client engaged in a personal tax return service. It is recommended that a list of low, medium and high risk business types be created that can be used objectively for all future clients. The same process is recommended for occupation types.

3.3.2.4.2 *Products and delivery channels*

Elements to consider within this factor include itemizing all products and services that are offered and assessing the risk of money laundering and/or terrorist financing associated with each specific product and service. For instance, the risk associated with a short tax engagement may be lower than the risk of an extensive investment advisory engagement spanning several years. The delivery channels through which products and services are offered also need to be analyzed within this risk factor. Specifically, you need to consider how the products and services are actually delivered to your clients. For instance, are all clients serviced through face-to-face meetings or are there any offerings available through non-face-to-face methods. The risk of having non-face-to-face delivery methods would, all else being equal, be higher than face-to-face as the ability to disguise identification becomes easier with the increase in distance between the service/product supplier and the client. It is recommended that a list of all products and services be created along with their associated risk. Any products or services that are determined to be a high risk of money laundering and/or terrorist financing would require your organization to document enhanced due diligence measures when those products or services are offered.

3.3.2.4.3 *Geographic location of the activities*

It is important to consider the geographic locations in which your organization operates in addition to the geographic location of your clients. Specific to area of operations, the level of detail may be as high-level as a breakdown by province or as granular as an office-by-office risk assessment. The crime level and prevalence of specific criminal activities are elements to consider when completing the assessment of geographic risk of your operations. As well, the same framework will guide your organization in assessing the geographic

location of your clients. However, the geographic location of the client may be included in their specific risk assessment. It is recommended that a risk scoring be done on all office locations to rank them according to risk.

3.3.2.4.4 Any other relevant factor

Within this “catch-all” remaining factor, things to consider include all elements outside of the first three factors. For instance, what is the level of turnover within your organization? Is there a restriction placed on staff members before they successfully complete AML training? The risk of money laundering and/or terrorist financing will increase for these elements if the turnover is high and there are no restrictions to staff responsibilities prior to completing training. It is recommended that for staff working in areas more prone to money laundering and/or terrorist financing risks, restrictions or oversight be placed upon their day-to-day activities until such a time as their training has been successfully completed.

3.3.2.4.5 Risk Mitigation

The purpose of the risk assessment is to apply a risk-based approach where resources are appropriately allocated to address high risk areas. The risk assessment should also include risk mitigation measures. This means that where you have identified areas of high risk, you have to take special measures to mitigate the risks to a level to which you are comfortable.

The AML Legislation prescribes special measures that are to be applied for identified areas of high risk, also known as enhanced due diligence measures. These measures can be specific to the prescribed factor or can be applied directly to the clients if they are deemed high risk.

3.3.3 Enhanced Due Diligence and Ongoing Monitoring

Where a client conducts a transaction that requires you to identify them, there are specific AML obligations that require you to conduct ongoing monitoring. Where you have identified a client to be high risk, you must also conduct enhanced due diligence measures to mitigate those risks.

Where you have identified the client to be high risk based on your ongoing monitoring, you must apply enhanced due diligence measures to mitigate the risk. The AML Legislation prescribes specific enhanced due diligence measures that are to be applied where there are high risk clients. This includes applying the following:

- Taking enhanced measures to ascertain client identification that are in addition to the standard client identification requirements.

- Taking any other enhanced measures to mitigate the identified risks including:
 - keeping client identification information and beneficial ownership information up-to-date
 - enhanced ongoing monitoring of business relationships for the purpose of detecting suspicious transactions to be reported to FINTRAC

Enhanced Due Diligence—Client Specific

The following enhanced due diligence measures can be utilized for high risk clients:

- Requiring that only an acceptable **photo** identification be accepted when required to ascertain the client's identification.
- Requiring a second piece of identification when required to ascertain the client's identification.
- Confirming the address of the client by requesting affirming documentation such as a utility bill or cable bill with a matching name.
- Confirming the occupation by requesting affirming documentation such as an employment letter or recent pay stub to confirm the current occupation.
- When dealing with an entity:
 - requiring that a status of corporation be provided instead of articles of incorporation to ensure the corporation is still active
 - ascertaining the identification of all directors or authorized signers of the entity
 - confirming the entity's operations by conducting a physical drive-by of the premises
 - asking for beneficial ownership information on all clients
- Reviewing the client's activity on a pre-determined frequency, such as every six months or annually, for any suspicious transactions.
- Internet searches for any negative news matches on individual clients or directors/signing officers from an entity client.
- Checking names against a reputable names list such as World-Check for potential Politically Exposed Foreign Persons (PEFP) upon the creation of an engagement.
- Extending the PEFP determination to include any domestic positions.

Enhanced Due Diligence—Products, Services, Delivery Channels, Geographical

The following enhanced due diligence measures can be utilized for high risk factors:

- For geographical areas ranked high risk, require secondary approval of all transactions.
- Prohibiting certain transactions if the client is domiciled in a high risk geographical area.
- Requesting source of funds/source of wealth documentation for clients in high risk areas.
- Requesting additional identification when offering products or services deemed high risk.

Ultimately the enhanced due diligence taken is a measure that goes above and beyond what is required for regular transactions to satisfy standard legislative requirements. It should be noted that a combination of measures may be used depending on the specific situation and when warranted.

3.3.4 Policies and Procedures

Accountants and Accounting Firms are required to have written and up-to-date compliance policies and procedures in support of the Compliance Regime. The compliance policies and procedures should document applicable legislative requirements and the organization's procedures to satisfy those requirements. Procedures should also include those that were developed as part of the risk-based approach program.

The compliance policies and procedures should be approved by a Senior Officer and kept up to date, taking into consideration:

- changes to AML legislative requirements
- changes to internal processes and procedures
- changes in products and services that have an effect on AML requirements (for example, new services that will trigger a qualifying activity)
- changes in organizational structures that could affect reporting procedures

3.3.4.1 Minimum Policies

Considering the parameters and organization of AML Legislation in respect to Accountants and Accounting Firms, we would expect that, at a minimum, the policies listed below would form part of their compliance program. In the immediately following section, we have listed expected headers in a set of policies and procedures for an Accountant or Accounting Firm.

3.3.4.1.1 General Policies

- “We will identify all Qualifying Activities as they occur within our organization.”
- Definitions of Qualifying Activities along with explanations of where within the organization such activities are being conducted.

3.3.4.1.2 Reporting

- “All large cash transactions will be reported to FINTRAC within 15 calendar days of receipt whether received at one time or within 24 hours.”
- “All suspicious transactions, whether completed or attempted, will be reported to FINTRAC within 30 days of suspicion.”
- A listing of all suspicious transaction indicators which will lead to reporting.
- “Any terrorist property will be reported to FINTRAC immediately upon knowing.”

3.3.4.1.3 Record Keeping

- “All required records will be documented and stored for at least five years.”
- “All records will be stored in such a way that allows for their retrieval within 30 days of notice by FINTRAC.”
- “A receipt of funds record will be kept for every transaction where we accept \$3,000 or more from a client.”
- “A large cash transaction record will be kept for every transaction where we accept \$10,000 or more in cash from a client, whether at one time or within 24 hours.”
- “Copies of official corporate records will be kept for all transactions that require the confirmation of the existence of a corporation.”
- “All suspicious transaction reports will be stored on file.”

3.3.4.1.4 Ascertaining Identification

- “When a large cash transaction is conducted, the identity of the conductor will be ascertained.”
- “All clients who are the subject of suspicious transactions will have their identification ascertained except when doing so would tip off the client that a suspicious report is being sent to FINTRAC.”
- “When a receipt of funds record is created, the client’s identification will be ascertained and if the individual is acting on behalf of an entity, the entity’s existence will also be confirmed.”

3.3.4.1.5 *Third Party Determination*

- “For every large cash transaction, a third party determination will be made and if there is a third party connected to the transaction, a record will be kept documenting their details.”

3.3.4.2 *Sample List of Policies and Procedure Headings*

Policies and Procedures need to include all legislative requirements under the PCMLTFA and be specific to your organization. The factors below can be used to determine the framework of a complete set of Policies and Procedures.

- Policy Statement
 - *Objective*—explains the objective of the policy.
 - *Responsibility*—explains who is responsible for the compliance program.
 - *Background* (including relevant legislative requirements and guidance)—provides a summary of legislation that is applicable to the document.
 - *Policy application*—explains to whom the policies are applicable.
- Procedures
 - *Responsibilities*—explanation of all accountable parties.
 - *Appointment of Compliance Officer*—statement explaining how the appointment is made and who is the current compliance officer.
 - *Procedure Application*—explains to whom the procedures are applicable.
 - *Foreign Currency Translation*—explanation of how transactions in a foreign currency will be treated.
- Compliance Operations
 - *Identifying Triggering Activities*—explanation of how these activities will be found in the organization.
 - *Receipt of funds of \$3,000 or more*—explains the record keeping and ascertaining identification steps taken when these occur.
 - *Receipt of cash of \$10,000 or more*—explains the record keeping, ascertaining identification and reporting steps taken when these occur.
 - *Completed and Attempted Suspicious Transactions*—explains how these transactions are initially detected and the measures taken when they are detected.

- *Terrorist Property Reports*—explains the process for determining if property is held and the steps taken when a positive match is found.
- *Business Relationship Establishment and Ongoing Monitoring*—explains the concept and what measures are taken to satisfy the requirements.
- *Enhanced Due Diligence*—establishes the measures taken and when they would be applicable.
- Risk-Based Approach
 - *Responsibility and Application*—explains who is accountable for this and how it applies.
 - *Risk Assessment*—includes the four prescribed factors and classifies all areas into a specific risk category.
 - *Risk Mitigation*—explains the enhanced due diligence measures taken for areas deemed to be high risk.
- Training Program
 - *Responsibility and Application*—explains who this applies to and the person/team accountable for this program.
 - *Program Content*—summarizes the training material.
- Effectiveness Review
 - *Responsibility and Application*—explains who is accountable for this program component.
 - *Requirements*—explains the methodology and frequency that will apply.

3.3.5 Ongoing Training Program

If you have employees, agents or other persons authorized to act on the company's behalf, you must develop and maintain a written ongoing compliance training program for those employees, agents or persons.

3.3.5.1 Who Must Take the AML Training?

- Anyone who interacts with clients.
- Anyone who sees client transaction activities.
- Anyone who handles cash or funds in any way.
- Anyone who is responsible for implementing or overseeing the Compliance Regime.

3.3.5.2 What Should Be Included in the Ongoing Training Program?

The ongoing compliance training program is required to be in writing. Although the AML Legislation does not state what specifically is to be included in the written training program, there are certain expectations of what the ongoing training program should cover. Below are sample headings to include in the ongoing training program:

- content of training material
- how training is to be delivered
- frequency of training
- how training is to be tracked and documented
- who is to receive training
- new hire training and any restrictions on their responsibilities prior to completion of training
- how to address individuals that were not present for training

The actual content of the training program should focus on the areas of greatest importance, and would ideally be role-specific. In an Accounting Firm, the most important concept to teach all staff members is the definition of a Triggering Activity and how to recognize one when it occurs. This key piece of information is a prerequisite to all requirements that come as a result of the Triggering Activity being conducted and should be understood by all staff at your organization. The various indicators of suspicious transactions should be taught to all staff as well. Staff members are the first line of defense in regards to flagging suspicious transactions to the compliance team and being aware of what types of transactions to flag will go a long way in the goal of having an effective Compliance Regime. Finally, the training material should also include a step-by-step process for all staff upon receiving funds for an engagement that includes Triggering Activities. These three areas are a must for all staff to understand and should be expanded on depending on the specific role that the staff member has at your organization.

3.3.5.3 Sample Training Schedule

A training schedule shows that you have ongoing training in place. It also provides a summary of your ongoing training program that can be used to manage internal resources when it comes to training. The training schedule should align with your ongoing training program and indicate who is to receive training and when training is to roll out. It is important to ensure that the material provided to staff is in context to their role within the organization. The following is a sample training schedule. It is recommended that the date of each training effort be documented.

Type of Staff	Identifying Triggering Activities	Ascertaining Identification and Record Keeping	Money Laundering Methods and Detection	Reporting Transactions	FINTRAC Exam Process
Leadership	Annual		Annual		
Compliance Administrators	Annual	Annual	Annual	Annual	Annual
Professional Staff	Annual	Bi-Annual	Annual	Bi-Annual	
Administrators	Annual	Annual	Annual	Annual	

3.3.6 Effectiveness Review

Accountants and Accounting Firms are required to have an effectiveness review done every two years. The review can be conducted by your internal or external auditor or by you or the firm if you do not have an auditor.

Important Note: The effectiveness review should be reported to a Senior Officer within 30 days after the assessment and is to include:

- *The findings of the review.*
- *Any updates made to the policies and procedures based on the assessment.*
- *The status of the implementation of the updates that were made to those policies and procedures.*

3.3.6.1 What Does the Effectiveness Review Cover?

The effectiveness review is a documented review of the effectiveness of the following areas of the Compliance Regime:

- policies and procedures
- risk assessment
- training program

The review must be documented into a report that includes information about the methodology that was used to conduct the review; the scope of the review; what was reviewed; and the findings. When testing the effectiveness of each specific Compliance Regime element above, there are several factors to consider.

Within the Policies and Procedures, testing the effectiveness should include:

- Checking for the presence of all legislative requirements within the document and that they include a policy statement.
- Checking for the presence of specific procedures that satisfy each policy statement.
- Verifying that the procedures are actually being adhered to by staff on a consistent basis throughout the organization.
- Reviewing documentation such as client information records and transaction records to test the procedures.
- Reviewing reported transactions such as LCTRs and STRs to verify the timing and quality component.

The Risk Assessment can be tested in a similar method except the verification process would be tailored with different documentation reviews:

- Checking for the presence of all four prescribed factors within the risk assessment documentation.
- Checking for the presence of inherently low, medium and high risk factors and analyzing whether the risk rankings are current and accurate to the organization.
- Checking for the presence of policy statements related to the risk-based approach specific to high risk areas that require mitigation measures.
- Testing high risk areas through a review of client information and transactions to verify whether the risk mitigation measures have been followed.
- Reviewing reported STRs and any transactions flagged as unusual to verify the process specific to high risk clients.

The Training Program is tested for effectiveness through several measures including:

- Comparing the training material against the specific recipient role within the organization to test the applicability.
- Testing whether all applicable staff are receiving training and whether any gaps exist through a comparison of current and past employees against a training tracking sheet.
- Reviewing any testing materials in place to ensure that appropriate questioning is being used.
- Checking staff quiz/test scores to test the process of adequate retention of material.
- Interviewing staff to test their understanding and retention of training material along with the practical applicability of the material specific to their role.

3.3.6.2 *Sample Scope*

The effectiveness review should include the scope of the review that takes into account the required component of the Compliance Regime. Below is a sample scope that can be used to ensure that all components are being covered in the effectiveness review:

Required Components	Scope	Items to Test
Policies and Procedures	Document Evaluation	AML Policies and Procedures
	Operational Evaluation	Client identification records FINTRAC reports Receipt of funds records
Risk Assessment	Document Evaluation	Risk assessment document <ul style="list-style-type: none"> • Procedures/methodology of risk assessment • Procedures on enhanced due diligence for high risk clients • Documented risk assessment of organization
	Operational Evaluation	High risk clients Application of enhanced due diligence Monitoring processes
Training Program	Document Evaluation	Ongoing training program Training materials
	Operational Evaluation	Training log Interviews with staff to test knowledge of AML

Included in Appendix N—Self-Review Checklist is a checklist against which an Accountant or Accounting Firm can evaluate their progress towards an effective compliance program.

CHAPTER 4

AML and Privacy Obligations

In Canada, Accountants and Accounting Firms have both AML and privacy obligations. One of the privacy principles is to “minimize collection.” This means Accountants and Accounting Firms must only collect personal information that you need.

The AML Legislation requires certain information to be collected by reporting entities and prescribes certain measures for “Know Your Client” (KYC) and “Customer Due Diligence” (CDD). These measures align with privacy principles as the information that is required is for KYC purposes.

4.1 Summary of KYC/CDD Requirements

KYC/CDD Requirements	Not Required for KYC/CDD
<ul style="list-style-type: none"> • Identification information (type of identification document, identification reference number, place of issue) • Occupation information • Date of birth • Address 	<ul style="list-style-type: none"> • Copy of the identification document • The inclusion of your client’s Social Insurance Number in a report to FINTRAC

4.2 Where AML and Privacy Get Complicated

The AML legislation requires that reporting entities apply a risk-based approach. This means that resources are allocated to areas of high risk in order to mitigate the risks. Based on the risk assessment that is required to be conducted and documented by all reporting entities, clients that have been identified as a high risk for money laundering or a terrorist financing offence should be subjected to enhanced due diligence (EDD) measures. However, the AML Legislation is not prescriptive when it comes to defining EDD measures.

4.3 What Does the AML Legislation Say About EDD Measures?

The AML Legislation requires enhanced measures be applied and prescribes certain measures that should be included as part of EDD. The Legislation also states that “any other enhanced measures” are to be applied to mitigate the risks. This allows reporting entities to apply their own controls, on top of the prescribed EDD.

4.4 What Is Required for EDD Measures?

When applying “other enhanced measures” for high risk clients, it is important that these measures be defined in the compliance policies and procedures and that these measures are clearly articulated with documented reasoning for collecting additional information.

4.5 What Information Should Be Documented?

1. Rationale—For collecting information that is in addition to the standard request.
2. Process—What information is to be collected for EDD, when EDD is to be applied, and when and how information is to be collected.

The Privacy Commissioner of Canada has issued two publications about privacy obligations and the PCMLTFA, a guide for point of service workers (www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp), and a questions and answers page (www.priv.gc.ca/information/pub/faqs_pcmltfa_01_e.asp#001).

Important Notes: Remember that it is acceptable to let the client know that the information that you are asking for is required under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, unless disclosing this would tip off the client about a completed or attempted suspicious transaction report.

CHAPTER 5

Interactions with Other Reporting Entities

There are several things to keep in mind when you are dealing with other reporting entities. All reporting entities, as defined in the AML Legislation, have specific AML obligations that are unique to their type of entity, as with Accountants and Accounting Firms. In the course of your interactions with other financial entities, when you are conducting services on behalf of your clients, you may be called upon to provide other information based on the activities of your clients.

Be aware that AML obligations require that reporting entities are adequately identifying their clients, understanding their clients' activities and are applying a risk based approach to their clients' activities. Information that may be requested will have to do with complying with these obligations.

CHAPTER 6

FINTRAC Examinations

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit. It is an independent agency that was established to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). The PCMLTFA allows FINTRAC to conduct examinations on reporting entities.

The exam involves a review of records and inquiries into the business for the purpose of ensuring compliance with the AML Legislation.

6.1 FINTRAC's Powers

FINTRAC examinations are legislated under section 62(1) of the PCMLTFA. It specifically states that "An authorized person may, from time to time, examine the records and inquire into the business and affairs of any person or entity referred to in section 5 for the purposes of ensuring compliance with Part 1..."

This power includes allowing an authorized person to enter any premises where there are records related to the business and access any computer system to examine any data and to reproduce those records. Authorized persons would be FINTRAC Compliance Officers who have been authorized by the Director to ensuring compliance under the legislation. In section 62(2) of the PCMLTFA, it explicitly states that reasonable assistance shall be given to authorized persons.

6.2 How to Prepare

FINTRAC may select you or your firm to conduct a compliance exam. These exams are to ensure that you are complying with the PCMLTFA and its enacted Regulations. When you receive confirmation from FINTRAC that

they will be conducting an exam, there are a few points to keep in mind. The FINTRAC Compliance Officer will call and explain the process after notification of a compliance examination. A notification letter will be received shortly after the initial conversation outlining what documentation FINTRAC will require. Before receiving the letter, it is suggested that all compliance documentation be assembled and a review of past FINTRAC interactions be completed. The logistics of the examination should be finalized to ensure all documentation is assembled as quickly as possible and that sufficient staff is available to answer any regulator questions. A room should be set aside for FINTRAC staff if they are coming to the premises and a photocopier should be made available for their use. Here are some additional things to keep in mind if you are having a FINTRAC compliance examination:

- Be aware of the deadlines that are noted in the letter from FINTRAC.
- If uncertain of any process, do not hesitate to call the FINTRAC Officer conducting the exam.
- Provide all documents and transactions that are listed in the letter from FINTRAC.
- Answer all questions calmly and honestly. Have resources available on hand during the exam.

6.3 What to Expect

The following list provides a summary of the exam process that you can expect during the exam.

1. Notification of Exam: You will receive a call from FINTRAC notifying that they will be conducting a compliance exam. The call may include questions regarding your “Triggering Activities.”
2. Information Request: Following the call, FINTRAC will send a letter requesting specific information.

Important Note: You have 30 days from the date of the letter to provide all the information to FINTRAC.

3. Date of Exam: The letter will also indicate the date when they will be conducting the exam. This can be either via conference call or on-site.

4. Exam: During the exam, FINTRAC will be asking the Compliance Officer specific questions. These questions can range from the following about your organization:
 - general business information
 - compliance regime
 - AML policies and procedures
 - risk assessment
 - ongoing training program
 - effectiveness compliance review
 - receipt of funds transactions
5. Exit Interview: At the end of the exam, FINTRAC will summarize deficiencies that were noted from the exam. They will also mention that a letter summarizing the deficiencies will be sent to you. Any questions stemming from deficiencies should be asked at this time including obtaining suggestions on how best to remedy all deficiencies.

6.4 Follow Up

After FINTRAC's exam, you should expect to receive a letter from FINTRAC summarizing all deficiencies found during the exam. The language of the letter will clearly communicate the expectations that FINTRAC has from you in addition to any further actions being considered by FINTRAC. An action plan should be developed and implemented internally to rectify all deficiencies in a timely manner. At a later date, FINTRAC may decide to conduct a follow-up exam to ensure that you have addressed the deficiencies and have implemented your action plan. Therefore, it is important that you follow your action plan and that you document what has been done to address those deficiencies.

The consequences of non-compliance vary from minor such as the issuance of a findings letter asking for continued cooperation to the severe with the issuance of a monetary penalty and a public naming summarizing all areas of non-compliance. The penalty amounts can be quite severe and it is not uncommon to see penalties in the six figure range. When egregious non-compliance has been observed by FINTRAC, the findings letter will explicitly state that administrative monetary penalties (AMPs) are being considered. Regardless of the decision, FINTRAC will send additional correspondence notifying your organization of their final decision. Should no AMP be pursued, the letter will state that fact explicitly. However if, FINTRAC decides to pursue an AMP based on its analysis, a notice of violation will be issued to your organization.

If a notice of violation is received, your organization has several options available. Paying the penalty would close the proceedings and result in an admission of all violations from the non-compliance, and give FINTRAC the right to publically report the penalty in most cases. Another option is to appeal the penalty directly with FINTRAC's Director by providing explanations or arguments for any or all violations cited. This involves a secondary review of all violations to determine if any of the reasons within the appeal are reasonable. However, the request for a review must be in writing and submitted within 30 days of receiving the notice of violation. If this appeal is unsuccessful, a second appeal can be made to the Federal Court. It is prudent to obtain legal advice and professional AML assistance to help manage responses and appeals.

Important Note: Always document your progress. Documentation is important when it comes to showing FINTRAC that you are complying with the AML Legislation and that you have addressed those deficiencies as stated in your action plan letter to FINTRAC.

6.5 Compliance Assessment Report

All reporting entities, including Accountants and Accounting Firms, may be asked by FINTRAC to complete a compliance assessment report (CAR). The CAR is essentially a questionnaire which attempts to obtain a high level overview of your organization's operations and if applicable, current level of compliance. The first section of the questionnaire will ask questions related to your scale of operations including financial information. The next section will ask questions regarding Qualifying Activities to determine whether your organization is subject to the PCMLTFA. If the response to the Qualifying Activities questions is positive, the remainder of the questionnaire will be specific to your legislative obligations and whether a Compliance Regime has been developed and implemented. It is important to answer these questions truthfully as FINTRAC relies on this to populate their understanding of your organization and may contact your organization in the future to verify any information. If any part of the CAR is not fully understood, it is recommended that your organization contacts FINTRAC for clarification.

CHAPTER 7

Appendix A — Canada's AML Legislation

7.1 Provenance

Canada is a founding member of the Financial Action Task Force (FATF), the international standard setting body for anti-money laundering and anti-terrorist financing activities. The objective of the FATF is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

As a member of the FATF, Canada has made a political commitment to implement the FATF Recommendations that includes implementing measures to ensure that the financial institutions and intermediaries are adequately able to identify their customers; to understand their activities; and to conduct ongoing scrutiny of customers' activities.

The PCMLTFA and its enacted Regulations sets out Canada's AML regime whereby designated financial and non-financial entities that provide access to Canada's financial system are obligated to comply with these standards.

7.2 Purpose

The objective of the PCMLTFA is to implement specific measures to detect and deter money laundering and the financing of terrorist activities and to facilitate the investigation and prosecution of money laundering offences and terrorist activity financing offences.

Canada's AML regime was developed to respond to the threat posed by organized crime by providing law enforcement officials with the resources they need and to assist Canada in fulfilling its international commitment in protecting the integrity of the international financial system.

7.3 Players

There are a wide range of players that are part of Canada's AML regime. They range from individuals to entities and from federal departments to international entities. Below is summary of the players:

<p>Who has reporting requirements to FINTRAC?</p>	<p>Reporting Entities:</p> <ul style="list-style-type: none"> • financial institutions • life insurance companies and life insurance brokers or agents • legal counsel and legal firms • securities dealers • money service businesses • Accountants and Accounting Firms • British Columbia notaries • real estate brokers, sales representatives and developers • dealers in precious metals and stones • casinos <p>Entities that may also report:</p> <ul style="list-style-type: none"> • public • federal agencies (e.g. Canada Border Services Agency, Canada Revenue Agency, Canadian Security Intelligence Service) • foreign financial intelligence units
<p>What is FINTRAC?</p>	<p>All reporting entities have reporting requirements to FINTRAC.</p> <p>FINTRAC is Canada's financial intelligence unit and is responsible for the overall supervision of reporting entities to determine compliance with Canada's AML regime.</p> <p>FINTRAC reports to the Department of Finance and is overseen by the following departments:</p> <ul style="list-style-type: none"> • Office of the Privacy Commissioner of Canada • Office of the Auditor General of Canada

Who does FINTRAC share information with?	<p>FINTRAC may disclose information if it has reasonable grounds to suspect that the information would be relevant to an investigation or prosecution of a money laundering or terrorist activity financing offence, or relevant to threats to the security of Canada.</p> <p>The following is a list of agencies FINTRAC may disclose information to:</p> <ul style="list-style-type: none"> • law enforcement • Canadian Security Intelligence Service • Canada Revenue Agency • Canada Border Services Agency • foreign financial intelligence units
--	--

7.4 Penalties and Criminal Fines for Non-Compliance

FINTRAC has legislative authority to issue criminal and administrative penalties against the entity and other persons where non-compliance has been identified.

Administrative Monetary Penalty (AMPs)

AMPs allow for a measured and proportionate response to particular instances of non-compliance. Violations are classified as follows:

Classification	Penalty
Minor	Carries maximum penalties up to \$1,000
Serious	Carries maximum penalties up to \$100,000
Very Serious	Carries maximum penalties up to \$500,000

Penalties are determined in relation to the degree at which the violation obstructs the ability to detect and deter money laundering and terrorist activities.

Criminal Penalties

FINTRAC may disclose cases of non-compliance to law enforcement when there is excessive non-compliance or little expectation of immediate or future compliance. Criminal penalties include:

- Failure to report suspicious transactions: up to \$2 million and/or five years imprisonment.
- Failure to report a large cash transaction: up to \$500,000 for the first offence, and \$1 million for subsequent offences.
- Failure to meet record keeping requirements: up to \$500,000 and/or five years imprisonment.

- Failure to provide assistance or provide information during compliance investigation: up to \$500,000 and/or five years imprisonment.
- Disclosing a fact that a suspicious transaction report was made, or disclosing contents or the report, with the intent to prejudice a criminal investigation: up to two years imprisonment.

CHAPTER 8

Appendix B— Links to FINTRAC Guidance⁵⁰

FINTRAC Guidelines for the accounting sector are divided into separate sections specific to the subject matter. The following Guidelines are applicable to Accountants and Accounting Firms:

Guideline 1—Backgrounder:

www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp

Guideline 2—Suspicious Transactions:

www.fintrac-canafe.gc.ca/publications/guide/Guide2/2-eng.asp

Guideline 3A—Submitting Suspicious Transaction Reports to FINTRAC Electronically:

www.fintrac-canafe.gc.ca/publications/guide/Guide3A/str-eng.asp

Guideline 3B—Submitting Suspicious Transaction Reports to FINTRAC by Paper:

www.fintrac-canafe.gc.ca/publications/guide/Guide3B/3b-eng.asp

Guideline 4—Implementation of a Compliance Regime:

www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp

Guideline 5—Submitting Terrorist Property Reports:

www.fintrac-canafe.gc.ca/publications/guide/Guide5/5-eng.asp

Guideline 6—Record Keeping and Client Identification:

www.fintrac-canafe.gc.ca/publications/guide/Guide6/6-eng.asp

⁵⁰ Please note that the information on FINTRAC's website is subject to change and is not intended to replace the PCMLTFA and associated Regulations.

Guideline 7A — Submitting Large Cash Transaction Reports to FINTRAC Electronically:
www.fintrac-canafe.gc.ca/publications/guide/Guide7A/lctr-eng.asp

Guideline 7B — Submitting Large Cash Transaction Reports to FINTRAC by Paper:
www.fintrac-canafe.gc.ca/publications/guide/Guide7B/7b-eng.asp

Please note that the Guidelines are periodically updated to reflect any changes in the legislation or any significant guidance that FINTRAC issues.

CHAPTER 9

Appendix C— Summary of Changes Effective February 1, 2014

Regulatory amendments known as SOR/2013-15 were published on January 31, 2013 in the *Canada Gazette* (<http://gazette.gc.ca/rp-pr/p2/2013/2013-02-13/html/sor-dors15-eng.html>) with an effective date of February 1, 2014. They have created new requirements for Accountants and Accounting Firms which have been incorporated into this guidance that include:

1. The requirement to recognize the establishment of a “business relationship” with clients for which a first Triggering Activity is performed following the effective date of the amendments, and to document the “purpose and intended nature of the business relationship.”
2. The requirement to conduct and document “ongoing monitoring” measures in respect of all business relationships established following the effective date of the amendments for the purpose of:
 - Detecting reportable transactions.
 - Keeping client identification up-to-date.
 - Re-assessing the level of risk associated with the client’s transactions and activities.
 - Determining if the transactions and activities are consistent with the information received from the client (including the “purpose and intended nature of the business relationship”).

CHAPTER 10**Appendix D —
FATF RBA Guidance for Legal
Professionals**



Financial Action Task Force
Groupe d'action financière

RBA GUIDANCE FOR LEGAL PROFESSIONALS

23 October 2008

© FATF/OECD 2008

All rights reserved. No reproduction, copy, transmission or translation of this publication may be made without written permission.

**Applications for permission to reproduce all or part of this publication should be made to:
FATF Secretariat, OECD, 2 rue André Pascal 75775 Paris Cedex 16, France**

TABLE OF CONTENTS

SECTION ONE: USING THE GUIDANCE PURPOSE OF THE RISK-BASED APPROACH	4
Chapter One: Background and Context	4
Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges	8
Chapter Three: FATF and the Risk-Based Approach.....	11
SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES	15
Chapter One: High-level principles for creating a risk-based approach.....	15
Chapter Two: Implementation of the Risk-Based Approach.....	19
SECTION THREE: GUIDANCE FOR LEGAL PROFESSIONALS ON IMPLEMENTING A RISK-BASED APPROACH.....	25
Chapter One: Risk Categories.....	25
Chapter Two: Application of a Risk-Based Approach	31
Chapter Three: Internal Controls	34
ANNEXES	36
ANNEX 1.....	36
A. Financial Action Task Force Documents	36
B. Legislation/and Court Decisions	36
C. Links to Information on the Supervisory Program in Certain Countries	36
D. Guidance on the Risk-based Approach	37
E. Other sources of information to help assist countries’ and legal professionals’ risk assessment of countries and cross-border activities.....	37
ANNEX 2.....	39
ANNEX 3.....	41

SECTION ONE: USING THE GUIDANCE

PURPOSE OF THE RISK-BASED APPROACH

Chapter One: Background and Context

1. In June 2007, the FATF adopted Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures, which includes guidance for public authorities and guidance for financial institutions. This was the culmination of extensive consultation between private and public sector members of an Electronic Advisory Group (EAG) established by the FATF.

2. In addition to financial institutions, the FATF Recommendations also cover a number of designated non-financial businesses and professions (DNFBPs). At its June 2007 meeting, the FATF's Working Group on Evaluation and Implementation (WGEI) endorsed a proposal to convene a meeting of the representatives from the DNFBPs to assess the possibility of developing Guidance on the risk-based approach for their sectors, using the same structure and style as the completed Guidance for financial institutions.

3. This meeting was held in September 2007 and was attended by members of organisations which represent lawyers, notaries, trust and company service providers (TCSPs), accountants, casinos, real estate agents and dealers in precious metals and dealers in precious stones. This private sector group expressed an interest in contributing to FATF Guidance on implementing a risk-based approach for their sectors. The Guidance for the DNFBPs would follow the principles of the risk-based approach already established by FATF, and would highlight risk factors specific to the DNFBPs, as well as suggest mitigation strategies that fit with the particular activities and businesses of the DNFBPs. The FATF established another EAG to facilitate the work.

4. The private sector group met again in December 2007 and was joined by a number of specialist public sector members. Separate working groups comprising public and private sectors members were established, and private sector chairs were appointed.

5. The EAG continued work until this Guidance for legal professionals was presented to the WGEI. After further international consultation with both public and private sectors, the FATF adopted this Guidance at its October 2008 Plenary. Guidance for each of the other DNFBP sectors is being published separately.

Purpose of the Guidance

6. The purpose of this Guidance is to:
- Support the development of a common understanding of what the risk-based approach involves.
 - Outline the high-level principles involved in applying the risk-based approach.
 - Indicate good practice in the design and implementation of an effective risk-based approach.

7. However, it should be noted that applying a risk-based approach is not mandatory. A properly applied risk-based approach does not necessarily mean a reduced burden, although it should result in a more cost effective use of resources. For some countries, applying a rules-based system might be more appropriate. Countries¹ will need to make their own determinations on whether to apply a risk-based approach, based on their specific money laundering/terrorist financing risks, size and nature of the DNFBP activities, and other relevant information. The issue of timing is also relevant for countries that may have applied anti-money laundering/counter-terrorist financing (AML/CFT) measures to DNFBPs, but where it is uncertain whether the DNFBPs have sufficient experience to implement and apply an effective risk-based approach.

Target Audience, Status and Content of the Guidance

8. This Guidance has been prepared for, and in relation to, legal professionals.² The legal professionals sector includes various professions, including lawyers and notaries, and in some countries there are also different categories of lawyers *e.g.* barristers and solicitors. Many legal professionals are required to comply with specific legislation and regulation and rules and regulations enacted or adopted by professional associations or other self regulatory organisations (SROs). The activities of legal professionals are very diverse, as are the legal and professional obligations with which they are required to comply. The specifics of an individual legal professional's and/or a firm or other collection of legal professionals' particular risk-based processes should accordingly be determined based on the activities undertaken by the legal professional, the ethical and existing supervisory structure for legal professionals and the susceptibility of a legal professional's activities (both generally and particularly) to money laundering and terrorist financing.

9. Legal professionals provide a range of services and activities that differ vastly, such as in their methods of delivery and in the depth and duration of the relationships formed with clients. This Guidance is written at a high level to take into account the differing practices of legal professionals in different countries, and the different levels and forms of supervision or monitoring that may apply. It is not intended as a template for national legislation imposing obligations on legal professionals or SROs. Each country and its national authorities should aim to establish an active dialogue with its legal professionals and other DNFBP sectors that will be mutually beneficial in establishing effective systems to combat money laundering and terrorist financing.

10. The following general observations about legal professionals should help inform the approach. Consideration should also be given to the particular activities performed by legal professionals on a national, provincial, or local basis. Because legal professionals typically refer to those benefiting from their services as "clients" rather than "customers", that term is thus generally used throughout this paper, except where specific terms of art such as "customer due diligence" and "know your customer" are used (in such cases a customer can be equated to a client).

11. For purposes of this Guidance, legal professionals include both lawyers and notaries.

- Lawyers are members of a regulated profession and are bound by their specific professional rules and regulations. Their work is fundamental to promoting adherence to the rule of law in the countries in which they practice. Lawyers hold a unique position in society by providing

¹ All references in the FATF Recommendations and in this document to country or countries apply equally to territories or jurisdictions.

² This refers to sole legal practitioners and partners or employed legal professionals within professional firms. It is not meant to refer to "internal" (*i.e.* in-house) professionals that are employees of other types of businesses, nor to legal professionals working for government agencies, who may already be subject to separate measures that would combat money laundering and terrorist financing. See FATF 40 Recommendations Glossary, definition of "Designated Non-Financial Businesses and Professions" (e).

access to law and justice for individuals and entities, assisting members of society to understand their increasingly complex legal rights and obligations, and assisting clients to comply with the law. Lawyers have their own professional and ethical codes of conduct by which they are regulated. Breaches of the obligations imposed upon them can result in a variety of sanctions, including disciplinary and criminal penalties. The provisions contained in this Guidance, when applied by each country, are subject to professional secrecy and legal professional privilege. As is recognised by the interpretative note to the FATF Recommendation 16, the matters that would fall under legal professional privilege or professional secrecy and that may affect any obligations with regard to money laundering and terrorist financing are determined by each country. Likewise, ethical rules that impose obligations, duties, and responsibilities on legal professionals vary by country. The legal professionals' counseling and advisory role, especially in an increasing regional and global marketplace, does not generally involve a cash handling function.

- Both civil and common law countries have notaries, but the roles of civil and common law notaries differ. Common law mainly differs from civil law in that precedents can be drawn from case law, while in civil systems codified rules are applied by judges to the cases before them. In some common law countries, the common law notary public is a qualified, experienced practitioner, trained in the drafting and execution of legal documents. In other common law countries, the notary public is a public servant appointed by a governmental body to witness the signing of important documents (such as deeds and mortgages) and administer oaths. Known only in civil law jurisdictions, civil law notaries are both members of an autonomous legal profession – although regulated by the law – and qualified public officials, as they are appointed by the State through a selective public contest among law graduates. Civil law notaries, who are bound by an obligation of impartiality with respect to both parties, must be regarded, in matters of real property (conveyancing), family law, inheritance and corporate legal services as practising non-contentious activities. They act as gatekeepers by drafting, ensuring the legality and certainty of the instruments and the authenticity of signatures presented to them; providing as well a public fiduciary function by performing the role of a trusted third party . Civil law notaries are obliged by law not to detach themselves from the core of the relationship, therefore making them responsible for all aspects of the deed. For this reason, civil law notaries are assigned functions of a public nature as part of their legal assignments. In civil law jurisdictions, notarial written documents are particular means of evidence, unlike in the common law systems, which are based on the free evidence of witnesses in court: special supreme State powers are devolved to civil law notaries and they can therefore assign “public authority” to each deed they perform. Thereby the civil law notary’s deed has a special effectiveness in a trial, whereby it is a means of peremptory binding evidence; furthermore, it is as judicially enforceable as a judgement; if it complies with the law, it can be registered on a public registry. Owing to these characteristics, civil law notaries play a different role in comparison to the services provided by other legal professionals. This Guidance does not cover those common law notaries who perform merely administrative acts such as witnessing or authenticating documents, as these acts are not specified activities.

12. Recommendation 12 mandates that the requirements for customer due diligence requirements (CDD), record-keeping, and paying attention to all complex, unusual large transactions set out in Recommendations 5, 6, and 8 to 11 apply to DNFBPs in certain circumstances. Recommendation 12 applies to legal professionals when they prepare for and carry out certain specified 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.

This Guidance has been prepared to assist legal professionals in those situations. Unless legal advice and representation consists of preparing for or carrying out transactions relating to these specified activities, it is not subject to the FATF Recommendations. The Recommendations would thus not cover, for example, an initial meeting before any preparatory work is carried out, or the usual level of advice given at legal aid or other “walk up” clinics.

13. It is possible that more than one legal professional will be preparing for or carrying out a transaction, in which case they will all need to observe the applicable CDD and record-keeping obligations. However, several legal professionals may be involved in a transaction for a specified activity but not all are preparing for or carrying out the overall transaction. In that situation, those legal professionals providing advice or services (*e.g.* a local law validity opinion) peripheral to the overall transaction who are not preparing for or carrying out the transaction may not be required to observe the applicable CDD and record-keeping obligations.

14. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions and AMLCFT controls, and Recommendation 21 regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, apply to DNFBPs subject to the certain qualifications. Specifically, Recommendation 16 applies to legal professionals when they engage in a financial transaction on behalf of a client, in relation to the activities referred to in Recommendation 12. Recommendation 16, however, provides that legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. The lawyer-client relationship is protected by law, regulations, and rules, and codes of conduct (such as legal professional privilege) in many countries, including in some countries by constitutional provisions. This is recognised by the Interpretative Note to Recommendation 16.

15. The wider audience for this Guidance includes countries, regulators, and self-regulatory organisations (SROs), which are considering how to apply AML/CFT measures to legal professionals. Countries need to identify the most appropriate regime, tailored to address individual country risks, which takes into consideration the activities and professional and ethical codes of conduct of legal professionals in their countries. This regime should recognise the differences between the DNFBP sectors, as well as the differences between the DNFBPs (particularly legal professionals) and financial institutions. However, this Guidance does not override the purview of national authorities. The manner in which legal professionals, SROs, or other supervisory bodies approach their responsibilities under a risk-based CDD system must necessarily be informed by and conform with the existing legal and oversight framework within each country’s jurisdiction.

- To the extent a country has adopted a risk-based approach regime, the legal professionals practising in that country should refer to that country’s guidance for that regime.
- This Guidance does not supplant specific professional guidance issued by designated competent authorities or SROs in a particular country, and does not constitute a legal interpretation of AML or CFT obligations of legal professionals, and should not be relied on by legal professionals or the judiciary in determining whether a legal professional has complied with his or her AML or CFT obligations.

16. The provisions in this Guidance are subject to applicable professional secrecy, legal professional privilege or rules of professional conduct, which are determined by each country.

Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges

The purpose of the Risk-Based Approach

17. The FATF Recommendations contain language that permits countries to some degree to adopt a risk-based approach to combating money laundering and terrorist financing. That language also authorises countries to permit DNFBPs to use a risk-based approach in applying certain of their AML and CFT obligations.

18. By adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk. This can inadvertently lead to a ‘tick box’ approach with the focus on meeting regulatory requirements rather than on combating money laundering or terrorist financing efficiently and effectively.

19. A number of the DNFBP sectors, including legal professionals, are already subject to regulatory or professional requirements (including as promulgated by SROs) that complement AML/CFT measures. For example, by virtue of their professional codes of conduct, many lawyers are already subject to an obligation to identify their clients (*e.g.* to check for conflict of interest) and the substance of the matter submitted to them by such clients, in order to appreciate the consequences that their advice may have. If a lawyer provides legal advice to a client that helps the client commit an offence, that lawyer may, depending on the lawyer’s state of knowledge, become an accomplice to the offence. This Guidance must be considered in the context of these professional and ethical codes of conduct. Where possible, it will be beneficial for legal professionals (and relevant authorities and SROs) to devise their AML/CFT policies and procedures in a way that harmonises with other regulatory or professional requirements. A risk-based AML/CFT regime should not impede free access to the services provided by legal professionals for legitimate purposes, but should create barriers to those who seek to misuse these services.

20. A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. Countries will need to identify the main vulnerabilities and address them accordingly. Legal professionals will need this assistance and information to help them to identify higher risk clients and services, including delivery channels, and geographical locations. These are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve.

21. The strategies to manage and mitigate money laundering and terrorist financing are typically aimed at preventing the activity from occurring through a mixture of deterrence (*e.g.* appropriate CDD measures), detection (*e.g.* monitoring and suspicious transaction reporting), and record-keeping so as to facilitate investigations.

22. Proportionate procedures should be designed based on assessed risk. Higher risk areas should be subject to enhanced procedures; this would include measures such as enhanced CDD checks and enhanced transaction monitoring. It also follows that in instances where risks are low, simplified, modified or reduced controls may be applied.

23. There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, an effective risk-based approach does involve identifying and categorising money laundering and terrorist financing risks and establishing reasonable controls based on risks identified.

24. An effective risk-based approach will allow legal professionals to exercise reasonable business and professional judgement with respect to clients. Application of a reasoned and well-articulated risk-based approach will justify the judgements made with regard to managing potential money laundering and terrorist financing risks. A risk-based approach should not be designed to prohibit or impede legal professionals from continuing with legitimate practice – especially given their role in society and the proper functioning of the justice system - or from finding innovative ways to diversify or expand their practices.

25. Regardless of the strength and effectiveness of AML/CFT controls, criminals will continue to attempt to move illicit funds undetected and will, from time to time, succeed. Criminals are more likely to target the DNFBP sectors, including legal professionals, if other routes become more difficult. For this reason, DNFBPs may be more or less vulnerable depending on the effectiveness of the AML/CFT procedures applied in other sectors. A risk-based approach allows DNFBPs, including legal professionals, to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

26. A reasonably designed and effectively implemented risk-based approach can provide an appropriate and effective control structure to manage identifiable money laundering and terrorist financing risks. However, it must be recognised that any reasonably applied controls, including controls implemented as a result of a reasonably designed and effectively implemented risk-based approach, will not identify and detect all instances of money laundering or terrorist financing. Therefore, designated competent authorities, SROs, law enforcement, and judicial authorities must take into account and give due consideration to a well reasoned risk-based approach. When there is a failure to implement an adequately designed risk-based approach or failure of a risk-based programme that was not adequate in its design, designated competent authorities, SROs, law enforcement or judicial authorities should take action as necessary and appropriate.

Potential Benefits and Challenges of the Risk-Based Approach

Benefits

27. The adoption of a risk-based approach to combating money laundering and terrorist financing can yield benefits for all parties, including the public. Applied effectively, the approach should allow a more efficient and effective use of resources and minimise burdens on clients. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively.

28. For legal professionals, the risk-based approach allows the flexibility to approach AML/CFT obligations using specialist skills and responsibilities. This requires legal professionals to take a wide and objective view of their activities and clients.

29. Efforts to combat money laundering and terrorist financing should also be flexible in order to adapt as risks evolve. As such, legal professionals should use their judgement, knowledge and expertise to develop an appropriate risk-based approach for their particular organisation, structure and practice activities.

Challenges

30. The risk-based approach is not necessarily an easy option and is challenging to both public and private sector entities. Some challenges may be inherent to the use of the risk-based approach. Others may stem from the difficulties in making the transition to a risk-based system. A risk-based approach requires resources and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems, and to train personnel. It further requires that sound and well-trained judgement be exercised in the design and implementation of procedures, and systems. It will certainly lead to a greater diversity in practice that should lead to innovations and improved compliance. However, it may also cause uncertainty regarding

expectations, difficulty in applying uniform regulatory treatment, and lack of understanding by clients regarding information required.

31. Implementing a risk-based approach requires that legal professionals have a sound understanding of the risks and are able to exercise sound judgement. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. The process will always benefit from information sharing by designated competent authorities and SROs. The provision of good practice guidance is also valuable. Attempting to pursue a risk-based approach without sufficient expertise may lead to flawed judgements. Legal professionals may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, thereby creating vulnerabilities. They, and (if applicable) their staff members, may be uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. This may also be true at various levels of management. However, in situations where management fails to recognise or underestimate the risks, a culture may develop that allows for inadequate resources to be devoted to compliance, leading to potentially significant compliance failures.

32. Designated competent authorities and SROs should place greater emphasis on whether legal professionals have an effective decision-making process with respect to risk management. Sample testing may be used or individual decisions reviewed as a means to test the effectiveness of a legal professional's overall risk management. Designated competent authorities and SROs should recognise that even though appropriate risk management structures and procedures are regularly updated, and the relevant policies, procedures, and processes are followed, decisions may still be made that are incorrect in light of additional information that was not reasonably available at the time.

33. In implementing the risk-based approach, legal professionals should be given the opportunity to make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices. Such potential diversity of practice will require that designated competent authorities and SROs make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges for staff working to monitor compliance. The existence of good practice guidance, continuing legal education, and supervisory training, industry studies and other materials will assist the designated competent authority or an SRO in determining whether a legal professional has made sound risk-based judgements.

34. Recommendation 25 requires adequate feedback to be provided to the financial sector and DNFBPs. Such feedback helps institutions, firms and businesses to more accurately assess the money laundering and terrorist financing risks and to adjust their risk programmes accordingly. This in turn makes the detection of suspicious activity more likely and improves the quality of any required suspicious transaction reports. As well as being an essential input to any assessment of country or sector wide risks, the promptness and content of such feedback is relevant to implementing an effective risk-based approach.

The potential benefits and potential challenges can be summarised as follows:

Potential Benefits:

- Better management of risks and cost-benefits
- Focus on real and identified threats
- Flexibility to adapt to risks that change over time

Potential Challenges:

- Identifying appropriate information to conduct a sound risk analysis
- Addressing short term transitional costs
- Greater need for more expert staff capable of making sound judgements. Regulatory response to potential diversity of practice.

Chapter Three: FATF and the Risk-Based Approach

35. The varying degrees of risk of money laundering or terrorist financing for particular types of DNFBPs, including legal professionals, or for particular types of clients, or transactions is an important consideration underlying the FATF Recommendations. According to the Recommendations, with regard to DNFBPs there are specific Recommendations where the degree of risk is an issue that a country either must take into account (if there is higher risk), or may take into account (if there is lower risk).

36. The risk-based approach is either incorporated into the Recommendations (and the Methodology) in specific and limited ways in a number of Recommendations, or it is inherently part of or linked to those Recommendations. For instance, for DNFBPs, including legal professionals risk is addressed in three principal areas (a) Customer/client Due Diligence (R.5, 6, 8 and 9); (b) legal professionals and/or firms' internal control systems (R.15); and (c) the approach of oversight/monitoring of DNFBPs, including legal professionals (R.24).

Client Due Diligence (R. 5, 6, 8 and 9)

37. Risk is referred to in several forms:

a) Higher risk – Under Recommendation 5, a country must require its DNFBPs, including legal professionals, to perform enhanced due diligence for higher-risk clients, business relationships or transactions. Recommendation 6 (politically exposed persons) is an example of this principle and is considered to be a higher risk scenario requiring enhanced due diligence.

b) Lower risk – A country may also permit legal professionals to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). Legal professionals may thus reduce or simplify (but not avoid completely) the required measures.

c) Risk arising from innovation – Under Recommendation 8, a country must require legal professionals to give special attention to the risks arising from new or developing technologies that might favour anonymity.

d) Risk assessment mechanism – The FATF standards require that there be an adequate mechanism by which designated competent authorities or SROs assess or review the procedures adopted by legal professionals to determine the degree of risk and how they manage that risk, as well as to review the actual determinations themselves. This expectation applies to all areas where the risk-based approach applies. In addition, where the designated competent authorities or SROs have issued guidelines on a suitable approach to risk-based procedures, it will be important to establish that these have been followed. The Recommendations also recognise that country risk is a necessary component of any risk assessment mechanism (R.5 & R.9).

Internal control systems (R.15)

38. Under Recommendation 15, the development of “appropriate” internal policies, training and audit systems will need to include a specific, and ongoing, consideration of the potential money laundering and terrorist financing risks associated with clients, products and services, geographic areas of operation and so forth. The Interpretative Note to Recommendation 15 makes it clear that a country may allow legal professionals to have regards to the money laundering and terrorist financing risks, and to the size of the business, when determining the type and extent of measures required.

Regulation and oversight by designated competent authorities or SROs (R.24)

39. Countries should ensure that legal professionals are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in a given business, *i.e.* if there is a low risk then reduced monitoring measures may be taken.

Applicability of the risk-based approach to terrorist financing

40. There are both similarities and differences in the application of a risk-based approach to terrorist financing and money laundering. They both require a process for identifying and assessing risk. However, the characteristics of terrorist financing make its detection difficult and the implementation of mitigation strategies may be challenging due to considerations such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

41. Funds that are used to finance terrorist activities may be derived either from criminal activity or may be from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing, though the activity, which may be indicative of suspicion, may not be identified as or connected to terrorist financing. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering. Where funds are from legal sources then it is even more difficult to determine if they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services to further their goals, with the only covert fact being the intended use of such materials and services purchased. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering. In all cases, however, legal professionals are not responsible for determining the type of underlying criminal activity or intended terrorist purpose.

42. The ability of legal professionals to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities is significantly more challenging than is the case for potential money laundering and other suspicious activity. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering).

43. Specific individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which such sanctions apply and the obligations on legal professionals to comply with those sanctions are decided by individual countries and are not a function of risk. Legal professionals may commit a criminal offence if they undertake business with a listed individual, organisation or country, or its agent, in contravention of applicable sanctions.

44. For these reasons, this Guidance has not comprehensively addressed the application of a risk-based process to terrorist financing. It is clearly preferable that a risk-based approach be applied where reasonably practicable, but further consultation with key stakeholders is required to identify a more comprehensive set of indicators of the methods and techniques used for terrorist financing, which can then be factored into strategies to assess terrorist financing risks and devise measures to mitigate them. DNFBPs, including legal professionals, would then have an additional basis upon

40-44 and such subsequent consultations when they occur.

Limitations to the risk-based approach

45. There are circumstances in which the application of a risk-based approach will not apply, or may be limited. There are also circumstances in which the application of a risk-based approach may not apply to the initial stages of a requirement or process, but then will apply to subsequent stages. The limitations to the risk-based approach are usually the result of legal or regulatory requirements that mandate certain actions to be taken.

46. Requirements to freeze assets of identified individuals or entities, in countries where such requirements exist, are independent of any risk assessment. The requirement to freeze is absolute and cannot be impacted by a risk-based process. Similarly, while the identification of potential suspicious transactions can be advanced by a risk-based approach, in countries where such obligations exist, the reporting of such suspicious transactions, once identified, is not risk-based. (See paragraph 119.)

47. CDD comprises several components – Identification and verification of the identity of clients and of beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing due diligence. Of these components, the identification and verification of identity of clients are requirements that must be completed regardless of the risk-based approach. However, in relation to all other CDD components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep records and documents that have been obtained for due diligence purposes, as well as transaction records, is not dependent on risk levels.

48. Countries may allow legal professionals to apply reduced or simplified measures where the risk of money laundering or terrorist financing is lower. However, these reduced or simplified measures do not necessarily apply to all aspects of CDD. Where these exemptions are subject to certain conditions being met, it is necessary to verify that these conditions apply, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. Information beyond client identity, such as client location, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a client should be sufficient to determine whether to go further, and in many cases client monitoring will provide additional information.

49. Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk clients, monitoring is needed to verify that transactions match the initial low risk profile and if not, trigger a process for appropriately revising the client's risk rating. Equally, risks for some clients may only become evident once a relationship with a client has begun. This makes appropriate and reasonable monitoring of client transactions an essential component of a properly designed risk-based approach; however, within this context it should be understood that not all transactions or clients will be monitored in exactly the same way. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this could be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption. Given the relationship between a legal professional and his/her client, the most effective form of ongoing monitoring will often be continued observance and awareness of a client's activities by the legal professional. This requires legal professionals to be alert to this basis of monitoring and for training of legal professionals to take this feature into account.

Distinguishing Risk-Based Monitoring and Risk-Based Policies and Processes

50. Risk-based policies and processes should be distinguished from risk-based monitoring by designated competent authorities or SROs. There is a general recognition within monitoring practice that resources should be allocated taking into account the risks posed by individual practices. The methodology adopted by the designated competent authorities or SROs to determine allocation of monitoring resources should cover the practice focus, the risk profile and the internal control environment, and should permit relevant comparisons between practices. Most fundamentally, such methodology needs to recognize that the relationship between the legal professional and the client is often an on-going one. The methodology used for determining the allocation of resources will need updating on an ongoing basis so as to reflect the nature, importance and scope of the risks to which individual practices are exposed. Consequently, this prioritisation should lead designated competent authorities or SROs to focus increased regulatory attention to legal professionals who engage in activities assessed to be of higher risk of money laundering or terrorist financing.

51. However, it should also be noted that the risk factors taken into account to prioritise the designated competent authorities or SROs' work will depend not only on the intrinsic risk associated with the activity undertaken, but also on the quality and effectiveness of the risk management systems put in place to address such risks.

52. Since designated competent authorities or SROs should have already assessed the quality of risk management controls applied by legal professionals, it is reasonable that their assessments of these controls be used, at least in part, to inform money laundering and terrorist financing risk assessments conducted by individual firms or businesses.

Summary box: A risk-based approach to countering money laundering and terrorist financing at the national level: key elements for success

- Legal professionals, designated competent authorities and/or SROs should have access to reliable and actionable information about the threats.
- There must be emphasis on cooperative arrangements among the policy makers, law enforcement, regulators, and the private sector.
- Authorities should publicly recognise that the risk-based approach will not eradicate all elements of risk.
- Authorities have a responsibility to establish an atmosphere in which legal professionals need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Designated competent authorities' and/or SROs' supervisory staff must be well-trained in the risk-based approach, both as applied by designated competent authorities/SROs and by legal professionals.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

Chapter One: High-level principles for creating a risk-based approach

53. The application of a risk-based approach to countering money laundering and the financing of terrorism will allow designated competent authorities or SROs and legal professionals to use their resources most effectively. This chapter sets out five high-level principles that should be considered by countries when designing a risk-based approach applicable to legal professionals. They could be considered as setting out a broad framework of good practice.

54. The five principles set out in this Guidance are intended to assist countries in their efforts to improve their AML/CFT regimes. They are not intended to be prescriptive, and should be applied in a manner that is well-considered, is appropriate to the particular circumstances of the country in question and takes into account the way in which legal professionals are regulated in that country and the obligations they are required to observe.

Principle One: Understanding and responding to the threats and vulnerabilities: a national risk assessment

55. Successful implementation of a risk-based approach to combating money-laundering and terrorist financing depends on a sound understanding of the threats and vulnerabilities. Where a country is seeking to introduce a risk-based approach at a national level, this will be greatly aided if there is a national understanding of the risks facing the country. This understanding can flow from a national risk assessment that can assist in identifying the risks.

56. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of designated competent authorities or SROs and the nature of DNFBPs, including legal professionals, each country's judgements about the risks will be unique, as will their decisions about how to implement a national assessment in practice. A national assessment need not be a single formal process or document. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and current understanding of the risks. Designated competent authorities and SROs, in consultation with the private sector, should consider how best to achieve this while also taking into account any jurisdictional limitations of applying the risk-based approach to legal professionals, as well as any risk associated with providing information on money laundering and terrorist vulnerabilities.

Principle Two: A legal/regulatory framework that supports the application of a risk-based approach

57. Countries should consider whether their legislative and regulatory frameworks are conducive to the application of the risk-based approach. Where appropriate the obligations imposed should be informed by the outcomes of the national risk assessment.

58. The risk-based approach does not mean the absence of a clear statement of what is required from the DNFBPs, including from legal professionals. However, under a risk-based approach, legal professionals should have a degree of flexibility to implement policies and procedures which respond appropriately to their own risk assessment. In effect, the standards implemented may be tailored

and/or amended by additional measures as appropriate to the risks of an individual legal professional and/or practice. The fact that policies and procedures, in accordance to the risk levels, may be applied to different services, clients and locations does not mean that policies and procedures need not be clearly defined.

59. Basic minimum AML/CFT requirements can co-exist with a risk-based approach. Indeed, sensible minimum standards, coupled with scope for these to be enhanced when the risk justifies it, should be at the core of risk-based AML/CFT requirements. These standards should, however, be focused on the outcome (combating through deterrence, detection, and, when there is a requirement in a particular country, reporting of money laundering and terrorist financing), rather than applying legal and regulatory requirements in a purely mechanistic manner to every client. SROs may assist in the development of such standards for legal professionals.

Principle Three: Design of a monitoring framework to support the application of the risk-based approach

60. In certain countries, SROs play a critical role in the regulation of legal professionals, which may be based on fundamental constitutional principles. Some SROs have the ability to audit or investigate their own members, although in some countries these powers may be limited to reviewing policies and procedures as opposed to specific clients and matters. Depending on the powers of and responsibilities accepted by SROs, SROs may be able to facilitate or ensure compliance by legal professionals with the relevant legislation and/or develop guidance relating to money laundering. In some countries, the SROs may provide a greater level of scrutiny than that which can be afforded by a government or regulatory AML program. SROs should be encouraged to work closely with domestic AML/CFT regulators. Countries should ensure that SROs have appropriate resources to discharge their AML/CFT responsibilities. In some cases, legal professionals may conduct activities falling within the scope of Recommendation 12 that under national law may also require supervision from appropriate authorities.

61. Where appropriate, designated competent authorities and SROs should seek to adopt a risk-based approach to the monitoring of controls to combat money laundering and terrorist financing. This should be based on a thorough and comprehensive understanding of the types of activity carried out by legal professionals, and the money laundering and terrorist financing risks to which these are exposed. Designated competent authorities and SROs will probably need to prioritise resources based on their overall assessment of where the risks are in the legal professionals' practices.

62. Designated competent authorities and SROs with responsibilities other than those related to AML/CFT will need to consider these risks alongside other risk assessments arising from the designated competent authority's or SRO's wider duties.

63. Such risk assessments should help the designated competent authority or SRO choose where to apply resources in its monitoring programme, with a view to using limited resources to achieve the greatest effect. A risk assessment may also indicate that the designated competent authority or SRO does not have adequate resources to deal with the risks. In such circumstances, the designated competent authority or SRO may need to obtain, where possible, additional resources or adopt other strategies to manage or mitigate any unacceptable residual risks.

64. The application of a risk-based approach to monitoring requires that designated competent authorities' and SROs' staff be able to make principle-based decisions in a fashion similar to what would be expected from the staff of a legal professional's practice. These decisions will cover the adequacy of the arrangements to combat money laundering and terrorist financing. As such, a designated competent authority or SRO may wish to consider how best to train its staff in the practical application of a risk-based approach to monitoring. This staff will need to be well-briefed as to the general principles of a risk-based approach, the possible methods of application, and what a risk-based approach looks like when successfully applied within the context of a national risk assessment.

Principle Four: Identifying the main actors and ensuring consistency

65. Countries should consider who the main stakeholders are when adopting a risk-based approach to combating money laundering and terrorist financing. These will differ from country to country. Thought should be given as to the most effective way to share responsibility between these parties, and how information may be shared to best effect. For example, consideration may be given to which body or bodies are best placed to provide guidance to legal professionals about how to implement a risk-based approach to AML/CFT.

66. A list of potential stakeholders may include the following:

- Government – This may include legislature, executive, and judiciary.
- Law enforcement agencies – This might include the police, customs and similar agencies.
- The financial intelligence unit (FIU), security services, and other similar agencies.
- Designated competent authorities/SROs (particularly bar associations and law societies).
- The private sector – This might include legal professionals and law firms and legal professional organisations and associations such as national, state, local, and specialty professional societies and bar associations.
- The public – Arrangements designed to counter money laundering and terrorist financing are ultimately designed to protect the law-abiding public. However, these arrangements may also act to place burdens on clients of legal professionals.
- Others – Those who are in a position to contribute to the conceptual basis underpinning the risk-based approach, such stakeholders may include academia and the media.

67. Clearly a government will be able to exert influence more effectively over some of these stakeholders than others. However, regardless of its capacity to influence, a government will be in a position to assess how all stakeholders can be encouraged to support efforts to combat money laundering and terrorist financing.

68. A further element is the role that governments have in seeking to gain recognition of the relevance of a risk-based approach from designated competent authorities. This may be assisted by relevant authorities making clear and consistent statements on the following issues:

- Legal professionals can be expected to have the flexibility to adjust their internal systems and controls taking into consideration lower and high risks, so long as such systems and controls are reasonable. However, there are also minimum legal and regulatory requirements and elements that apply irrespective of the risk level, such as minimum standards of CDD.
- Acknowledging that a legal professional's ability to detect and deter money laundering and terrorist financing may sometimes be necessarily limited and that information on risk factors is not always robust or freely available. There can therefore be reasonable policy and monitoring expectations about what a legal professional with good controls aimed at preventing money laundering and the financing of terrorism is able to achieve. A legal professional may have acted in good faith to take reasonable and considered steps to prevent money laundering, and documented the rationale for his/her decisions, and yet still be abused by a criminal.

- Acknowledging that not all high-risk situations are identical and as a result will not always require the application of precisely the same type of enhanced due diligence.

Principle Five: Information exchange between the public and private sector

69. Effective information exchange between the public and private sector will form an integral part of a country's strategy for combating money laundering and terrorist financing. In some cases, it will allow the private sector to provide designated competent authorities and SROs with information they identify as a result of previously provided government intelligence. In countries where SROs regulate and monitor legal professionals for AML compliance, such SROs may well acquire information that would be relevant to a country's strategy for combating money laundering and terrorist financing. To the extent that such information may be released in accordance with applicable laws, regulations, and rules, the results may be made available to the designated competent authorities.

70. Public authorities, whether law enforcement agencies, designated competent authorities or other bodies, have privileged access to information that may assist legal professionals to reach informed judgements when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, legal professionals are able to understand their clients' legal needs reasonably well. It is desirable that public and private bodies work collaboratively to identify what information is valuable to help combat money laundering and terrorist financing, and to develop means by which this information might be shared in a timely and effective manner.

71. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, designated competent authorities and law enforcement agencies should be able to share information and feedback on results and identified vulnerabilities, so that consistent and meaningful inputs can be provided to the private sector. All parties should of course, consider what safeguards are needed to adequately protect sensitive information held by public bodies from being disseminated in contravention of applicable laws and regulations.

72. Relevant stakeholders should seek to maintain a dialogue so that it is well understood what information has proved useful in combating money laundering and terrorist financing. For example, the types of information that might be usefully shared between the public and private sector would include, if available:

- Assessments of country risk.
- Typologies or assessments of how money launderers and terrorists have abused DNFBPs, especially legal professionals.
- Feedback on suspicious transaction reports and other relevant reports.
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards and a country's legal and regulatory framework, it may also be appropriate for authorities to share targeted confidential information with legal professionals.
- Countries, persons or organisations whose assets or transactions should be frozen.

73. When choosing what information can be properly and profitably shared, public authorities may wish to emphasise to legal professionals that information from public bodies should inform, but not be a substitute for legal professionals' own judgements. For example, countries may decide not to create what are perceived to be definitive country-approved lists of low risk client types. Instead,

public authorities may prefer to share information on the basis that this will be one input into legal professionals' decision making processes, along with any other relevant information that is available to legal professionals.

Chapter Two: Implementation of the Risk-Based Approach

Assessment of Risk to Inform National Priorities:

74. A risk-based approach should be built on sound foundations: effort must first be made to ensure that the risks are well understood. As such, a risk-based approach should be based on an assessment of the threats. This is true whenever a risk-based approach is applied, at any level, whether by countries or individual legal professionals and/or firms. A country's approach should be informed by its efforts to develop an understanding of the risks in that country. This can be considered as a "national risk assessment".

75. A national risk assessment should be regarded as a description of fundamental background information to assist designated competent authorities, law enforcement authorities, the FIU, financial institutions and DNFBPs to ensure that decisions about allocating responsibilities and resources at the national level are based on a practical, comprehensive and up-to-date understanding of the risks.

76. A national risk assessment should be tailored to the circumstances of the individual country, both in how it is executed, and its conclusions, though countries should be mindful that money laundering and terrorist financing can often have an international dimension, and that such information may also add value to the national risk assessment. Factors that may influence the risk of money laundering and terrorist financing in a country could include the following:

- Political environment.
- Legal environment.
- A country's economic structure.
- Cultural factors, and the nature of civil society.
- Sources, location and concentration of criminal activity.
- Size and composition of the financial services industry.
- Ownership structure of financial institutions and DNFBPs businesses.
- Size and nature of the activity carried out by DNFBPs, including legal professionals.
- Corporate governance arrangements in relation to financial institutions and DNFBPs and the wider economy.
- The nature of payment systems and the prevalence of cash-based transactions.
- Geographical spread of the financial industry's and DNFBPs' operations and clients.
- Types of products and services offered by the financial services industry and DNFBPs.
- Types of customers/clients serviced by financial institutions and DNFBPs.
- Types of predicate offences.

- Amounts of illicit money generated domestically.
- Amounts of illicit money generated abroad and laundered domestically.
- Main channels or instruments used for laundering or financing terrorism.
- Sectors of the legal economy affected.
- Underground/informal areas in the economy.

77. Countries should also consider how an understanding of the risks of money laundering and terrorist financing can be best achieved at the national level. Relevant questions could include: Which body or bodies will be responsible for contributing to this assessment? How formal should an assessment be? Should the designated competent authority's or SRO's view be made public? These are all questions for the designated competent authority or SRO to consider.

78. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and up-to-date understanding of the risks. To achieve the desired outcome, designated competent authorities and SROs should ensure that they identify and provide DNFBPs (including legal professionals) with the information needed to develop this understanding and to design and implement measures to mitigate the identified risks.

79. Developing and operating a risk-based approach involves forming judgements. It is important that these judgements are well informed. It follows that, to be effective, the risk-based approach should be information-based and include intelligence where appropriate. Effort should be made to ensure that risk assessments are based on fresh and accurate information. Governments utilising partnerships with law enforcement bodies, FIUs, designated competent authorities/SROs and legal professionals themselves, are well placed to bring their knowledge and expertise to bear in developing a risk-based approach that is appropriate for their particular country. Their assessments will not be static and will change over time, depending on how circumstances develop and how the threats evolve. As such, countries should facilitate the flow of information between different bodies, so that there are no institutional impediments to information dissemination.

80. Whatever form they take, a national assessment of the risks, along with measures to mitigate those risks, can inform how resources are applied to combat money laundering and terrorist financing, taking into account other relevant country policy goals. It can also inform how these resources are most effectively assigned to different public bodies and SROs, and how those bodies make use of those resources in an effective manner.

81. As well as assisting designated competent authorities and SROs to decide how to allocate funds to combat money laundering and terrorist financing, a national risk assessment can also inform decision-makers on the best strategies for implementing a regulatory regime to address the risks identified. An over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on legal professionals. Alternatively, less aggressive efforts may not be sufficient to protect society from the threats posed by criminals and terrorists. A sound understanding of the risks at the national level could help obviate these dangers.

Effective systems for monitoring and ensuring compliance with AML/CFT requirements – General Principles

82. FATF Recommendation 24 requires that legal professionals should be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether there is an effective system, regard may be had to the risk of money laundering or terrorist financing in the sector. There should be a designated competent authority or SRO responsible for

monitoring and ensuring compliance by legal professionals; and the authority or SRO should have adequate powers and resources to perform its functions, including powers to monitor and sanction.

Defining the acceptable level of risk

83. The level of AML/CFT risk will generally be affected by both internal and external risk factors. For example, risk levels may be increased by internal risk factors such as weak compliance resources, inadequate risk controls and insufficient senior management involvement. External level risks may rise due to factors such as the action of third parties and/or political and public developments.

84. As described in Section One, all activity involves an element of risk. Designated competent authorities and SROs should not prohibit legal professionals from conducting business with high risk clients. However, legal professionals would be prudent to identify, with assistance from this or other Guidance, the risks associated with acting for high risk clients. When applicable law prohibits legal professionals from acting for a client, the risk-based approach does not apply.

85. However, this does not exclude the need to implement basic minimum requirements. For instance, FATF Recommendation 5 (that applies to legal professionals through the incorporation of R.5 into R.12) states that “where [the legal professional] is unable to comply with [CDD requirements], it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transaction report in relation to the customer.” So the level of risk should strike an appropriate balance between the extremes of not accepting clients, and conducting business with unacceptable or unmitigated risk. As is recognised by the interpretative note to FATF Recommendation 16, however, in those countries where a reporting requirement has been adopted the matters that would fall under legal professional privilege or professional secrecy are determined by each country.³

86. Where legal professionals implement a risk-based approach, designated competent authorities and SROs must expect legal professionals to put in place effective policies, programmes, procedures and systems to mitigate the risk and acknowledge that even with effective systems not every suspect transaction will necessarily be detected. They should also ensure that those policies, programmes, procedures and systems are applied effectively to prevent legal professionals from becoming conduits for illegal proceeds and ensure that they keep records and make reports (where obligated) that are of use to national authorities in combating money laundering and terrorist financing. Efficient policies and procedures will reduce the level of risks, but are unlikely to eliminate them completely. Assessing money laundering and terrorist financing risks requires judgement and is not an exact science. Monitoring aims at detecting unusual or suspicious transactions among an extremely large number of legitimate transactions; furthermore, the demarcation of what is unusual may not always be straightforward since what is “customary” may vary depending on the clients’ business. This is why developing an accurate client profile is important in managing a risk-based system. Moreover, although procedures and controls are frequently based on previous typologies, criminals will adapt their techniques, which may quickly limit the utility of such typologies.

87. Additionally, not all high risk situations are identical, and therefore will not always require precisely the same level of enhanced due diligence. As a result, designated competent authorities/SROs will expect legal professionals to identify individual high risk categories and apply specific and appropriate mitigation measures. Further information on the identification of specific risk categories is provided in Section Three, “Guidance for Legal Professionals on Implementing a Risk-Based Approach.”

³ See Annex 1 for a summary of decisions by judicial authorities on these issues.

Proportionate Supervisory/Monitoring Actions to support the Risk-Based Approach

88. Designated competent authorities and SROs should seek to identify weaknesses through an effective programme of both on-site and off-site supervision, and through analysis of internal and other available information.

89. In the course of their examinations, designated competent authorities and SROs should review a legal professional's AML/CFT risk assessments, as well as its policies, procedures and control systems to arrive at an overall assessment of the risk profile of legal professionals' practices and the adequacy of their mitigation measures. Where available, assessments carried out by or for legal professionals may be a useful source of information. The designated competent authority/SRO assessment of management's ability and willingness to take necessary corrective action is also a critical determining factor. Designated competent authorities and SROs should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe response.

90. Nevertheless, it may happen that the lack of detection of an isolated high risk transaction, or of transactions of an isolated high risk client, will in itself be significant, for instance where the amounts are significant, or where the money laundering and terrorist financing typology is well known, or where a scheme has remained undetected for a long time. Such a case might indicate an accumulation of weak risk management practices or regulatory breaches regarding the identification of high risks, monitoring, staff training and internal controls, and therefore, might alone justify action to ensure compliance with the AML/CFT requirements.

91. Designated competent authorities and SROs can and should use their knowledge of the risks associated with services, clients and geographic locations to help them evaluate legal professionals' money laundering and terrorist financing risk assessments, with the understanding, however, that they may possess information that has not been made available to legal professionals and, therefore, legal professionals would not have been able to take such information into account when developing and implementing a risk-based approach. Designated competent authorities and SROs (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist legal professionals in managing their risks. Where legal professionals are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by their designated competent authorities and SROs⁴. Guidance specifically designed for legal professionals is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where legal professionals use excessively narrow risk categories that do not capture all existing risks, or adopt criteria that lead to the identification of a large number of higher risk relationships, but without providing for adequate additional CDD measures.

92. In the context of the risk-based approach, the primary focus for designated competent authorities and SROs should be to determine whether or not the legal professional's AML/CFT compliance and risk management programme is adequate to: (a) meet the minimum regulatory requirements, and (b) appropriately and effectively mitigate the risks. The monitoring goal is not to prohibit high risk activity, but rather to be confident that legal professionals have adequately and effectively implemented appropriate risk mitigation strategies. Appropriate authorities should, when considering taking action (including applying penalties and sanctions), take into account and give due consideration to the reasoned judgements of legal professionals who are implementing and/or operating an appropriate risk-based approach, which judgements, in hindsight, may ultimately be determined to have been incorrect. In some countries and situations, judicial authorities alone will determine whether the legal professional has complied with the obligation to exercise reasonable judgement.

⁴ FATF Recommendations 5 and 25, Methodology Essential Criteria 25.1 and 5.12.

93. Under FATF Recommendation 24, designated competent authorities and SROs should have adequate powers to perform their monitoring functions, including the power to impose adequate sanctions for failure to comply with statutory and regulatory requirements to combat money laundering and terrorist financing. Fines and/or penalties are not appropriate in all regulatory actions, nor will they be permissible in all jurisdictions, to correct or remedy AML/CFT deficiencies. However, subject to the requirements of this paragraph, competent authorities, judicial authorities and SROs must have the authority and willingness to apply appropriate sanctions in cases where substantial deficiencies exist. Often, action will take the form of a remedial programme through the normal monitoring processes.

94. In considering the above factors it is clear that proportionate monitoring will be supported by two central features:

a) Regulatory Transparency

95. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Designated competent authorities and SROs are aware that legal professionals, while looking for professional freedom to make their own risk judgements, will also seek guidance on regulatory obligations. As such, the designated competent authority/SRO with AML/CFT supervisory/monitoring responsibilities should seek to be transparent in setting out what it expects, and will need to consider appropriate mechanisms of communicating these messages. For instance, this may be in the form of high-level requirements, based on desired outcomes, rather than detailed processes. If SROs responsible for the regulation of the relevant legal professionals (including regulation of AML risks) carry out regular AML compliance reviews of their members or otherwise take measures to supervise compliance, the form of an SRO monitoring programme should be determined by each SRO's rules and regulations.

96. No matter what individual procedure is adopted, the guiding principle will be that there is an awareness of legal responsibilities and regulatory expectations. In the absence of this transparency there is the danger that monitoring actions may be perceived as either disproportionate or unpredictable, which may undermine even the most effective application of the risk-based approach by legal professionals.

b) General Education, Staff Training of Designated Competent Authorities, SROs, and Enforcement Staff

97. SROs or other bodies that have a supervisory or educational role for legal professionals and legal professional organisations all have a stake in an effective risk-based system. This includes making available to legal professionals educational materials, further guidance and increasing awareness of money laundering concerns and risks. Central to the ability of legal professionals to seek to train and guard against money laundering effectively in a risk-based approach, is the provision of realistic typologies, particularly those where there is unwitting involvement.

98. In the context of the risk-based approach, it is not possible to specify precisely what a legal professional has to do, in all cases, to meet its regulatory obligations. Thus, a prevailing consideration will be how best to ensure the consistent implementation of predictable and proportionate monitoring actions. The effectiveness of monitoring training will therefore be important to the successful delivery of proportionate supervisory/monitoring actions.

99. Training should aim to allow designated competent authorities/SRO staff to form sound comparative judgements about AML/CFT systems and controls. It is important in conducting assessments that designated competent authorities and SROs have the ability to make judgements regarding management controls in light of the risks assumed by firms and considering available industry practices. Designated competent authorities and SROs might also find it useful to undertake

comparative assessments so as to form judgements as to the relative strengths and weaknesses of different legal professional organisations' arrangements.

100. The training should include instructing designated competent authorities and SROs about how to evaluate whether senior management has implemented adequate risk management measures, and determine if the necessary procedures and controls are in place. The training should also include reference to specific guidance, where available. Designated competent authorities and SROs also should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

101. To fulfil these responsibilities, training should enable designated competent authorities and SROs monitoring staff to adequately assess:

- i. The quality of internal procedures, including ongoing employee training programmes and internal audit, compliance and risk management functions.
- ii. Whether or not the risk management policies and processes are appropriate in light of legal professionals' risk profile, and are periodically adjusted in light of changing risk profiles.
- iii. The participation of senior management to confirm that they have undertaken adequate risk management, and that the necessary procedures and controls are in place.

102. Educating legal professionals on AML/CFT issues and the risk-based approach is a key element of an effective risk-based approach. Designated competent authorities should thus consider, in discussion with SROs and legal professionals and other appropriate organisations, ways of encouraging educational bodies (such as universities and law schools) to include within the education and training of legal professionals at all levels appropriate references to AML/CFT laws and the appropriate role that legal professionals can play in combating money laundering and terrorist financing.

SECTION THREE: GUIDANCE FOR LEGAL PROFESSIONALS ON IMPLEMENTING A RISK-BASED APPROACH

Chapter One: Risk Categories

103. Potential money laundering and terrorist financing risks faced by legal professionals will vary according to many factors including the activities undertaken by the legal professional, the type and identity of client, and the nature of the client relationship and its origin. Legal professionals should identify the criteria that enable them to best assess the potential money laundering and where feasible terrorist financing risks their practices give rise to and should then implement a reasonable risk based approach based on those criteria. These criteria are not exhaustive and are not intended to be prescriptive, and should be applied in a manner that is well-considered, is appropriate to the particular circumstances of the country and takes into account the way in which legal professionals are regulated in that country and the obligations they are required to observe.

104. Identification of the money laundering risks and terrorist financing risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate these risks. Although a risk assessment should normally be performed at the inception of a client relationship, for a legal professional, the ongoing nature of the advice and services the legal professional often provides means that automated transaction monitoring systems of the type used by financial institutions will be inappropriate for many legal professionals. The individual legal professionals working with the client are better positioned to identify and detect changes in the type of work or the nature of the client's activities, this is because the lawyer's knowledge of the client and its business will develop throughout the duration of what is expected to be a longer term relationship. Legal professionals will need to pay attention to the nature of the risks presented by isolated, small and short-term client relationships that, depending upon the circumstances, may be low risk (*e.g.* advice provided to walk-ups in a legal aid clinic).

105. The amount and degree of monitoring will depend on the nature and frequency of the relationship. A legal professional may also have to adjust his or her risk assessment of a particular client based upon information received from a designated competent authority, SRO, or other credible sources.

106. Money laundering and terrorist financing risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling legal professionals, where required, to subject each client to reasonable and proportionate risk assessment. The most commonly used risk criteria are: country or geographic risk; client risk; and risk associated with the particular service offered. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering or terrorist financing may vary from one legal professional and/or firm to another, particularly given the size, sophistication, nature and scope of services offered by the legal professional and/or firm. These criteria, however, should not be considered in isolation. Legal professionals, in light of their individual practices and based on their reasonable judgements, will need to assess independently the weight to be given to each risk factor.

107. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is merely intended to provide a suggested framework for approaching the management of potential risks.

Country/Geographic Risk

108. There is no universally agreed definition by either designated competent authorities, SROs, or legal professionals that prescribes whether a particular country or geographic area (including the country within which the legal professional practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Money laundering and terrorist financing risks have the potential to arise from almost any source, such as the domicile of the client, the location of the transaction and the source of the funding. Countries that pose a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but that may not be universally recognised, may be taken into account by a legal professional because of the standing of the issuer of the sanctions and the nature of the measures.
- Countries identified by credible sources⁵ as generally lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as being a location from which funds or support are provided to terrorist organizations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.

Client Risk

109. Determining the potential money laundering or terrorist financing risks posed by a client, or category of clients, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a legal professional should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of clients whose activities may indicate a higher risk include:

- PEPs are considered as higher risk clients – If a legal professional is advising a client that is a PEP, or where a PEP is the beneficial owner of the client, with respect to the activities specified in Recommendation 12, then a legal professional will need to carry out appropriate enhanced CDD, as required by Recommendation 6. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's home country, the type of work the PEP is instructing the legal professional to perform or carry out, and the scrutiny to which the PEP is under in the PEP's home country.

⁵ “Credible sources” refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

- If a PEP is otherwise involved in a client (other than in the circumstances of Recommendation 6), then the nature of the risk should be considered in light of all relevant circumstances, such as:
 - The nature of the relationship between the client and the PEP. Even if the PEP does not have a controlling interest or a dominant position on the board or in management and therefore does not qualify as a beneficial owner, the PEP may nonetheless affect the risk assessment.
 - The nature of the client (*e.g.* is it a public listed company).
 - The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company and the client is purchasing real property for adequate consideration.
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated in all the circumstances of the representation).
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely fashion the true beneficial owner or controlling interests, such as the unexplained use of legal persons or legal arrangements, nominee shares or bearer shares.
- Clients that are cash (and cash equivalent) intensive businesses including:
 - Money services businesses (*e.g.* remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities).
 - Casinos, betting and other gambling related activities.
 - Businesses that while not normally cash intensive, generate substantial amounts of cash.
- Where clients that are cash intensive businesses are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations this may mitigate the risks.
- Charities and other “not for profit” organisations (NPOs) that are not subject to monitoring or supervision (especially those operating on a “cross-border” basis) by designated competent authorities⁶ or SROs.
- Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SROs.
- Clients having convictions for proceeds generating crimes who instruct the legal professional (who has actual knowledge of such convictions) to undertake specified activities on their behalf.
- Clients who have no address, or multiple addresses without legitimate reasons.
- Clients who change their settlement or execution instructions without appropriate explanation.

⁶ See Special Recommendation VIII.

- The use of legal persons and arrangements without any apparent legal or legitimate tax, business, economic or other reason.

Service Risk

110. An overall risk assessment should also include determining the potential risks presented by the services offered by a legal professional, noting that the various legal professionals provide a broad and diverse range of services. The context of the services being offered or delivered is always fundamental to a risk-based approach. Any one of the factors discussed in this Guidance alone may not itself constitute a high risk circumstance. High risk circumstances can be determined only by the careful evaluation of a range of factors that cumulatively and after taking into account any mitigating circumstances would warrant increased risk assessment. When determining the risks associated with provision of services related to specified activities, consideration should be given to such factors as:

- Services where legal professionals, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they actually control in the act of closing a business transaction.
- Services to conceal improperly beneficial ownership from competent authorities.
- Services requested by the client for which the legal professional does not have expertise excepting where the legal professional is referring the request to an appropriately trained professional for advice.
- Transfer of real estate between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.⁷
- 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.
- Transactions where it is readily apparent to the legal professional that there is inadequate consideration, such as when the client does not identify legitimate reasons for the amount of the consideration.
- Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes.
- Clients who offer to pay extraordinary fees for services which would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where a legal professional may receive a significant premium for a successful representation, should not be considered a risk factor.
- The source of funds and the source of wealth – The source of funds is the activity that generates the funds for a client, while the source of wealth describes the activities that have generated the total net worth of a client.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a client that would otherwise appear to be higher risk might allow for a legal professional to treat the client as lower risk.

⁷ See the FATF Typologies report *Money Laundering and Terrorist Financing through the Real Estate Sector* at <http://www.fatf-gafi.org/dataoecd/45/31/40705101.pdf>.

- Shell companies, companies with ownership through nominee shareholding and control through nominee and corporate directors⁸.
- Situations where it is difficult to identify the beneficiaries of trusts; this might include a discretionary trust that gives the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust, and when a trust is set up for the purpose of managing shares in a company that can make it more difficult to determine the beneficiaries of assets managed by the trust⁹;
- Services that deliberately have provided or purposely depend upon more anonymity in the client identity or participants than is normal under the circumstances and experience of the legal professional.
- Legal persons that, as a separate business, offer TCSP services should have regard to the TCSP Guidance, even if such legal persons are owned or operated by legal professionals. Legal professionals, however, who offer TCSP services should have regard to this Guidance, and should consider customer or service risks related to TCSPs such as the following:
 - Unexplained use of express trusts.
 - Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices.
 - In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
 - In the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and classes within an expression of wishes.

Variables that May Impact Risk

111. Due regard must be accorded to the vast and profound differences in practices, size, scale and expertise, amongst legal professionals. As a result, consideration must be given to these factors when creating a reasonable risk-based approach and the resources that can be reasonably allocated to implement and manage it. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a risk-based approach proportionate to the scope and nature of the practitioner's practice.

112. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular legal professional. This factor must always be considered in the context of the legal professional's practice. A legal professional's risk-based approach methodology may thus take into account risk variables specific to a particular client or type of work. Consistent with the risk-based approach and the concept of proportionality, the presence of one or more of these variables may cause a legal professional to conclude that either enhanced due diligence and monitoring is warranted, or conversely that normal CDD and monitoring can be reduced, modified or simplified. These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

⁸ See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" published 13 October 2006.

⁹ See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" Annex 2 on trusts, for a more detailed description of "potential for misuse" of trusts.

- The nature of the client relationship and the client's need for the legal professional to provide specified activities.
- The level of regulation or other oversight or governance regime to which a client is subject. For example, a client that is a financial institution or legal professional regulated in a country with a satisfactory AML/CFT regime poses less risk of money laundering than a client in an industry that has money laundering risks and yet is unregulated for money laundering purposes.
- The reputation and publicly available information about a client. Legal persons that are transparent and well known in the public domain and have operated for a number of years without being convicted of proceeds generating crimes may have low susceptibility to money laundering.
- The regularity or duration of the relationship.
- The familiarity of the legal professional with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a legal professional's own activities within the country.
- The proportionality between the magnitude or volume and longevity of the client's business and its legal requirements, including the nature of professional services sought.
- Subject to other factors (including the nature of the services and the source and nature of the client relationship), providing limited legal services in the capacity of a local or special counsel may be considered a low risk factor. This may also, in any event, mean that the legal professional is not "preparing for" or "carrying out" a transaction for a regulated activity specified in Recommendation 12.
- Significant and unexplained geographic distance between the legal professional organisation and the location of the client where there is no nexus to the type of work being undertaken.
- Where a prospective client has instructed the legal professional to undertake a single transaction-based service (as opposed to an ongoing advisory relationship) and one or more other risk factors are present.
- Risks that may arise from the use of new or developing technologies that permit non-face to face relationships and could favour anonymity. However, due to the prevalence of electronic communication between legal professionals and clients in the delivery of legal services, non-face to face interaction between legal professionals and clients should not, standing alone, be considered a high risk factor. For example, non-face to face, cross-border work for an existing client is not necessarily high risk work for certain organisations (such as regional, national or international law firms or other firms regardless of size that practice in that type of work) nor would customary services rendered by a sole practitioner on a local basis to a client in the local community who does not otherwise present increased risks.
- The nature of the referral or origination of the client. A prospective client may contact a legal professional in an unsolicited manner or without common or customary methods of introduction or referrals, which may increase risk. By contrast, where a prospective client has been referred from another trusted source subject to an AML/CFT regime that is in line with the FATF standards, the referral may be considered a mitigating risk factor.
- The structure of a client or transaction. Structures with no apparent legal, tax, business, economic or other legitimate reason may increase risk. Legal professionals often design

structures (even if complex) for legitimate legal, tax, business, economic or other legitimate reasons, in which case the risk of money laundering could be reduced.

- Trusts that are pensions may be considered lower risk.

Controls for Higher Risk Situations

113. Legal professionals should implement appropriate measures and controls to mitigate the potential money laundering and terrorist financing risks with respect to those clients that, as the result of the legal professional or firm risk-based approach, are determined to be higher risk. Paramount among these measures is the requirement to train legal professionals and appropriate staff to identify and detect changes in activity by reference to risk-based criteria. These measures and controls may include:

- General training on money laundering methods and risks relevant to legal professionals.
- Targeted training for increased awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work.
- Increased levels of CDD or enhanced due diligence for higher risk situations.
- Escalation or additional review and/or consultation by the legal professional or within a firm at the establishment of a relationship.
- Periodic review of the services offered by the legal professional and/or firm to determine whether the risk of money laundering and terrorist financing occurring has increased.
- Reviewing client relationships from time to time to determine whether the risk of money laundering and terrorist financing occurring has increased.
- The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that a legal professional establish specific controls targeting each risk criterion.

Chapter Two: Application of a Risk-Based Approach

Customer Due Diligence/Know Your Customer

114. Client Due Diligence/Know Your Client is intended to enable a legal professional to form a reasonable belief that it has appropriate awareness of the true identity of each client. The legal professional's procedures should apply in circumstances where a legal and professional is preparing for or carrying out¹⁰ the activities listed in Recommendation 12 and include procedures to:

- a) Identify and appropriately verify the identity of each client on a timely basis.
- b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner such that the legal professional is reasonably satisfied that it knows who the beneficial owner is. The general rule is that clients should be subject to the full range of CDD measures, including the requirement to identify the beneficial owner in accordance with this paragraph. The purpose of identifying beneficial ownership is to ascertain those natural persons who exercise effective control over a client, whether by means of ownership, voting

¹⁰ See paragraphs 12-13 regarding when a legal professional would or would not be engaged in "preparing for" or "carrying out" transactions for clients, and hence the requirements of Recommendation 12 would apply.

rights or otherwise. Legal professionals should have regard to this purpose when identifying the beneficial owner. They may use a risk-based approach when determining the extent to which they are required to identify the beneficial owner, depending on the type of client, business relationship and transaction and other appropriate factors in accordance with Recommendation 5 and its Interpretative Note, § 9-12¹¹.

c) Obtain appropriate information to understand the client's circumstances and business depending on the nature, scope and timing of the services to be provided. This information may be obtained from clients during the normal course of their instructions to legal professionals.

115. The starting point is for a legal professional to assess the risks that the client may pose taking into consideration any appropriate risk variables (and any mitigating factors) before making a final determination. The legal professional's assessment of risk will then inform the overall approach to CDD requirements and appropriate verification. Legal professionals will reasonably determine the CDD requirements appropriate to each client given the legal professional's familiarity with the client, which may include:

- A standard level of CDD, generally to be applied to all clients.
- The standard level being reduced after consideration of appropriate risk variables, and in recognised lower risk scenarios, such as:
 - Publicly listed companies (and their majority owned subsidiaries).
 - Financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.
 - Government authorities and state run enterprises (other than those from sanctioned countries).
- An increased level of CDD in respect of those clients that are reasonably determined by the legal professional to be of higher risk. This may be the result of the client's business activity, ownership structure, particular service offered including work involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as the risks outlined in paragraphs 108-109.

Monitoring of Clients and Specified Activities

116. The degree and nature of monitoring by a legal professional will depend on the type of legal professional, and if it is a firm, the size and geographic 'footprint' of the firm, the AML/CFT risks that the firm has identified and the nature of the regulated activity provided. Given the nature of the advisory relationship legal professionals have with their clients and that an element of that advisory relationship will usually involve frequent client contact, monitoring is typically best achieved by trained individuals having contact with the client (either face to face or by other means of communication). For purposes of paragraphs 116 to 118 (and related paragraphs), "monitoring" does not oblige the legal professional to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis his or her client. It rather refers to maintaining awareness throughout

¹¹ Legal professionals should have regard to the Interpretative Notes to Recommendation 5 and the AML/CFT 2004 Methodology Essential Criteria 5.5 and 5.8-5.12, which, among other things, provide more details on the measures that need to be taken to identify beneficial owners, and the impact of higher or lower risk on the required measures.

the course of work for a client to money laundering or terrorist financing activity and/or changing risk factors.

117. Monitoring of these advisory relationships cannot be achieved solely by reliance on automated systems and whether any such systems would be appropriate will depend in part on the nature of a legal professional's practice and resources reasonably available to the legal professional. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate monitoring systems and a risk-based approach proportionate to the scope and nature of the practitioner's practice. A legal professional's advisory relationships are best monitored by the individuals having direct client contact being appropriately trained to identify and detect changes in the risk profile of a client. Where appropriate this should be supported by systems, controls and records within a framework of support by the firm (*e.g.* tailored training programs appropriate to the level of staff responsibility).

118. Legal professionals should also assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs can fall within the system and control framework developed to manage the risk of the firm. The results of the monitoring may also be documented.

119. The civil law notary does not represent parties to a contract and therefore must maintain a fair position with regard to any duty to both parties.

Suspicious Transaction Reporting

120. This Guidance does not address FATF Recommendations relating to suspicious transaction reporting (STR) and the proscription against "tipping off" those who are the subject of such reports. Different countries have undertaken different approaches to these Recommendations of the FATF. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of the suspicious activity under these circumstances is not applicable. STRs are not part of risk assessment, but rather reflect a response mechanism – typically to an SRO or government enforcement authority – once a suspicion of money laundering has been identified. For those reasons, this Guidance does not address those elements of the FATF Recommendations.

Education, Training and Awareness

121. Recommendation 15 requires that legal professionals provide their staff with AML/CFT training, and it is important that legal professional staff receive appropriate and proportional training with regard to money laundering. For legal professionals, and those in smaller firms in particular, such training may assist with monitoring obligations. A legal professional's commitment to having appropriate controls relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant legal professionals with at least general information on AML/CFT laws, regulations and internal policies. To satisfy a risk-based approach, particular attention should be given to risk factors or circumstances occurring in the legal professional's own practice. In addition, governments, SROs and other representative bodies for both common and civil law notaries and bar associations should work with educational institutions to see that both legal professionals, and students taking courses to train for or become legal professionals, are educated on money laundering and terrorist financing risks. For example, bar societies and associations should be encouraged to produce continuing legal education programs on AML/CFT and the risk-based approach.

122. Applying a risk-based approach to the various methods available for training, however, gives each legal professional flexibility regarding the frequency, delivery mechanisms and focus of such training. Legal professionals should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

- Tailored to the relevant staff responsibility (*e.g.* client contact or administration).

- At the appropriate level of detail (*e.g.* considering the nature of services provided by the legal professional).
- At a frequency suitable to the risk level of the type of work undertaken by the legal professional.
- Used to test to assess staff knowledge of the information provided.

Chapter Three: Internal Controls

123. Many DNFBPs differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of DNFBPs have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against money laundering and terrorist financing. For a number of DNFBPs, a single person may be responsible for the functions of front office, back office, money laundering reporting, and senior management. This particularity of DNFBPs, including legal professionals, should be taken into account in designing a risk-based framework for internal controls systems. The Interpretative Note to Recommendation 15, dealing with internal controls, specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size of the business.

124. To enable legal professionals to have effective risk-based approaches, the risk-based process must be a part of the internal controls of the legal professional or firm. Legal professionals operate within a wide range of differing business structures, from sole practitioners to large partnerships. These structures often mean that legal professionals' businesses have a flat management structure and that most or all of the principals (or partners) of the firm hold ultimate management responsibility. In other organisations, legal professionals employ corporate style organisational structures with tiered management responsibility. In both cases the principals or the managers are ultimately responsible for ensuring that the organisation maintains an effective internal control structure. Engagement by the principals and managers in AML/CFT is an important aspect of the application of the risk-based approach since such engagement reinforces a culture of compliance, ensuring that staff adheres to the legal professional's policies, procedures and processes designed to limit and control money laundering risks.

125. The nature and extent of the AML/CFT controls, as well as meeting national requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will depend upon a number of factors, such as:

- The nature, scale and complexity of a legal professional's business.
- The diversity of a legal professional's operations, including geographical diversity.
- The legal professional's client, service and activity profile.
- The degree of risk associated with each area of the legal professional's operations.
- The services being offered and the frequency of client contact (either in person or by other means of communication).

126. Subject to the size and scope of the legal professional's organisation, the framework of risk-based internal controls should:

- Have appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP.
- Provide increased focus on a legal professional's operations (*e.g.* services, clients and geographic locations) that are more vulnerable to abuse by money launderers.
- Provide for periodic review of the risk assessment and management processes, taking into account the environment within which the legal professional operates and the activity in its marketplace.
- Designate personnel at an appropriate level who are responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme if appropriate given the scale of the organisation and the nature of the legal professional's practice.
- Inform the principals of compliance initiatives, identified compliance deficiencies and corrective action taken.
- Provide for programme continuity despite changes in management or employee composition or structure.
- Focus on meeting all regulatory record keeping or other requirements, as well as promulgated measures for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based CDD policies, procedures and processes.
- Provide for adequate controls for higher risk clients and services as necessary, such as review with or approvals from others.
- Provide for adequate supervision and support for staff activity that forms part of the organisation's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of relevant personnel.
- Provide for appropriate training to be given to all relevant staff.
- For groups, to the extent possible, provide a common control framework.

ANNEXES

ANNEX 1

SOURCES OF FURTHER INFORMATION

Various sources of information exist that may help governments and legal professionals in their development of a risk-based approach. Although not an exhaustive list, this Annex 1 highlights a number of useful web-links that governments and legal professionals may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such as AML/CFT assessments.

A. Financial Action Task Force Documents

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. Key resources include the 40 Recommendations on Money Laundering and 9 Special Recommendations on Terrorist Financing, the Methodology for Assessing Compliance with the FATF Recommendations, the Handbook for Countries and Assessors, methods and trends (typologies) reports and mutual evaluation reports.

www.fatf-gafi.org

B. Legislation/and Court Decisions

The rulings by the ECJ of June 26th 2007 by the Belgium Constitution Court of January 23rd 2008 and the French Conseil d'État of April 10th, 2008 have confirmed that anti-money laundering regulation cannot require or permit the breach the lawyer's duty of professional secrecy when performing the essential activities of the profession. In addition, the Court of First Instance in the Joined Cases T-125/03 & T-253/03 Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission of the European Communities has recently restated the ruling in the *AM&S* case that professional secrecy "meets the need to ensure that every person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it (*AM&S*, paragraph 18). That principle is thus closely linked to the concept of the lawyer's role as collaborating in the administration of justice by the courts (*AM&S*, paragraph 24).

C. Links to Information on the Supervisory Program in Certain Countries

Switzerland

1. See articles 18 to 21 of the lawyers and notaries' SRO regulations (SRO SAV/SNV): www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf

2. See articles 38 and 45 to 47 of the lawyers and notaries' SRO statutes (SRO SAV/SNV): www.oad-fsa-fsn.ch/fr/02_beitritt/01_regelwerke.htm/01_Statuten.pdf

D. Guidance on the Risk-based Approach

1. Law Society of Ireland: www.lawsociety.ie.
2. Law Society of England and Wales: www.lawsociety.org.uk
3. Law Society of Hong Kong: www.hklawsoc.org.hk
4. Organisme d'autoréglementation de la fédération suisse des avocats et de la fédération suisse des notaires (SRO SAV/SNV): home page: www.sro-sav-snv.ch/
www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf (art. 41 to 46)
5. The Netherlands Bar Association: www.advocatenorde.nl
6. The Royal Dutch Notarial Society: www.notaris.nl

E. Other sources of information to help assist countries' and legal professionals' risk assessment of countries and cross-border activities

In determining the levels of risks associated with particular country or cross border activity, legal professionals and governments may draw on a range of publicly available information sources, these may include reports that detail observance of international standards and codes, specific risk ratings associated with illicit activity, corruption surveys and levels of international cooperation. Although not an exhaustive list the following are commonly utilised:

- IMF and World Bank Reports on observance of international standards and codes (Financial Sector Assessment Programme)
 - World Bank reports: www1.worldbank.org/finance/html/cntrynew2.html
 - International Monetary Fund: www.imf.org/external/np/rosc/rosc.asp?sort=topic#RR
 - Offshore Financial Centres (OFCs) IMF staff assessments www.imf.org/external/np/ofca/ofca.asp
- Mutual evaluation reports issued by FATF Style Regional Bodies:
 1. Asia/Pacific Group on Money Laundering (APG) www.apgml.org/documents/default.aspx?DocumentCategoryID=8
 2. Caribbean Financial Action Task Force (CFATF) www.cfatf.org/profiles/profiles.asp
 3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/5_money_laundering/Evaluations/Reports_summaries_3.asp#TopOfPage
 4. Eurasian Group (EAG)

www.eurasiangroup.org/index-7.htm

5. GAFISUD

www.gafisud.org/miembros.htm

6. Middle East and North Africa FATF (MENAFATF)

www.menafatf.org/TopicList.asp?cType=train

7. The Eastern and South African Anti Money Laundering Group (ESAAMLG)

www.esaamlg.org/

8. Groupe Inter-gouvernemental d'Action contre le Blanchiment d'Argent (GIABA)

www.giabasn.org/?lang=en&sid

- OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting)
www.oecd.org/document/49/0,2340,en_2649_34171_1901105_1_1_1_1,00.html
- International Narcotics Control Strategy Report (published annually by the US State Department)
www.state.gov/p/inl/rls/nrcrpt/
- Egmont Group membership - Coalition of financial intelligence units that participate in regular information exchange and the sharing of good practice, acceptance as a member of the Egmont Group is based a formal procedure that countries must go through in order to be acknowledged as meeting the Egmont definition of an FIU.
www.egmontgroup.org/
- Signatory to the United Nations Convention against Transnational Organized Crime
www.unodc.org/unodc/crime_cicp_signatures_convention.html
- The Office of Foreign Assets Control (“OFAC”) of the US Department of the Treasury economic and trade, Sanctions Programmes
www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml
- Consolidated list of persons, groups and entities subject to EU Financial Sanctions
http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm
- UN Security Council Sanctions Committee - Country Status:
www.un.org/sc/committees/

ANNEX 2

GLOSSARY OF TERMINOLOGY

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a client 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.

Competent authorities

Competent authorities refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

Designated Non-Financial Businesses and Professions (DNFBPs)

- a. Casinos (which also includes internet casinos).
- 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, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the 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.
 - Acting as (or arranging for another person to act as) a nominee shareholder for another person.

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 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).

FATF Recommendations

Refers to the FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing.

Legal Person

Legal person refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent client relationship with a legal professional or otherwise own property.

Legal Professional

In this Guidance, the term “*Legal professional*” refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Individuals who are or have been entrusted with prominent public functions in 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Self-regulatory organisation (SRO)

A body that represents a profession (*e.g.* lawyers, notaries, other independent legal professionals or accountants), and which is made up of member professionals or a majority thereof, has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

ANNEX 3

MEMBERS OF THE ELECTRONIC ADVISORY GROUP

FATF and FSRB members and observers

Argentina; Asia Pacific Group (APG); Australia; Belgium; Azerbaijan; Canada; Chinese Taipei, China; European Commission (EC); Nigeria; France; Hong Kong, China; Italy; Japan; Luxembourg; MONEYVAL; Netherlands; New Zealand; Offshore Group of Banking Supervisors (OGBS); Portugal; Romania; Spain; South Africa; Switzerland; United Kingdom; United States.

Dealers in precious metals and dealers in precious stones industries

Antwerp World Diamond Centre, International Precious Metals Institute, World Jewellery Confederation, Royal Canadian Mint, Jewellers Vigilance Committee, World Federation of Diamond Bourses, Canadian Jewellers Association.

Real estate industry

International Consortium of Real Estate Agents, National Association of Estate Agents (UK), the Association of Swedish Real Estate Agents.

Trust and company service providers industry

The Society of Trust and Estate Practitioners (STEP), the Law Debenture Trust Corporation.

Accountants

American Institute of Certified Public Accountants, Canadian Institute of Chartered Accountants, European Federation of Accountants, German Institute of Auditors, Hong Kong Institute of Public Accountants, Institute of Chartered Accountants of England & Wales.

Casino industry

European Casino Association (ECA), Gibraltar Regulatory Authority, Kyte Consultants (Malta), MGM Grand Hotel & Casino, Unibet, William Hill plc.

Lawyers and notaries

Allens Arther Robinson, American Bar Association (ABA), American College of Trust and Estate Council, Consejo General del Notariado (Spain), Council of the Notariats of the European Union, Council of Bars and Law Societies of Europe (CCBE), International Bar Association (IBA), Law Society of England & Wales, Law Society of Upper Canada.

CHAPTER 11

Appendix E— FINTRAC Interpretation Notice No. 7

Source: www.fintrac-canafe.gc.ca/publications/FINS/2011-02-17-eng.asp

The screenshot shows the FINTRAC website interface. At the top, there are logos for the Financial Transactions and Reports Analysis Centre of Canada in both French and English, and the Canadian flag. Below this is a navigation bar with links for 'Français', 'Home', 'Contact Us', 'Help', 'Search', and 'Canada.ca'. The main content area is titled 'FINTRAC Interpretation Notice no. 7' and is dated 'February 17, 2011'. The notice is titled 'Insolvency Practitioners Providing Trustee in Bankruptcy Services' and discusses the application of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its regulations to insolvency practitioners offering bankruptcy services. A sidebar on the left contains a table of contents with links to various sections of the website.

FINTRAC	FINTRAC Interpretation Notice no. 7
Who we are	February 17, 2011
Media room	Insolvency Practitioners Providing Trustee in Bankruptcy Services
What you need to know	Paragraph 5(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and subsections 34(1), sections 35 and 36 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.
The Act	The purpose of this notice is to clarify the application of the PCMLTFA relating to insolvency practitioners offering bankruptcy services.
Regulations	Insolvency practitioners provide trustee in bankruptcy services. These services are not triggering activities for any obligations under the PCMLTFA. Trustee in bankruptcy services or insolvency practitioners are not covered as services or as an entity under our legislation. However, if you are an insolvency practitioner and you are an accountant or an accounting firm, you may have obligations relating to other activities.
Guidelines	Insolvency practitioners who are accountants:
Reporting	If you are an individual accountant or an accounting firm offering trustee in bankruptcy services or acting as an insolvency practitioner, you may have obligations under the PCMLTFA if you engage in certain triggering activities other than bankruptcy services. However, as explained above, bankruptcy services you provide as an insolvency practitioner, including acting as a trustee in bankruptcy, do not fall within the triggering activities under our legislation.
Money services businesses registry	Definition of accountants
Penalties	An accountant means a chartered accountant, a certified general accountant or a certified management accountant. An accounting firm means an entity that provides accounting services to the public that has at least one partner, employee or administrator that is an accountant.
Reviews and appeals	
Access to information and privacy protection	
Publications	
Reporting publications	
General publications	
Corporate publications	

Multimedia		
Frequently asked questions	<p>In this context, if you are an insolvency practitioner, whether a chartered insolvency and restructuring professional or otherwise, you would not be considered to be "providing accounting services to the public" if you only provide such services as follows:</p>	
Careers	<ul style="list-style-type: none"> • As receiver, pursuant to the provisions of a Court order or by way of a private letter appointment pursuant to the terms of a security interest • As trustee in bankruptcy • As monitor under the provisions of the Companies' Creditors Arrangement Act or any other proceeding that results in the dissolution or restructuring of an enterprise or individual and to which the firm, individual or insolvency practitioner serves as an officer of the Court or agent to a creditor(s) or the debtor. 	
<p>Triggering activities for accountants</p>		
<p>If you are an accountant or an accounting firm, as explained above, you have obligations under the PCMLTFA if you engage in any of the following activities on behalf of any individual or entity (other than your employer) or give instructions in respect of those activities on behalf of any individual or entity (other than your employer):</p>		
<ul style="list-style-type: none"> • receiving or paying funds; • purchasing or selling securities, real property or business assets or interests; or • transferring funds or securities by any means. 		
<p>In this context, an accountant or an accounting firm appointed by a Court, or acting as a trustee in bankruptcy, is not considered to be acting on behalf of any other individual or entity.</p>		
<p>Obligations under the PCMLTFA, as referred to throughout this interpretation notice, include reporting, client identification, record keeping, and implementing a compliance regime. For more information about these, see FINTRAC's guidelines.</p>		
<hr/>		
<p>Date Modified: 2011-09-20</p>	<p> Top of Page</p>	<p>Terms and Conditions</p>

CHAPTER 12

Appendix F— Sample Receipt of Funds Record

RECEIPT OF FUNDS RECORD

The following information must be collected, retained and recorded for each prescribed transaction where the organization receives funds with a value of CAD 3,000 or more in any form from a client in respect of Triggering Activities.

INFORMATION ON THE INDIVIDUAL FROM WHOM YOU RECEIVED THE FUNDS

Last Name		First Name	
Street Address			Apartment/Unit #
City	Prov.	Postal Code	
Date of Birth	Nature of Principal Business or Occupation		

TRANSACTION INFORMATION

Transaction Date	Amount	Currency
Purpose, Details and Type of Transaction	Other Persons or Entities Involved	
If funds were received in cash, how the cash was received		

IF AN ACCOUNT WAS AFFECTED BY THE TRANSACTION

Account #	Type of Account
Accountholder's Full Name	Currency of Transaction

ENTITY INFORMATION, IF APPLICABLE

Name of Entity	Nature of Principal Business
Street Address	Apartment/Unit #
City	Prov. Postal Code

If the receipt of funds record is about a corporation, you also need to keep a copy of the part of the official corporate records showing the provisions relating to the power to bind the corporation regarding the transaction.

Instructions on completing the Receipt of Funds Record

Information on the person providing the funds should be included on this form and be as specific as possible. Specifically:

- The address should be their physical location and not a PO Box.
- The occupation should be as specific as possible and should avoid vague occupations such as “self-employed,” “consultant” and “import export.”
- The purpose of the transaction should explain the whole transaction such as “received funds from client to wire.”
- If the funds are in cash form, this should be explained using such wording as “in person” “mailed” or “courier.”
- The sections on accounts would be applicable if the funds were received in a form other than cash. For instance, if the client gave you a cheque, the account information related to that cheque should be recorded.
- The section on entity information would be applicable if the client is not an individual. In that case, information on the individual conducting the transaction on behalf of the entity and the information on the entity would both be required.

If the client is an entity that is incorporated, a copy of their record that binds them to the transaction needs to be kept.

CHAPTER 13

Appendix G— Identification of Individuals in Person: Method and Form

13.1 Requirements

A client's identification must be ascertained when any of the following occur as part of an engagement for which Triggering Activities have occurred.

- receipt of funds of \$3,000 or above
- large cash transaction
- suspicious transaction (completed or attempted)

When dealing with an entity, both the entity and the individual conducting the transaction on the entity's behalf must be identified.

13.2 Method

Face-to-face client identification means that you can physically meet the client and can refer to their identification document. For an identification document to be valid, it must include the following:

- Not be prohibited by provincial or territorial legislation for identification purposes.
- Must have a unique identifier number.
- Must have been issued by a provincial, territorial or federal government.
- Cannot have been expired.
- Must be an original and not a copy of the document.

Some examples of identification documents that FINTRAC has provided include:

- Insurance Corporation of British Columbia
- Alberta Registries
- Saskatchewan Government Insurance
- Department of Service Nova Scotia and Municipal Relations
- Department of Transportation and Public Works of the Province of Prince Edward Island
- Service New Brunswick
- Department of Government Services and Lands of the Province of Newfoundland and Labrador
- Department of Transportation of the Northwest Territories
- Department of Community Government and Transportation of the Territory of Nunavut

What information needs to be collected when referring to the identification document?

When you refer to a client's identification document, you must keep a record of the following information:

- The type of identification document.
- The reference number on the identification document.
- The place of issue of the identification document.

You do not need to take a copy of the identification document, as long as you keep the required information about the identification document.

13.3 Form

Collect the following information for each individual (personal) client or for individuals who can authorize a transaction on behalf of the entity.

Acceptable identification must be an original (not a copy), valid (not expired), bear a unique reference number and be issued by a provincial, federal or similar government.

The name and address information here must match the identification documents and the address must be a physical address and not a PO Box or general delivery address.

Last Name		First	
Home Address			Apartment/Unit #
City	Prov.	Postal Code	
Date of Birth	Occupation		
ID Type	<input type="checkbox"/> Driver's License	<input type="checkbox"/> Passport	<input type="checkbox"/> Other (Specify)
ID number	Place of issue (Province or Country)		

EXAMPLES OF ACCEPTABLE IDENTIFICATION DOCUMENTS

- Insurance Corporation of British Columbia
- Alberta Registries
- Saskatchewan Government Insurance
- Department of Service Nova Scotia and Municipal Relations
- Department of Transportation and Public Works of the Province of Prince Edward Island
- Service New Brunswick
- Department of Government Services and Lands of the Province of Newfoundland and Labrador
- Department of Transportation of the Northwest Territories
- Department of Community Government and Transportation of the Territory of Nunavut

CHAPTER 14

Appendix H— Identification of Individuals Non-Face-to-Face: Methods

14.1 Requirements

A client's identification must be ascertained when any of the following occur as part of an engagement for which Triggering Activities have occurred.

- receipt of funds of \$3,000 or above
- large cash transaction
- suspicious transaction (completed or attempted)

When dealing with an entity, both the entity and the individual conducting the transaction on the entity's behalf must be identified.

14.2 Methods

If you are unable to identify a client face-to-face, there are prescribed non-face-to-face methods that can be used. Non-face-to-face identification involves a combination method that gives you the option of selecting two of the following five options.

1. Identification Product Method: Refer to an independent and reliable identification product that is based on personal information and Canadian credit history about the individual of at least six months duration.
2. Credit File Method: With the individual's permission, refer to a credit file. The credit file must have been in existence for at least six months.

3. Attestation Method: Obtain an attestation that an original identification document for the individual has been seen by a commissioner of oaths or a guarantor.
4. Cleared Cheque Method: Confirm that a cheque drawn on a deposit account that the individual has with a financial entity has cleared.
5. Deposit Account Method: Confirm that the individual has a deposit account with a financial entity. This requirement would be specific to an account held with a Canadian financial institution and it must be a deposit account (e.g., a chequing or savings account and not a credit card account). To confirm that a client has a deposit account, you can either receive confirmation from the financial institution or ask your client for a copy of their deposit account statement (paper or electronic versions are both acceptable).

The AML Legislation restricts the type of combinations that you can use depending on the options. The following is a list of combinations that can be used for non-face-to-face client identification:

- identification product and attestation
- identification product and cleared cheque
- identification product and confirmation of deposit account
- credit file and attestation
- credit file and cleared cheque
- credit file and confirmation of deposit account
- attestation and cleared cheque

CHAPTER 15

Appendix I— Identification of Individuals by Third Parties: Methods

15.1 Requirements

A client's identification must be ascertained when any of the following occur as part of an engagement for which Triggering Activities have occurred.

- receipt of funds of \$3,000 or above
- large cash transaction
- suspicious transaction (completed or attempted)

When dealing with an entity, both the entity and the individual conducting the transaction on the entity's behalf must be identified.

15.2 Methods

You can also rely on an agent or mandatary (a person engaged to perform a mandate on your behalf) to conduct client identification for you using the face-to-face method. This requires that you have in place a written agreement with the agent or mandatary that sets out what you expect from them and that you obtain from them the client identification information prior to the performance of the identification function. It is recommended that the effective date of the agreement and the signature of the agent/mandatary and the Accountant or Accounting Firm also be included on the agreement. An agent or mandatary can be any individual or entity.

An agent/mandatary agreement should explicitly state that the agreement is for the purpose of ascertaining client identification on behalf of the Accountant or Accounting Firm under the obligations of the PCMLTFA. It should also describe what will be done to confirm the identification (e.g., original ID will be reviewed and compared to the client to confirm that it is the person in question). It should also obligate the agent/mandatary to remit to the Accountant or Accounting Firm details collected in respect of each identification conducted.

When an agent/mandatary ascertains the client's identification under the agreement, a record should document the client's personal information including their name, address, occupation and date of birth, and details of the identification include the identification type, reference number and place of issue. The form included in Appendix G—Identification of Individuals in Person: Method and Form can be adapted for that purpose.

CHAPTER 16

Appendix J— Confirming the Existence of an Entity

16.1 Requirements

A client's identification must be ascertained when any of the following occur as part of an engagement for which Triggering Activities have occurred.

- receipt of funds of \$3,000 or above
- large cash transaction
- suspicious transaction (completed or attempted)

When dealing with an entity, both the entity and the individual conducting the transaction on the entity's behalf must be identified.

16.2 Method

Where you are required to identify an entity, you must identify that entity within 30 days of the transaction associated to the record. Identifying an entity involves the following:

1. Confirming the existence of the entity.
2. For entities that are corporations
 - a. obtain the corporation's name, address
 - b. the names of its directors

To confirm the existence of the entity, you can refer to following documents:

- partnership agreement
- articles of association
- business registration
- trust agreement

To confirm the existence of a corporation, and the corporation's name and address, you can refer to the following documents:

- corporation's certificate status
- record that has to be filed annually under provincial securities legislation
- letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government
- corporation's published annual report signed by an independent audit firm

If you received funds from an entity, you must obtain and keep a copy of the official corporate records that contains any provisions relating to the power to bind the corporation.

16.3 Form

ENTITY INFORMATION		
Name of Entity		
Street Address		Apartment/Unit #
City	Prov.	Postal Code
Country		
Principal Business		
Names of Directors (if entity is a corporation)		
COPY OF RECORD CONFIRMING EXISTENCE OF ENTITY		
To confirm the existence of a Corporation, refer to the articles of incorporation, certification of corporate status, published annual report or government notice of assessment.		
To confirm the existence of an entity that is not a corporation, refer to partnership agreement, articles of association or applicable documentation that confirms the formation/existence of the entity.		
If record is paper format, a copy must be kept. If electronic version, a record of the entity's registration number and type and source of record must be indicated on this form.		
If you received funds from an entity, you must obtain and keep a copy of the official corporate records that contains any provisions relating to the power to bind the corporation.		
Type of entity		
Type of verification record		
Source of verification record		
Registration number of entity		

CHAPTER 17

Appendix K— Large Cash Transaction Report Form

This form is reproduced with permission from the Financial Transactions and Reports Analysis Centre of Canada and was up-to-date at the time of printing. As this form may change, we recommend you check the website to ensure you are using the latest version.

Source: www.fintrac-canafe.gc.ca/publications/LCTR-2008-eng.pdf

NOTE: Please copy this page for each additional, related, disposition (per transaction) (if required).

Transaction Disposition of

PART B2 — Information about how the transaction was completed

Indicate whether this transaction was conducted on behalf of anyone other than the individual who conducted it. If not, indicate "not applicable."

On behalf of: not applicable an entity (other than an individual) (also complete PART F) another individual (also complete PART G) employee depositing cash to employer's business account

8. Disposition of funds*

<input type="checkbox"/> Cash out	<input type="checkbox"/> Outgoing electronic funds transfer	<input type="checkbox"/> Purchase of jewellery	<input type="checkbox"/> Purchase of traveller's cheques
<input type="checkbox"/> Conducted currency exchange	<input type="checkbox"/> Purchase of bank draft	<input type="checkbox"/> Purchase of money order	<input type="checkbox"/> Real estate purchase/deposit
<input type="checkbox"/> Deposit to an account	<input type="checkbox"/> Purchase of casino chips	<input type="checkbox"/> Purchase of precious metals	<input type="checkbox"/> Securities purchase/deposit
<input type="checkbox"/> Life insurance policy purchase/deposit	<input type="checkbox"/> Purchase of diamonds	<input type="checkbox"/> Purchase of precious stones (excluding diamonds)	<input type="checkbox"/> Other _____ <small>DESCRIPTION (OTHER)</small>

POLICY NUMBER _____

9. Amount of disposition*

10. Disposition currency code* — Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper*.

Additional information about the funds described in field 8 above

11. Other institution name and number or other entity or person name* (if applicable)

12. Other entity or person account number or policy number* (if applicable)



NOTE: Please copy this page for each additional disposition (if applicable).

PART C — Account information, if the transaction involved an account

Transaction Disposition

Complete this Part ONLY if the transaction involved an account.

1. Branch or transit number where the account is held* (if this part is applicable)

2. Account number* (if this part is applicable)

3. Type of account* (if this part is applicable)

Personal Business Trust Other _____
DESCRIPTION (OTHER)

4. Account currency code* (if this part is applicable) — Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper.*

5. Full name of each account holder (the individual(s) or the entity that hold the account)* (if this part is applicable)

1) _____

2) _____

3) _____



NOTE: Please copy this page for each additional transaction (if applicable).

Transaction

PART D — Information about the individual conducting the transaction if it is not a deposit into a business account (if applicable)

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for any mandatory fields in this part was not obtained at the time of the transaction (and is not available from your records), you can leave those fields blank.

1. Surname* (if this part is applicable) 2. Given name* (if this part is applicable) 3. Other/Initial

4. Client number assigned by reporting entity* (if applicable and if this part is applicable)

5. Street address* (if this part is applicable)

6. City* (if this part is applicable)

7. Province or State* (if this part is applicable) 8. Country* (if this part is applicable)

9. Postal or Zip code* (if this part is applicable)

10. Country of residence

11. Home telephone number (with area code)

12. Individual's identifier* (if this part is applicable)

Birth certificate Driver's licence Passport Provincial health card Record of landing / Permanent resident card

Other DESCRIPTION (OTHER)

13. ID number (from question 12)* (if this part is applicable)

14. Place of issue – Province or State* (if this part is applicable) 15. Place of issue – Country* (if this part is applicable)

16. Individual's date of birth* (if this part is applicable)

YEAR MONTH DAY

17. Individual's occupation* (if this part is applicable)

18. Individual's business telephone number (with area code) 18A. Telephone extension number



NOTE: Please copy this page for each additional transaction (if applicable).

Transaction

**PART E — Information about the individual conducting the transaction if it is a deposit into a business account —
other than a night deposit or quick drop (if applicable)**

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for any mandatory fields in this part was not obtained at the time of the transaction (and is not available from your records), you can leave those fields blank.

1. Surname* (if this part is applicable)

2. Given name* (if this part is applicable)

3. Other/Initial



NOTE: Please copy this page for each additional disposition (if required).

Transaction Disposition

PART F — Information about the entity on whose behalf the transaction was conducted (if applicable)

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for any mandatory fields in this part was not obtained at the time of the transaction (and is not available from your records), you can leave those fields blank.

1. Name of corporation, trust or other entity* (if this part is applicable)

2. Type of business* (if this part is applicable)

3. Street address* (if this part is applicable)

4. City* (if this part is applicable)

5. Province or state* (if this part is applicable)

6. Country* (if this part is applicable)

7. Postal or Zip code* (if this part is applicable)

8. Business telephone number (with area code)

8A. Telephone extension number

9. Incorporation number* (if applicable and if this part is applicable)

10. Place of issue – Province or State* (if applicable and if this part is applicable)

11. Place of issue – Country* (if applicable and if this part is applicable)

12. Individual(s) authorized to bind the entity or act with respect to the account (up to three)

1 _____

2 _____

3 _____



NOTE: Please copy this page for each additional disposition (if required).

Transaction Disposition

PART G — Information about the individual on whose behalf the transaction was conducted (if applicable)

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for any mandatory fields in this part was not obtained at the time of the transaction (and is not available from your records), you can leave those fields blank.

1. Surname* (if this part is applicable) _____ 2. Given name* (if this part is applicable) _____ 3. Other/Initial _____

4. Street address* (if this part is applicable) _____

5. City* (if this part is applicable) _____

6. Province or State* (if this part is applicable) _____ 7. Country* (if this part is applicable) _____

8. Postal or Zip code* (if this part is applicable) _____

9. Home telephone number (with area code) _____

10. Business telephone number (with area code) _____ 10A. Telephone extension number _____

11. Individual's date of birth
YEAR MONTH DAY

12. Individual's identifier
 Birth certificate Driver's licence Passport Provincial health card Record of landing / Permanent resident card
 Other _____
DESCRIPTION (OTHER)

13. ID number (from question 12) _____ 14. Country of residence _____

15. Place of issue of individual's identifier – Province or State _____ 16. Place of issue of individual's identifier – Country _____

17. Individual's occupation _____

Relationship
 18. Relationship of the individual named in Part D or Part E to the individual named above (fields 1 to 3)
 Accountant Borrower Customer Friend Relative
 Agent Broker Employee Legal counsel Other _____
DESCRIPTION (OTHER)

The information on this form is collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act). It will be used for analytical purposes and may also be used for the purposes of ensuring compliance with the Act. Any personal information is protected under the provisions of the *Privacy Act*. For more information, consult the Financial Transactions and Reports Analysis Centre of Canada chapter in the *Sources of Federal Government Information* publication, available on the Government of Canada Info Source Web site (<http://www.infosource.gc.ca>).

Source: www.fintrac-canafe.gc.ca/publications/guide/Guide7B/7b-eng.asp#s441

5. Instructions for Completing a Large Cash Transaction Report

The fields in this section correspond with the paper form called the Large Cash Transaction Report. As explained in section 3.4, completing a paper report is only permitted if you do not have the capability to report electronically.

Fields in reports are either mandatory, mandatory where applicable, or require "reasonable efforts" to complete, as follows:

- **Mandatory:** All fields of a report marked with an asterisk (*) **have to be completed.**
- **Mandatory where applicable:** The fields that have both an asterisk and "where applicable" next to them have to be completed if they are applicable to you or the transaction being reported.
- **Reasonable efforts:** For all other fields that do not have an asterisk, you have to make reasonable efforts to get the information. "Reasonable efforts" means that you tried to get the information requested on the report. If the information is available to you, you must provide it in the report. If the information was not available at the time of the transaction, and it is not contained in your files or records, the field may be left blank.

In certain circumstances, only as directed in the instructions for certain fields, if you need to indicate that a required field in a report is not applicable, enter "N/A" or "n/a". Do not substitute any other abbreviations, special characters (e.g., "x", "-" or "***") or words (e.g., unknown).

As explained in subsection 3.1, a large cash transaction report can be about multiple transactions of less than \$10,000 each conducted within 24 consecutive hours of each other that add up to \$10,000 or more. Because those individual transactions were under \$10,000, the information for some mandatory fields in the report may not be available in your records or from the time of the transaction. In this case, "reasonable efforts" applies to those otherwise mandatory fields.

There are eight parts to the large cash transaction report, but some are only to be completed if applicable. To report a large cash transaction follow the following four steps:

- **Step 1** - Complete Part A to provide information about the reporting entity and about where the transaction took place.
- **Step 2** - Complete Part B1 to provide details about the transaction. If you have to include more than one transaction in your report (for cash transactions of less than \$10,000 each made within 24 consecutive hours of each other that total \$10,000 or more), repeat steps 2, 3 and 4 for each one.

If the transaction was a night deposit or a quick drop to a business account, make sure to indicate this in field B3.

- **Step 3** - Complete Part B2 to provide details about the transaction's disposition. If the transaction's disposition was related to an account, also complete Part C. If the transaction's disposition was on behalf of a corporation or other entity (other than an employee depositing cash into his or her employer's business account), also complete Part F. If the transaction's disposition was on behalf of an individual (other than an employee depositing cash into his or her employer's business account), complete Part G.

If there was more than one disposition for the transaction, repeat this step for each disposition.

- **Step 4** - Complete Part D or E to provide information about the individual conducting the transaction, depending on whether or not the transaction's disposition was a deposit to a business account. If the transaction had no other dispositions than deposits to a business account, complete Part E. If the transaction involved a disposition that was **not** a deposit to a business account, complete Part D. However, if the transaction was a night deposit or a quick drop to a business account, **neither** Part D nor Part E is required.

The rest of this section will cover each part of the Large Cash Transaction Report form.

When completing the paper form, enter the date and time when you begin completing it at the top of the form. If you have to file a correction to a report on paper, follow the instructions on the first page of the form. If you need to get a paper form, see [section 4](#).

24-hour-rule

If this report is about one transaction of \$10,000 or more, answer **no** to the 24-hour-rule question. In this case, your report should only include one transaction.

If this report is about a transaction that is part of a group of two or more cash transactions of less than \$10,000 each made within 24 consecutive hours of each other that total \$10,000 or more, answer **yes** to the 24-hour-rule question. Include each such transaction in the same large cash transaction report, unless they were not all conducted at the same location. If the transactions in such a group were conducted at different locations, separate large cash transaction reports would be required to group them for each location.

Part A: Information about where the transaction took place

This part is for information about the reporting entity required to report the transaction to FINTRAC. It is also for information about the physical location where the transaction took place.

If you need more information about what type of individual or entity is a reporting entity, see section 2 of this guideline.

If you have multiple branch or office locations, the information in this part should refer to the branch or office location where the transaction took place. Transactions that happened at different branch or office locations should be reported on separate reports.

Some reporting entities have contractual arrangements with someone outside their entity to conduct transactions on their behalf. For example, a money services business arranges for transactions, such as electronic funds transfers, to be conducted for them at a grocery store. If you have this type of arrangement, as the reporting entity, your name belongs in Part A. However, since the transaction was conducted at someone else's place of business, it is that address that must appear in Part A.

Field A1* Reporting entity's identifier number (if applicable)

This is the institution or licence number, or other identification number for the reporting entity, as outlined below. If you are a reporting entity that has multiple branch or office locations, the identification number should refer to the branch or office where the transaction took place.

- If you are an **accountant**, enter your provincial chartered accountant (CA), provincial certified management accountant (CMA), or provincial certified general accountant (CGA) number.
- If you are a **bank, caisse populaire, cooperative credit society or credit union**, enter your financial institution number issued by the Canadian Payments Association (CPA).
- If you are an **agent of the Crown that sells or redeems money orders**, enter your post office or similar number.
- If you are a **life insurance broker or agent**, enter your provincial broker or agent licence number.
- If you are a **federally regulated life insurance company**, enter your Office of the Superintendent of Financial Institutions (OSFI) Institution Code.
- If you are a **life insurance company that is not federally regulated**, enter your provincial licence number.
- If you are a **provincial savings office**, enter your financial institution number issued by the CPA.
- If you are a **real estate broker or sales representative**, enter your provincial broker number.
- If you are a **securities dealer**, enter your provincial dealer licence number.
- If you are a **trust and loan company**, enter your financial institution number issued by the CPA.
- If you are a **provincial trust and loan** that is not a member of the CPA, enter your registration number.
- If you are a **money services business**, enter your money services business registration number issued by FINTRAC.
- If you are a **dealer in precious metals and stones**, leave this field blank.
- If you are a **British Columbia public notary**, enter your membership number. If you are a **notary corporation of British Columbia**, enter your permit number.
- If you are a **real estate developer**, enter your provincial licence number if you have one. Otherwise, leave this field blank.

Field A2* Reporting entity's full name

Enter the full legal name of the business or corporation that is the reporting entity. If you are a reporting entity that does not have a business name (for example, you are a reporting entity that is an individual), enter your full name.

Fields A3* to A6* Reporting entity's full address

Enter the civic address, town or city, province and postal code where the transaction took place. If you have more than one location, this information should refer to where the transaction took place. As explained above, transactions that happened at different branch or office locations should be reported on separate reports.

Field A6A Reporting entity report reference number

If you use a reference number for your own internal purposes, you can enter it in your report to FINTRAC. This field can contain up to 20 alpha or numeric characters and must be unique for each of your reporting entity's reports.

If you do not wish to use such an internal reference number, leave this field empty.

Fields A7*, A8* and A9 Contact name

Enter the name of the individual FINTRAC can contact for clarification about this report.

Field A10* Contact telephone number

Enter the telephone number, including the area code, of the individual FINTRAC can contact for clarification. Include the extension, if applicable, in field A10A.

Field A11* Which one of the following types of reporting entities best describes you?

Enter the type of activity applicable to you. If you are involved in more than one activity type, indicate the one applicable to the transaction being reported. If there is more than one activity for one or more transactions on the report, check only one box to indicate your principal type of activity.

Part B1: Information about how the transaction was initiated

This part is for information about how the transaction was initiated (i.e., where the money came from).

You should make separate large cash transaction reports for each single transaction of \$10,000 or more.

If you are reporting two or more cash transactions of less than \$10,000 each made by or on behalf of the same individual within 24 consecutive hours of each other that total \$10,000 or more, you should group those in the same report. If the information in Part A is different for any of those multiple transactions, however, you will have to send separate reports to group them by location.

When you need to report more than one transaction, complete a separate Part B1 for each transaction. To do this, you can copy Part B1. Fill in the "Transaction ___ of ___" area at the top of Part B1 to distinguish between each transaction. When you provide the details of the transaction in Part D or E, the details of disposition in Part B2, as well as the additional details of disposition in Parts C, F and G, as applicable, indicate to which transaction that information applies.

Fields B1*, B2 and B3* When the transaction took place

Enter the date (yyyy-mm-dd) and time (hh:mm:ss) of the large cash transaction. Use a 24-hour format for time. For example, enter "15:30:00" to represent 3:30 p.m.

The time of the transaction (field B2) can be left blank if it is not available from the moment of the transaction or in your records.

The date of transaction (field B1) is mandatory. However, if the transaction was a night deposit, and you do not provide the date, you can leave field B1 blank. In this case, make sure to use the night deposit indicator at field B3 and make sure to provide the date of posting in field B4.

If the transaction was either a **night deposit** or a **quick drop** to a business account, make sure to select the appropriate indicator at field B3. In this case, neither of Parts D, E, F or G will apply to the transaction.

Field B4 Date of posting

Enter the date (yyyy-mm-dd) the transaction cleared, if this differs from the date of the transaction provided in field B1. In the case of a night deposit, if you do not provide the date of transaction at field B1, you must provide the date of posting for the transaction in field B4.

Field B5* Amount of transaction

Enter the total amount of cash involved in the transaction. This is the total cash amount received to start the transaction. What happens as a result of that cash amount will be explained in Part B2 as one or more dispositions.

If this cash was not in Canadian funds, you do not have to convert it, but you have to provide the currency information in field B6.

Field B6* Transaction currency code

Enter the code for the type of currency for the transaction. Enter CAD if Canadian dollars, or USD for United States dollars. If the transaction was in another type of currency, see the list of currency codes in Appendix 1 in *Guideline 38: Submitting Suspicious Transaction Reports to FINTRAC by Paper*.

Field B7* How was the transaction conducted?

Check the appropriate box to indicate how the transaction was conducted. For example, if the transaction was done through an automated banking machine, check that box. If the selections provided do not cover this particular transaction, indicate "Other" and provide details in the field provided.

Part B2: How the transaction was completed

This part is for information about how the transaction was completed (i.e., where the money went).

"On behalf of" indicator

At the top of Part B2, you have to indicate whether the individual who conducted the transaction was doing so on anyone else's behalf. You have to select one of the following for this entry:

- **Not applicable**

This means that **neither** Part F **nor** Part G applies to this report. "Not applicable" indicates that none of the other "On behalf of" selections is applicable to the transaction. For example, the disposition was not on anyone else's behalf (i.e., it was on behalf of the individual that conducted it).

- **On behalf of an entity**

This indicates that the disposition was on behalf of an entity, such as a business, a partnership, a corporation, a trust or other entity, but was **not** an employee depositing cash to his or her employer's business account. For a transaction that was conducted on behalf of an entity, complete Part F for this report to provide the information about that entity.

- **On behalf of another individual**

This indicates that the disposition was on behalf of another individual but was **not** an employee depositing cash to his or her employer's business account. For a transaction that was conducted on behalf of another individual, complete Part G to provide the information about that other individual.

- **Employee depositing cash to employer's business account**

This indicates that the disposition was an employee depositing cash to his or her employer's **business** account. If it was an employee depositing cash to his or her employer's business account, **neither** Part F **nor** Part G of this report applies. Do not use this indicator if the employee deposited other than cash or if the employer's account was other than a business account.

Unless the transaction was a night deposit or a quick drop, you have to provide information about the individual conducting the transaction in Part D or Part E. If the transaction had no other dispositions than a deposit to a business account, complete Part E. If the transaction involved a disposition that was **not** a deposit to a business account, complete Part D. If the transaction was a night deposit or a quick drop, neither of Parts D, E, F or G applies.

More than one disposition

There could be more than one disposition for a particular transaction. For example, your client could initiate a transaction in cash, send an electronic funds transfer (EFT) for part of it (disposition 1), order a bank draft for another part (disposition 2) and deposit the rest (disposition 3). In that case, make sure you include the information for each disposition. If you are including more than one transaction in this report (for cash transactions of less than \$10,000 each made within 24 consecutive hours of each other that total \$10,000 or more), you have to complete Part B2 for all dispositions for each transaction.

If you have to include more than one disposition, complete a separate Part B2 for each one. To do this, you can copy Part B2. Fill in the "Transaction ____ Disposition ____ of ____" area at the top of Part B2 to distinguish between each disposition. If you have to include more than one transaction in this report, indicate to which transaction the disposition information applies, based on the number you assigned the transaction in Part B1. When you provide the details of disposition in Parts C, F and G, as applicable, also indicate to which disposition and which transaction that information applies.

Field B8* Disposition of funds

This describes what happened to the funds involved in the transaction.

If the disposition of funds was a life insurance policy purchase or deposit, check that box and provide the life insurance policy number in the appropriate field. If the selections provided do not cover this particular disposition, indicate "Other" and provide details in the appropriate field.

If the transaction being reported was an employee depositing cash to an employer's business account (as indicated by the "on behalf of" indicator at the top of Part B2), the disposition of funds in field B8 should be "deposit to an account".

If you are a dealer in precious metals and stones, select the disposition of funds in field B8 that best describes what your client purchased.

Field B9* Amount of disposition

Enter the amount of funds involved in the disposition. If the amount was not in Canadian funds, you do not have to convert it but you have to provide the currency code in field B10.

Field B10* Disposition currency code

Enter the code for the type of currency for the disposition. Enter CAD if Canadian dollars, or USD for United States dollars. If the transaction was in another type of currency, see the list of currency codes in Appendix 1 in *Guideline 38: Submitting Suspicious Transaction Reports to FINTRAC by Paper*.

Fields B11* and 12* Other institution, entity or person name, number and account or policy number (if applicable)

These fields are for additional information about the disposition described in field B8. Where applicable, in field B11, provide the name (including the institution identification number if applicable) of any other institution, individual or entity involved in the disposition. In addition, where applicable, in field B12, provide the account number of any other individual or entity involved in the disposition. Also provide any policy number related to the other entity or individual in field B12, if applicable.

Part C : Account information, if the transaction involved an account

This part is for information about the account involved in the transaction, if it in fact involved an account. As explained earlier, it is possible to have more than one transaction per report and more than one disposition per transaction. Provide the account information, if applicable, for each disposition included in the report.

If you have to include account information for more than one disposition, complete a separate Part C to provide information for each account involved. To do this, you can copy Part C. Fill in the "Transaction ____ Disposition ____" area at the top of Part C to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Field C1* Branch or transit number where the account is held (if this part is applicable)

Enter the branch number, transit number or other appropriate identifying number of the entity where the relevant account is held, if an account is applicable to the transaction.

Field C2* Account number (if this part is applicable)

Enter the number of the relevant account.

Field C3* Type of account (if this part is applicable)

Indicate the type of the relevant account. For example, a business account would be one that, at the time it was opened, was for a business or for a non-profit organization, etc. (i.e., other than a personal or trust account). If the selections "personal, business or trust" do not cover this particular account, indicate "Other" and provide details in the appropriate field.

If the transaction being reported was an employee depositing cash to an employer's business account (as indicated by the "on behalf of" indicator at the top of Part B2), the account type in field C3 should be "business".

Field C4* Account currency code (if this part is applicable)

Enter the code for the type of currency for the relevant account. Enter CAD if Canadian dollars, or USD for United States dollars. If the account is another type of currency, see the list of currency codes in Appendix 1 in *Guideline 38: Submitting Reports to FINTRAC by Paper*.

Field C5* Full name of the individual(s) or entity that hold the account (if this part is applicable)

Enter the full name of each account holder (up to three).

This is for information about each individual or entity that holds the account. For example, in the case of a joint account for husband and wife, include the names of each spouse at field C5.

The account holder might be different from the individual(s) authorized to give instructions for the account. For example, an account for a corporation will have one or more individuals authorized to give instructions for that account. In this case, it is the name of the corporation that holds the account that is required in field C5. Information about individuals authorized to bind the entity or to act with respect to the account belongs in Part F, if applicable, in field F12.

Part D: Information about the individual conducting the transaction if it is not a deposit into a business account (if applicable)

This part is for information about the individual who conducted the transaction if any of this transaction's dispositions was **not** a deposit into a business account. If the transaction involved nothing other than deposits to a business account, complete Part E.

If the transaction was a night deposit or a quick drop to a business account, neither of Parts D, E, F or G applies.

As explained earlier, it is possible to have more than one transaction per report. Provide information about the individual who conducted the transaction in either Part D or Part E, as appropriate, for each transaction included in the report. Fill in the "Transaction ____" area at the top of Part D to distinguish between each transaction, based on the number you assigned the transaction in Part B1.

If you are a dealer in precious metals and stones, the conductor of the transaction is the individual from whom you bought or to whom you sold precious metals or stones.

Fields D1*, D2* and D3 Individual's full name (if this part is applicable)

Enter the last name, first name and middle initial (if applicable) of the individual who conducted the transaction.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields D1 and D2 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field D4* Entity client number (if applicable and if this part is applicable)

Enter the client number you issued to the individual who conducted the transaction, if applicable.

Fields D5* to D9* Individual's full address (if this part is applicable)

Enter the civic address, town or city, province or state, country and postal code of the individual who conducted the transaction.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields D5 to D9 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field D10 Country of residence

Enter the country of permanent residence of the individual who conducted the transaction.

Field D11 Home telephone number

Enter the home telephone number, including the area code, of the individual who conducted the transaction.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field D12* Individual's identifier (if this part is applicable)

Check the appropriate box to show the document used to identify the individual who conducted the transaction.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in the appropriate field.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field D12, but do not provide the number in field D13.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field D12 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Field D13* ID Number (if this part is applicable)

Enter the number of the document described in field D12 that was used to identify the individual who conducted the transaction. Remember that a health card number is not acceptable for this purpose in some provinces. Furthermore, as explained above, a SIN should not be provided on this form. If the identifier document in field D12 (and D12A) is a SIN card, enter "N/A" in field D13 to indicate the number is not applicable.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field D13 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Fields D14* and D15* Place of issue (if this part is applicable)

Enter the province or state and country of issue of the document used to identify the individual who conducted the transaction. If the document was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields D14 and D15 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field D16* Individual's date of birth (if this part is applicable)

Enter the date (yyyy-mm-dd) of birth of the individual who conducted the transaction.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field D16 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Field D17* Individual's occupation (if this part is applicable)

Enter the occupation of the individual who conducted the transaction.

Be as descriptive as possible regarding occupation. Provide information that clearly describes it, rather than use a general term. For example, in the case of a consultant, the occupation should reflect the area of consulting, such as "IT consultant" or "consulting forester". As another example, in the case of a professional, the occupation should reflect the nature of the work, such as "petroleum engineer" or "family physician".

If the individual is not employed or engaged in any type of business or profession, provide information that best describes their situation, such as "student", "unemployed", "retired", etc.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field D17 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Field D18 Individual's business telephone number

Enter the business telephone number, including the area code, of the individual who conducted the transaction. Include the extension if applicable in field D18A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Part E: Information about the individual conducting the transaction if it is a deposit into a business account - other than a quick drop or night deposit (if applicable)

This part is for information about the individual who conducted the transaction if this transaction had no other dispositions than **deposits into a business account**. As explained earlier, it is possible to have more than one transaction per report. Provide this information for each transaction included in the report. Fill in the "Transaction ____" area at the top of Part E to distinguish between each transaction, based on the number you assigned the transaction in Part B1.

If the transactions involved any disposition that was not a deposit to a business account, complete Part D. If the transaction was a night deposit or a quick drop to a business account, neither of Parts D or E applies.

Fields E1*, E2* and E3 Individual's full name (if this part is applicable)

Enter the last name, first name and middle initial (if applicable) of the individual who conducted the transaction.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields E1 and E2 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Part F: Information about the entity on whose behalf the transaction was conducted (if applicable)

This part only applies if the transaction's disposition was conducted on behalf of a third party that is an entity, as indicated in Part B2. If an employee deposited cash in his or her employer's business account, or if the transaction was a deposit to a business account by night deposit or quick drop, Part F does not apply.

Complete a separate Part F for each disposition that was conducted on behalf of an entity. To do this, you can copy Part F. Fill in the "Transaction ____ Disposition ____" area at the top of Part F to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Field F1* Name of corporation, trust or other entity (if this part is applicable)

Enter the full name of the business, corporation, trust or other entity on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field F1 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Field F2* Type of business (if this part is applicable)

Describe the type of business or entity on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field F2 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Field F2* Type of business (if this part is applicable)

Describe the type of business or entity on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for field F2 was not obtained at the time of the transaction (and is not available from your records), you can leave this field blank.

Fields F3* to F7* Full address of entity (if this part is applicable)

Enter the civic address, town or city, province or state, country and postal code of the business, corporation or other entity on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields F3 to F7 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field F8 Business telephone number

Enter the telephone number, including the area code, of the business, corporation or other entity on whose behalf the transaction was conducted. Include the extension, if applicable, at field F8A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Fields F9* to F11* Incorporation information (if applicable and if this part is applicable)

If the transaction was conducted on behalf of an entity that is a corporation, provide the incorporation number. Also provide the province or state, and country of the incorporation number's place of issue. If an incorporation number does not exist for the corporation, enter "N/A" in fields F9, F10 and F11. If the incorporation number was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields F9, F10 and F11 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field F12 Individual(s) authorized to bind the entity or act with respect to the account (up to three)

Provide the names of up to three individuals who have authority to bind the entity or conduct transactions through the account.

Part G: Information about the individual on whose behalf the transaction was conducted (if applicable)

This part only applies when the transaction's disposition was conducted on behalf of a third party that is an individual, as indicated in Part B2.

If the individual conducted the transaction's disposition on his or her own behalf, this part does not apply. In that case, see Part D or Part E.

If an employee deposited cash in his or her employer's business account, or if the transaction was a deposit to a business account by night deposit or quick drop, Part G does not apply. If the transaction's disposition was conducted on behalf of an entity (such as a business, a partnership, a corporation, etc.), see Part F.

Complete a separate Part G for each disposition that was conducted on behalf of an individual. To do this, you can copy Part G. Fill in the "Transaction ____ Disposition ____" area at the top of Part G to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Fields G1*, G2* and G3 Individual's full name (if this part is applicable)

Enter the last name, first name and middle initial (if applicable) of the individual on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields G1 and G2 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Fields G4* to G8* Individual's full address (if this part is applicable)

Enter the civic address, town or city, province or state, country and postal code of the individual on whose behalf the transaction was conducted.

If the transaction is reportable as one of multiple cash transactions of less than \$10,000 each and, because of this, information for fields G4 to G8 was not obtained at the time of the transaction (and is not available from your records), you can leave these fields blank.

Field G9 Home telephone number

Enter the home telephone number, including the area code, of the individual on whose behalf the transaction was conducted.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field G10 Business telephone number

Enter the business telephone number, including the area code, of the individual on whose behalf the transaction was conducted. Include the extension if applicable at field G10A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field G11 Individual's date of birth

Enter the date of birth (yyyy-mm-dd) of the individual on whose behalf the transaction was conducted.

Field G12 Individual's identifier

Check the appropriate box to show the document used to identify the individual on whose behalf the transaction was conducted.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in the appropriate field.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field G12, but do not provide the number in field G13.

Field G13 ID number

Enter the number of the document described in field G12 that was used to identify the individual on behalf of whom the transaction was conducted. Remember that a health card number is not acceptable for this purpose in some provinces. Furthermore, as explained above, a SIN should not be provided on this form. If the identifier document in field G12 (and G12A) is a SIN card, enter "N/A" in field G13 to indicate the number is not applicable.

Field G14 Country of residence

Enter the country of permanent residence of the individual on whose behalf the transaction was conducted.

Fields G15 and G16 Place of issue of the individual's identifier

Enter the province or state, and country of issue of the document used to identify the individual on whose behalf the transaction was conducted. If the document was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

Field G17 Individual's occupation

Enter the occupation of the individual on whose behalf the transaction was conducted.

Be as descriptive as possible regarding occupation. Provide information that clearly describes it, rather than use a general term. For example, in the case of a consultant, the occupation should reflect the area of consulting, such as "IT consultant" or "consulting forester". As another example, in the case of a professional, the occupation should reflect the nature of the work, such as "petroleum engineer" or "family physician".

If the individual is not employed or engaged in any type of business or profession, provide information that best describes their situation, such as "student", "unemployed", "retired", etc.

Field G18 Relationship of the individual named in Part D or Part E to the individual named above

Check the appropriate box to indicate the relationship of the individual conducting the transaction to the individual on whose behalf the transaction was conducted.

If the selections provided do not cover the relationship, indicate "Other" and provide details in the appropriate field.

CHAPTER 18

Appendix L— Suspicious Transaction Report Form

This form is reproduced with permission from the Financial Transactions and Reports Analysis Centre of Canada and was up-to-date at the time of printing. As this form may change, we recommend you check the website to ensure you are using the latest version.

Source: www.fintrac-canafe.gc.ca/publications/STR-2008-eng.pdf

NOTE: Please copy this page for each additional, related, suspicious transaction (if required).

Transaction of

PART B1 — Information about how the transaction was initiated

If the transaction being reported was attempted and, because of this, information for any mandatory fields in this part is not available, you can leave those fields blank.

1. Date of the transaction* 2. Time of the transaction 4. Date of posting (if different from date of transaction)

YEAR MONTH DAY HOUR MINUTES SECONDS YEAR MONTH DAY

2 | 0 2 | 0

or

3. Night deposit indicator*
 If the transaction was **not** a night deposit, leave this box empty.

5. Detail of funds involved in initiating the transaction*

<input type="checkbox"/> Cash in	<input type="checkbox"/> Negotiated bank draft	<input type="checkbox"/> Negotiated securities	<input type="checkbox"/> Real estate
<input type="checkbox"/> Diamonds	<input type="checkbox"/> Negotiated cheque	<input type="checkbox"/> Negotiated traveller's cheques	<input type="checkbox"/> Redeemed casino chips
<input type="checkbox"/> Incoming electronic funds transfer	<input type="checkbox"/> Negotiated life insurance policy	<input type="checkbox"/> Precious metals	<input type="checkbox"/> Withdrawal from account
<input type="checkbox"/> Jewellery	<input type="checkbox"/> Negotiated money order	<input type="checkbox"/> Precious stones (excluding diamonds)	<input type="checkbox"/> Other <input type="text"/>

6. Amount of transaction*

7. Transaction currency code* — Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper.*

Additional information about the funds described in field 5 above

8. Other institution name and number or other entity or person name* (if applicable)

9. Other entity or person account number* (if applicable)

10. How was the transaction conducted?*

<input type="checkbox"/> Armoured car	<input type="checkbox"/> In-branch/Office/Store	<input type="checkbox"/> Quick drop
<input type="checkbox"/> Automated banking machine	<input type="checkbox"/> Mail deposit	<input type="checkbox"/> Telephone
<input type="checkbox"/> Courier	<input type="checkbox"/> Night deposit	<input type="checkbox"/> Other <input type="text"/>

11. ID number of the person initially identifying a suspicious transaction
 →

NOTE: Please copy this page for each additional, related, disposition (per transaction) (if required).

Transaction Disposition of

PART B2 — Information about how the transaction was completed

If the transaction being reported was attempted and, because of this, information for any mandatory fields in this part is not available, you can leave those fields blank.

Indicate whether this transaction was conducted on behalf of anyone other than the individual who conducted it. If not, indicate "not applicable."

On behalf of: **not applicable** **another individual** (also complete PART F)
 an entity (other than an individual) **employee depositing cash to employer's business account**
(also complete PART E)

12. Disposition of funds*

<input type="checkbox"/> Cash out	<input type="checkbox"/> Outgoing electronic funds transfer	<input type="checkbox"/> Purchase of jewellery	<input type="checkbox"/> Purchase of traveller's cheques
<input type="checkbox"/> Conducted currency exchange	<input type="checkbox"/> Purchase of bank draft	<input type="checkbox"/> Purchase of money order	<input type="checkbox"/> Real estate purchase/deposit
<input type="checkbox"/> Deposit to an account	<input type="checkbox"/> Purchase of casino chips	<input type="checkbox"/> Purchase of precious metals	<input type="checkbox"/> Securities purchase/deposit
<input type="checkbox"/> Life insurance policy purchase/deposit	<input type="checkbox"/> Purchase of diamonds	<input type="checkbox"/> Purchase of precious stones (excluding diamonds)	<input type="checkbox"/> Other _____ <small>DESCRIPTION (OTHER)</small>

_____ POLICY NUMBER

13. Amount of disposition*

14. Disposition currency code* — Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper*.

Additional information about the funds described in field 12 above

15. Other institution name and number or other entity or person name* (if applicable)

16. Other entity or person account number or policy number* (if applicable)



NOTE: Please copy this page for each additional disposition (if applicable).

PART C — Account information, if the transaction involved an account

If the transaction being reported was attempted and, because of this, information for any mandatory fields in this part is not available, you can leave those fields blank.

Transaction Disposition

Complete this Part ONLY if the transaction involved an account.

- 1. Branch or transit number where the account is held* (if this part is applicable)
- 2. Account number* (if this part is applicable)

- 3. Type of account* (if this part is applicable)

Business
 Personal
 Trust
 Other (DESCRIPTION (OTHER))

- 4. Account currency code* (if this part is applicable) — Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper.*

- 5. Full name of each account holder (the individual (s) or entity that hold the account)* (if this part is applicable)

1) _____

2) _____

3) _____

- 6. Date opened

YEAR MONTH DAY

- 7. Date closed

2 | 0 YEAR MONTH DAY

- 8. Status of the account at the time the transaction was initiated* (if this part is applicable)

Active
 Inactive
 Dormant



NOTE: Please copy this page for each additional transaction (if applicable).

PART D — Information about the individual conducting the transaction

Transaction

1. Surname 2. Given name 3. Other/Initial

4. Client number assigned by reporting entity* (if applicable)

5. Street address

6. City

7. Province or State 8. Country

9. Postal or Zip code

10. Country of residence 10A. Country of citizenship

11. Home telephone number (with area code)

12. Individual's identifier

- Birth certificate
 Driver's licence
 Passport
 Provincial health card
 Record of landing / Permanent resident card
 Other

13. ID number (from question 12)

14. Place of issue – Province or State 15. Place of issue – Country

16. Individual's date of birth
 YEAR MONTH DAY

17. Individual's occupation

18. Individual's business telephone number (with area code) 18A. Telephone extension number

Information about individual's employer

19. Individual's employer

20. Employer's street address

21. Employer's city

22. Employer's province or state 23. Employer's country

24. Postal or Zip code

25. Employer's business telephone number (with area code) 25A. Telephone extension number



NOTE: Please copy this page for each additional disposition (if required).

Transaction Disposition

PART E — Information about the entity on whose behalf the transaction was conducted (if applicable)

1. Name of corporation, trust or other entity

2. Type of business

3. Street address

4. City

5. Province or State

6. Country

7. Postal or Zip code

8. Business telephone number (with area code)

8A. Telephone extension number

9. Incorporation number

10. Place of issue – Province or State

11. Place of issue – Country

12. Individual(s) authorized to bind the entity or act with respect to the account (up to three)

1 _____

2 _____

3 _____



NOTE: Please copy this page for each additional disposition (if required).

Transaction Disposition

PART F — Information about the individual on whose behalf the transaction was conducted (if applicable)

1. Surname _____ 2. Given name _____ 3. Other/Initial _____

4. Street address _____

5. City _____

6. Province or State _____ 7. Country _____

8. Postal or Zip code _____

9. Home telephone number (with area code) _____

10. Business telephone number (with area code) _____ 10A. Telephone extension number _____

11. Individual's date of birth
 YEAR MONTH DAY

12. Individual's identifier

Birth certificate Driver's licence Passport Provincial health card Record of landing/Permanent resident card
 Other _____
DESCRIPTION (OTHER)

13. ID number (from question 12) _____

14. Country of residence _____ 14A. Country of citizenship _____

15. Place of issue of individual's identifier — Province or State _____ 16. Place of issue of individual's identifier — Country _____

17. Individual's occupation _____

Information about individual's employer

18. Individual's employer _____

19. Employer's street address _____

20. Employer's city _____

21. Employer's province or state _____ 22. Employer's country _____

23. Postal or Zip code _____

24. Employer's business telephone number (with area code) _____ 24A. Telephone extension number _____

Relationship

25. Relationship of the individual named in Part D to the individual named above (fields 1 to 3)
 Accountant Borrower Customer Friend Relative
 Agent Broker Employee Legal counsel Other _____
DESCRIPTION (OTHER)



PART G — Description of suspicious activity

1. Please describe clearly and completely the factors or unusual circumstances that led to the suspicion of money laundering or terrorist activity financing.*
Provide as many details as possible to explain what you found suspicious.

If this report is about one or more transactions that were attempted, also describe why each one was not completed.

PART H — Description of action taken (if applicable)

1. Please describe what action, if any, was or will be taken by you as a result of the suspicious transaction(s).* (if this part is applicable)

The information on this form is collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act). It will be used for analytical purposes and may also be used for the purposes of ensuring compliance with the Act. Any personal information is protected under the provisions of the *Privacy Act*. For more information, consult the Financial Transactions and Reports Analysis Centre of Canada chapter in the *Sources of Federal Government Information* publication, available on the Government of Canada Info Source Web site (<http://www.infosource.gc.ca>).

Suspicious Transaction Report

Source: www.fintrac-canafe.gc.ca/publications/guide/Guide3B/3b-eng.asp#s441

5. Instructions for Completing a Suspicious Transaction Report

The fields in this section correspond with the paper form called the *Suspicious Transaction Report*. As explained in subsection 3.3, completing a paper report is only permitted if you do not have the capability to report electronically.

Fields in reports are either mandatory, mandatory if applicable, or require "reasonable efforts" to complete, as follows:

- **Mandatory:** All fields of a report marked with an asterisk (*) **have to be completed.**
- **Mandatory if applicable:** The fields that have both an asterisk and "if applicable" next to them have to be completed if they are applicable to you or the transaction being reported.
- **Reasonable efforts:** For all other fields that do not have an asterisk, you have to make reasonable efforts to get the information. "Reasonable efforts" means that you tried to get the information requested on the report. If the information is available to you, you must provide it in the report. If the information was not available at the time of the transaction, and it is not contained in your files or records, the field may be left blank.

In certain circumstances, only as directed in the instructions for certain fields, if you need to indicate that a required field in a report is not applicable, enter "N/A" or "n/a". Do not substitute any other abbreviations, special characters (for example, "x", "*" or "***") or words (for example, "unknown").

When completing the paper form, enter the date and time when you begin completing it at the top of the form. If you have to file a correction to a report on paper, follow the instructions on the first page of the form. If you need to get a paper form, see section 4.

There are eight parts on the *Suspicious Transaction Report* form, but some are only to be completed if applicable. To report a suspicious transaction, follow the following five steps:

- Step 1 - Complete [Part A](#) to provide information about the reporting entity and about where the transaction took place or was attempted.
- Step 2 - Complete [Part B1](#) to provide details about the transaction.
- Step 3 - Complete [Part B2](#) to provide details about the transaction's disposition. If the transaction's disposition was related to an account, also complete [Part C](#). If the transaction's disposition was on behalf of a business, a corporation or other entity (other than an employee depositing cash into his or her employer's business account), also complete [Part E](#). If the transaction's disposition was on behalf of an individual (other than an employee depositing cash into his or her employer's business account), complete [Part F](#).

If there was more than one disposition for the transaction, repeat this step for each disposition.

- Step 4 - Complete [Part D](#) to provide information about the individual conducting or attempting to conduct the transaction.
- Step 5 - Complete [Part G](#) to explain the reason for your suspicion. In the case of a report about attempted transactions, this must include the reason why they were not completed. Also, complete [Part H](#) to provide information about any action taken, if applicable.

If you have to include more than one transaction in your report, repeat steps 2, 3 and 4 for each one. You may need to use extra copies of Parts B1, B2, C, D, E or F to complete your report.

The rest of this section will cover each part of the *Suspicious Transaction Report* form.

Transaction status indicator

To report a **completed** transaction, check "Completed" as the transaction status indicator. This applies to the entire report, so you should not include any other transactions in this report if they were attempted.

To report an **attempted** transaction, check "Attempted" as the transaction status indicator. This applies to the entire report, so you should not include any other transactions in this report if they were completed.

If you need more information about when a transaction is completed or attempted, see *Guideline 2: Suspicious Transactions*.

Part A : Information about where the transaction took place

This part is for information about the reporting entity required to report the transaction to FINTRAC. It is also for information about the physical location where the transaction took place or was attempted.

If you need more information about what type of individual or entity is a reporting entity, see section 2 of this guideline.

If you have multiple branch or office locations, the information in this part should refer to the branch or office location where the transaction took place or was attempted. Transactions that happened or were attempted at different branch or office locations should be reported on separate reports.

Some reporting entities have contractual arrangements with someone outside their entity to conduct transactions on their behalf. For example, a money services business arranges for transactions, such as electronic funds transfers, to be conducted for them at a grocery store. If you have this type of arrangement, as the reporting entity, your name belongs in Part A. However, since the transaction was conducted at someone else's place of business, it is that address that must appear in Part A.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, there are special instructions for you to complete several of the fields in this part.

Field A1* Reporting entity's identifier number (if applicable)

This is the institution or licence number, or other identification number for the reporting entity, as outlined below. If you are a reporting entity that has several branch locations, the identification number should refer to the branch or office where the transaction occurred.

- If you are an **accountant**, enter your provincial chartered accountant (CA), provincial certified management accountant (CMA), or provincial certified general accountant (CGA) number.
- If you are a **bank, caisse populaire, cooperative credit society or credit union**, enter your financial institution number issued by the Canadian Payments Association (CPA).
- If you are an **agent of the Crown that sells or redeems money orders**, enter your post office or similar number.
- If you are a **life insurance broker or agent**, enter your provincial broker or agent licence number.
- If you are a **federally regulated life insurance company**, enter your Office of the Superintendent of Financial Institutions (OSFI) Institution Code.
- If you are a **life insurance company that is not federally regulated**, enter your provincial licence number.
- If you are a **provincial savings office**, enter your financial institution number issued by the CPA.
- If you are a **real estate broker or sales representative**, enter your provincial broker number.
- If you are a **securities dealer**, enter your provincial dealer licence number.
- If you are a **trust and loan company**, enter your financial institution number issued by the CPA.
- If you are a **provincial trust and loan** that is not a member of the CPA, enter your registration number.
- If you are a **money services business**, enter your money services business registration number issued by FINTRAC.
- If you are a **dealer in precious metals and stones**, leave this field blank.
- If you are a **British Columbia public notary**, enter your membership number. If you are a **notary corporation of British Columbia**, enter your permit number.
- If you are a **real estate developer**, enter your provincial licence number if you have one. Otherwise, leave this field blank.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, enter **"EMPLOYEE"** in field A1.

Field A2* Reporting entity's full name

Enter the full legal name of the business or corporation that is the reporting entity. If you are a reporting entity that does not have a business name (for example, you are a reporting entity that is an individual), enter your full name.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, enter your **own** name in field A2.

Fields A3* to A6* Reporting entity's full address

Enter the civic address, town or city, province and postal code where the transaction took place or was attempted. If you have more than one location, this information should refer to where the transaction took place or was attempted. As explained above, transactions that happened at different branch or office locations should be reported on separate reports.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, enter the complete address of where the transaction took place or was attempted in fields A3 to A6.

Field A6A Reporting entity report reference number

If you use a reference number for your own internal purposes, you can enter it in your report to FINTRAC. This field can contain up to 20 alpha or numeric characters and must be unique for each of your reporting entity's reports.

If you do not wish to use such an internal reference number, leave this field empty.

Fields A7*, A8* and A9 Contact name

Enter the name of the individual FINTRAC can contact for clarification about this report.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, enter your **own** contact information in these fields.

Field A10* Contact telephone number

Enter the telephone number, including the area code, of the individual FINTRAC can contact for clarification. Include the extension if applicable in field A10A.

Field A11* Which one of the following types of reporting entities best describes you?

Enter the type of activity applicable to you. If you are involved in more than one activity type, indicate the one applicable to the transaction being reported. If there is more than one activity for one or more transactions on the report, check only one box to indicate your principal type of activity, and provide additional details in Part G.

If you are an **employee** of a reporting entity and you are making this report about a suspicious transaction that you did **not** report to your superior, enter the type of reporting entity **for your employer** in this field.

Part B1 : Information about how the transaction was initiated

This part is for information about how the transaction was initiated (i.e., where the money came from) for the transaction that led you to the suspicion of a connection to money laundering or terrorist financing. In the case of an attempted transaction, this would include information about how it was proposed to be initiated.

Your suspicion could be based on a series of transactions. In that case, include in this report the information for each transaction that led to the suspicion.

When you need to report more than one transaction, complete a separate Part B1 for each transaction. To do this, you can copy Part B1. Fill in the "Transaction ___ of ___" area at the top of Part B1 to distinguish between each transaction. When you provide the details of the transaction in Part D, the details of disposition in Part B2, as well as the additional details of disposition in Parts C, E, and F, as applicable, indicate to which transaction that information applies.

Fields B1*, B2 and B3* When the transaction took place

Enter the date (yyyy-mm-dd) and time (hh:mm:ss) of the suspicious transaction. Use a 24-hour format for time. For example, enter "15:30:00" to represent 3:30 p.m.

The time of the transaction (field B2) can be left blank if it is not available from the moment of the transaction or in your records.

The date of the transaction (field B1) is mandatory. However, if the transaction was a night deposit, and you do not provide the date, you can leave field B1 blank. In this case, make sure to indicate that it was a night deposit at field B3.

If the transaction being reported was attempted and, because of this, information for field B1 or B3 is not available, you can leave the field blank.

Field B4 Date of posting

Enter the date (yyyy-mm-dd) the transaction cleared, if this differs from the date of the transaction provided above. In the case of an attempted transaction, this field would not apply.

Field B5* Detail of funds involved in initiating transaction

Check the appropriate box to describe the type of funds involved in initiating the transaction. For example, if your client brought in cash, "Cash in" is the type of funds, or if your client is cashing in a life insurance policy, "Negotiated life insurance policy" is the description of funds. If the selections provided do not cover the particular transaction, indicate "Other" and provide details in the field provided. For example, if annuities were involved in initiating the transaction, indicate "Other" and provide information about the type of annuity in the "Other" field.

If there was more than one type of funds, indicate only one that best represents how the transaction was initiated. Provide information about the rest of the types of funds in Part G.

If the transaction being reported was attempted and, because of this, information for field B5 is not available, you can leave the field blank.

If you are a dealer in precious metals and stones, select the type of funds in field B5 that best describes what you received in the transaction, or what you were supposed to receive in an attempted transaction. If you were buying precious metals or stones, indicate the type of funds that best describes what you bought or attempted to buy. The same would apply if you were to receive precious metals or stones from a client for a trade-in sale. If you were selling precious metals or stones to a client, indicate the type of funds based on how the client paid or attempted to pay. For example, if the client paid cash, indicate "cash in" or if the client paid by debit card or credit card, indicate "Other" and provide details in the "Other" field.

Field B6* Amount of transaction

Enter the total amount of funds involved in the transaction. This is the total amount received to start the transaction. What happens as a result of that amount will be explained in Part B2 as one or more dispositions.

If this amount was not in Canadian funds, you do not have to convert it but you have to provide the currency information in field B7.

If the transaction being reported was attempted and, because of this, information for field B6 is not available, you can leave the field blank.

Field B7* Transaction currency code

Enter the currency code applicable to the transaction, even if it was in Canadian funds. Enter CAD for Canadian dollars or USD for United States dollars. If the transaction was in another type of currency, see the list of currency codes in Appendix 1 at the end of this guideline.

If the transaction being reported was attempted and, because of this, information for field B7 is not available, you can leave the field blank.

Fields B8* and B9* Other institution, entity or person name, number and account number (if applicable)

These fields are for additional information about the funds described in field B5. Where applicable, in field B8, provide the name (including the institution identification number if applicable) of any other institution, entity or individual involved in the transaction. In addition, where applicable, in field B9, provide the account number of any other individual or entity involved in the disposition. If more than one other individual or institution was involved, put the information about the others in Part G.

Field B10* How was the transaction was conducted?

Check the appropriate box to indicate how the transaction was conducted or attempted. For example, if the transaction was done through an automated banking machine, check that box. If the selections provided do not cover this particular transaction, indicate "Other" and provide details in the field provided.

If the transaction being reported was attempted and, because of this, information for field B10 is not available, you can leave the field blank.

Field B11 ID number of the person initially identifying a suspicious transaction

Enter the identification number of the individual who first identified the suspicious behaviour leading to the report. If that individual does not have an ID number, this field may be left blank.

Part B2: Information about how the transaction was completed

This part is for information about how the transaction was completed (i.e., where the money went). In the case of an attempted transaction, this would include information about how it was proposed to be completed.

"On behalf of" indicator

At the top of Part B2, you have to indicate whether the individual who conducted or attempted the transaction was doing so on anyone else's behalf. You have to select one of the following for this entry:

- **Not applicable**
This means that **neither** Part E **nor** Part F applies to this report. "Not applicable" indicates that, to your knowledge, none of the other "On behalf of" selections is applicable to the transaction. For example, the transaction was a night deposit or a quick drop, or the disposition was not on anyone else's behalf (i.e., it was on behalf of the individual that conducted or attempted it).
- **On behalf of an entity**
This indicates that the disposition was on behalf of an entity, such as a business, a partnership, a corporation, a trust or other entity, but was **not** an employee depositing cash to his or her employer's business account. For a transaction that was conducted or attempted on behalf of an entity, complete Part E for this report to provide the information about that entity.
- **On behalf of another individual**
This indicates that the disposition was on behalf of another individual but was **not** an employee depositing cash to his or her employer's business account. For a transaction that was conducted or attempted on behalf of another individual, complete Part F to provide the information about that other individual.
- **Employee depositing cash to employer's business account**
This indicates that the disposition was an employee depositing cash to his or her employer's **business** account. If it was an employee depositing cash to his or her employer's business account, **neither** Part E **nor** Part F applies for this report. Do not use this indicator if the employee deposited other than cash or if the employer's account was other than a business account.

More than one disposition

There could be more than one disposition for a particular transaction. For example, your client could initiate a transaction in cash, send an electronic funds transfer (EFT) for part of it (disposition 1), order a bank draft for another part (disposition 2) and deposit the rest (disposition 3). In that case, make sure you include the information for each disposition. If you are including more than one transaction in this report, you have to complete Part B2 for all dispositions for each transaction.

If you have to include more than one disposition, complete a separate Part B2 for each one. To do this, you can copy Part B2. Fill in the "Transaction ____ Disposition ____ of ____" area at the top of Part B2 to distinguish between each disposition. If you have to include more than one transaction in this report, indicate to which transaction the disposition information applies, based on the number you assigned the transaction in Part B1. When you provide the details of disposition in Parts C, E, and F, as applicable, also indicate to which disposition and which transaction that information applies.

Field B12* Disposition of funds

This describes what happened to the funds involved in the transaction.

If the disposition of funds was a life insurance policy purchase or deposit, check that box and provide the life insurance policy number in the appropriate field. If the selections provided do not cover this particular disposition, indicate "Other" and provide details in the appropriate field.

If the transaction being reported was an employee depositing cash to an employer's business account (as indicated by the "on behalf of" indicator at the top of Part B2), the disposition of funds in field B12 should be "deposit to an account".

If the transaction being reported was attempted and, because of this, information for field B12 is not available, you can leave the field blank.

If you are a dealer in precious metals and stones, select the disposition of funds in field B12 that best describes what you paid or sold (or what you attempted to pay or sell) to the conductor of the transaction. If you were buying precious metals or stones, select the disposition of funds that best describes how you paid or attempted to pay for them. For example, if you paid in cash, indicate "cash out" or if you paid by cheque, indicate "Other" and provide details in the "Other" field. If you were selling precious metals or stones (including a trade-in sale), select the disposition of funds that best describes what your client purchased or attempted to purchase.

Field B13* Amount of disposition

Enter the amount of funds involved in the disposition. If the amount was not in Canadian funds, you do not have to convert it but you have to provide the currency information in field B14.

If the transaction being reported was attempted and, because of this, information for field B13 is not available, you can leave the field blank.

Field B14* Disposition currency code

Enter the code for the currency of the disposition, even if it was in Canadian funds. Enter CAD for Canadian dollars or USD for United States dollars. If the transaction was in another type of currency, see the list of currency codes in Appendix 1 at the end of this guideline.

If the transaction being reported was attempted and, because of this, information for field B14 is not available, you can leave the field blank.

Fields B15* and B16* Other institution, entity or person name, number and account or policy number (if applicable)

These fields are for additional information about the disposition described in field B12. Where applicable, in field B15, provide the name (including the institution identification number if applicable) of any other institution, individual or entity involved in the disposition. In addition, where applicable, in field B16, provide the account number of any other individual or entity involved in the disposition. Also provide any policy number related to the other entity or individual in field B16, if applicable.

If more than one other individual, entity or institution was involved, put the information about the others in Part G.

Part C: Account information, if the transaction involved an account

This part is for information about the account involved in the transaction, if it in fact involved an account. In the case of an attempted transaction, this would include information about the account that was proposed to be involved.

As explained earlier, it is possible to have more than one transaction per report, and more than one disposition per transaction. Provide the account information, if applicable, for each disposition included in the report.

If you have to include account information for more than one disposition, complete a separate Part C to provide information for each account involved. To do this, you can copy Part C. Fill in the "Transaction ____ Disposition ____" area at the top of Part C to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Field C1* Branch or transit number where the account is held (if this part is applicable)

Enter the branch number, transit number, or other appropriate identifying number of the entity where the relevant account is held, if an account is applicable to the transaction.

If the transaction being reported was attempted and, because of this, information for field C1 is not available, you can leave the field blank.

Field C2* Account number (if this part is applicable)

Enter the number of the relevant account.

If the transaction being reported was attempted and, because of this, information for field C2 is not available, you can leave the field blank.

Field C3* Type of account (if this part is applicable)

Indicate the type of the relevant account. For example, a business account would be one that, at the time it was opened, was for a business or for a non-profit organization, etc. (i.e., other than a personal or trust account). If the selections "personal, business or trust" do not cover this particular account, indicate "Other" and provide details in the field provided.

If the transaction being reported was an employee depositing cash to an employer's business account (as indicated by the "on behalf of" indicator at the top of Part B2), the account type in field C3 should be "business".

If the transaction being reported was attempted and, because of this, information for field C3 is not available, you can leave the field blank.

Field C4* Account currency code (if this part is applicable)

Enter the code of the currency for the relevant account. Enter CAD for Canadian dollars or USD for United States dollars. If the account is in another type of currency, see the list of currency codes in Appendix 1 at the end of this guideline.

If the transaction being reported was attempted and, because of this, information for field C4 is not available, you can leave the field blank.

Field C5* Full name of the individual(s) or entity that hold the account (if this part is applicable)

Enter the full name of each account holder (up to three).

This is for information about each individual or entity that holds the account. For example, in the case of a joint account for husband and wife, include the names of each spouse at field C5.

The account holder might be different from the individual(s) authorized to give instructions for the account. For example, an account for a corporation will have one or more individuals authorized to give instructions for that account. In this case, it is the name of the corporation that holds the account that is required in field C5. Information about individuals authorized to bind the entity or to act with respect to the account belongs in Part E, if applicable, in field E12.

If the transaction being reported was attempted and, because of this, information for field C5 is not available, you can leave the field blank.

Field C6 Date opened

Enter the date (yyyy-mm-dd) the account was opened.

Field C7 Date closed

Enter the date (yyyy-mm-dd) the account was closed, if applicable.

Field C8* Status of the account at the time the transaction was initiated (if this part is applicable)

Indicate whether the account was active, inactive or dormant at the time the transaction was initiated.

The status of an account is determined by your policies and procedures. For example, your policy may be to assign inactive status to all accounts if there is no client activity for an account over a certain period of time, and dormant status if that inactivity is prolonged.

If you do not have such policies or procedures to assign inactive or dormant status to unused accounts, simply leave this field blank.

If the transaction being reported was attempted and, because of this, information for field C8 is not available, you can leave the field blank.

Part D: Information about the individual conducting the transaction

This part is for information about the individual who conducted or attempted to conduct the transaction. As explained earlier, it is possible to have more than one transaction per report. Provide this information for each transaction included in the report.

If you need to report more than one transaction, complete a separate Part D for each transaction. To do this, you can copy Part D. Fill in the "Transaction ___" area at the top of Part D to distinguish between each transaction, based on the number you assigned the transaction in Part B1.

If you are a dealer in precious metals and stones, the individual who conducted or attempted to conduct the transaction is the one from whom you were buying or to whom you were selling precious metals or stones.

Fields D1 to D3 Individual's full name

Enter the last name, first name and middle initial (if applicable) of the individual who conducted or attempted to conduct the transaction.

Field D4* Entity client number (if applicable)

Enter the client number you issued to the individual who conducted or attempted to conduct the transaction, if applicable.

Fields D5 to D9 Individual's full address

Enter the civic address, town or city, province or state, country and postal code of the individual who conducted or attempted to conduct the transaction.

Field D10 Country of residence

Enter the country of permanent residence of the individual who conducted or attempted to conduct the transaction.

Field D10A Country of citizenship

Enter the country of citizenship of the individual who conducted or attempted to conduct the transaction.

Field D11 Home telephone number

Enter the home telephone number, including the area code, of the individual who conducted or attempted to conduct the transaction.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field D12 Individual's identifier

Check the appropriate box to show the document used to identify the individual who conducted or attempted to conduct the transaction.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in the field provided.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field D12, but do not provide the number in field D13.

Field D13 ID Number

Enter the number of the document described in field D12 that was used to identify the individual who conducted or attempted to conduct the transaction. Remember that a health card number is not acceptable for this purpose in some provinces. Furthermore, as explained above, a SIN should not be provided on this form. If the identifier document in field D12 (and D12A) is a SIN card, enter "N/A" in field D13 to indicate the number is not applicable.

Fields D14 and D15 Place of issue of individual's identifier

Enter the province or state and country of issue of the document used to identify the individual who conducted or attempted to conduct the transaction. If the document was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

Field D16 Individual's date of birth

Enter the date (yyyy-mm-dd) of birth of the individual who conducted or attempted to conduct the transaction.

Field D17 Individual's occupation

Enter the occupation of the individual who conducted or attempted to conduct the transaction.

Be as descriptive as possible regarding occupation. Provide information that clearly describes it, rather than use a general term. For example, in the case of a consultant, the occupation should reflect the area of consulting, such as "IT consultant" or "consulting forester". As another example, in the case of a professional, the occupation should reflect the nature of the work, such as "petroleum engineer" or "family physician".

If the individual is not employed or engaged in any type of business or profession, provide information that best describes their situation, such as "student", "unemployed", "retired", etc.

Field D18 Individual's business telephone number

Enter the business telephone number, including the area code, of the individual who conducted or attempted to conduct the transaction. Include the extension if applicable at field D18A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field D19 Individual's employer

Enter the name of the entity or individual who is the employer of the individual who conducted or attempted to conduct the transaction.

Fields D20 to D24 Employer's business address

Enter the civic address, town or city, province or state, country and postal code of the employer of the individual who conducted or attempted to conduct the transaction.

Field D25 Employer's business telephone number

Enter the business telephone number, including the area code, of the employer of the individual who conducted or attempted to conduct the transaction. Include the extension if applicable at field D25A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Part E: Information about the entity on whose behalf the transaction was conducted (if applicable)

This part only applies if the transaction's disposition was conducted or attempted on behalf of a third party that is an entity, as indicated in Part B2. If an employee deposited cash in his or her employer's business account, Part E does not apply.

Complete a separate Part E for each disposition that was conducted or attempted on behalf of a business, corporation or other entity. To do this, you can copy Part E. Fill in the "Transaction ____ Disposition ____" area at the top of Part E to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Field E1 Name of corporation, trust or other entity

Enter the full name of the business, corporation, trust or other entity on whose behalf the transaction was conducted or attempted.

Field E2 Type of business

Describe the type of business or entity on whose behalf the transaction was conducted or attempted.

Fields E3 to E7 Full address of business or corporation

Enter the civic address, town or city, province or state, country and postal code of the business, corporation or other entity on whose behalf the transaction was conducted or attempted.

Field E8 Business telephone number

Enter the telephone number, including the area code, of the business, corporation or other entity on whose behalf the transaction was conducted or attempted. Include the extension, if applicable, at field E8A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Fields E9 to E11 Incorporation information

If the transaction was conducted or attempted on behalf of an entity that is a corporation, provide the incorporation number. Also provide the province or state and country of the incorporation number's place of issue. If an incorporation number does not exist for the corporation, enter "N/A" in fields E9, E10 and E11. If the incorporation number was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

Field E12 Individual(s) authorized to bind the entity or act with respect to the account (up to three)

Provide the names of up to three individuals who have authority to conduct transactions through the account.

Part F: Information about the individual on whose behalf the transaction was conducted (if applicable)

This part only applies when the transaction's disposition was conducted or attempted on behalf of a third party that is an individual, as indicated in Part B2.

If the individual conducted or attempted the transaction's disposition on his or her own behalf, this Part does not apply. In that case, information about the individual should be put in Part D.

If an employee deposited cash in his or her employer's business account, Part F does not apply. If the transaction's disposition was conducted or attempted on behalf of a business, corporation or other entity, Part E should be completed.

Complete a separate Part F for each disposition that was conducted or attempted on behalf of an individual. To do this, you can copy Part F. Fill in the "Transaction ____ Disposition ____" area at the top of Part F to distinguish between each disposition, based on the number you assigned the disposition in Part B2.

Fields F1 to F3 Individual's full name

Enter the last name, first name and middle initial (if applicable) of the individual on whose behalf the transaction was conducted or attempted.

Fields F4 to F8 Individual's full address

Enter the civic address, town or city, province or state, country and postal code of the individual on whose behalf the transaction was conducted or attempted.

Field F9 Home telephone number

Enter the home telephone number, including the area code, of the individual on whose behalf the transaction was conducted or attempted.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field F10 Business telephone number

Enter the business telephone number, including the area code, of the individual on whose behalf the transaction was conducted or attempted. Include the extension if applicable in field F10A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field F11 Individual's date of birth

Enter the date of birth (yyyy-mm-dd) of the individual on whose behalf the transaction was conducted or attempted.

Field F12 Individual's identifier

Check the appropriate box to show the document used to identify the individual on whose behalf the transaction was conducted or attempted.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in the field provided.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field F12, but do not provide the number in field F13.

Field F13 ID number

Enter the number of the document described in field F12 that was used to identify the individual on behalf of whom the transaction was conducted or attempted. Remember that a health card number is not acceptable for this purpose in some provinces. Furthermore, as explained above, a SIN should not be provided on this form. If the identifier document in field F12 (and F12A) is a SIN card, enter "N/A" in field F13 to indicate the number is not applicable.

Field F14 Country of residence

Enter the country of permanent residence of the individual on whose behalf the transaction was conducted or attempted.

Field F14A Country of citizenship

Enter the country of citizenship of the individual on whose behalf the transaction was conducted or attempted.

Fields F15 and F16 Place of issue

Enter the province or state and country of issue of the document used to identify the individual on whose behalf the transaction was conducted or attempted. If the document was issued nationally and there was no province or state included in the place of issue, leave the province or state field blank.

Field F17 Individual's occupation

Enter the occupation of the individual on whose behalf the transaction was conducted or attempted.

Be as descriptive as possible regarding occupation. Provide information that clearly describes it, rather than use a general term. For example, in the case of a consultant, the occupation should reflect the area of consulting, such as "IT consultant" or "consulting forester". As another example, in the case of a professional, the occupation should reflect the nature of the work, such as "petroleum engineer" or "family physician".

If the individual is not employed or engaged in any type of business or profession, provide information that best describes their situation, such as "student", "unemployed", "retired", etc.

Field F18 Individual's employer

Enter the name of the entity or individual who is the employer of the individual on whose behalf the transaction was conducted or attempted.

Fields F19 to F23 Employer's business address

Enter the civic address, town or city, province or state, country and postal code of the employer of the individual on whose behalf the transaction was conducted or attempted.

Field F24 Employer's business telephone number

Enter the business telephone number, including the area code, of the employer of the individual on whose behalf the transaction was conducted or attempted. Include the extension if applicable in field F24A.

If the number is one from Canada or the United States, enter the area code and local number. This should be in the following format: "999-999-9999".

If the number is from outside Canada or the United States, provide the country code, city code and local number components. As each of those components can vary in length, use a dash (-) to separate each one. For example, "99-999-9999-9999" would indicate a two-digit country code, a three-digit city code and an eight digit local number.

Field F25 Relationship of the individual named in Part D to the individual named above

Check the appropriate box to indicate the relationship of the individual conducting or attempting the transaction to the individual on whose behalf the transaction was conducted or attempted.

If the selections provided do not cover the relationship, indicate "Other" and provide details in the appropriate field.

Part G: Description of Suspicious Activity

This Part is to provide details of why you suspected that the transaction or the series of transactions were related to money laundering or terrorist financing.

Field G1* Description of suspicious activity

This section explains what led you to believe there was something suspicious about the transaction. The more information that you provide to explain the basis of your suspicion, the more valuable your report will be. The ideal response would clearly and completely describe all of the factors or unusual circumstances which led you to a suspicion of money laundering or terrorist financing, and would provide as many relevant details as possible to support this determination.

Do not leave information about the description of suspicious activity out of your report by referring to any other files or documents. FINTRAC will not have access to that information unless you provide the details in your report.

If this report is about one or more transactions that were attempted, also describe why each one was not completed.

Part H: Action Taken (if applicable)

This Part is for you to describe what action, if any, was taken by you, as a result of the suspicious transaction.

Field H1* Action taken (if this part is applicable)

Identify whether you have taken or will take any action as a result of the suspicious transaction, in addition to reporting to FINTRAC. For example, if you are also making a report to a law enforcement agency, indicate this in Part H.

CHAPTER 19

Appendix M— Terrorist Property Form

This form is reproduced with permission from the Financial Transactions and Reports Analysis Centre of Canada and was up-to-date at the time of printing. As this form may change, we recommend you check the website to ensure you are using the latest version.

Source: www.fintrac-canafe.gc.ca/publications/TPR-2008-eng.pdf

NOTE: Please copy this page for each additional, related, suspicious transaction (if required).

Transaction of

PART B — Reason for filing this report

1. Please describe clearly and completely what led you to file this report about terrorist property.*
Provide as many details as possible to explain how you came to be in possession or control of the property.
If there is not enough room on the form, attach a separate sheet to provide all the relevant information.
Make sure to indicate that this information belongs in field 1 of Part B.

2. Provide as many details as possible about how you know this property is owned or controlled by or on behalf of a terrorist or a terrorist group or about how you believe that this property is owned or controlled by or on behalf of a listed person.

Also include details of what other action you have taken regarding the property, in addition to sending this report to FINTRAC.
If there is not enough room on the form, attach a separate sheet to provide all the relevant information. Make sure to indicate that this information belongs in field 2 of Part B.

Note: You must disclose this property's existence to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service, along with any information about a transaction or proposed transaction for that property. See Guideline 5: Submitting Terrorist Property Reports to FINTRAC for more information.

Information about the terrorist, terrorist group or listed entity

Name of terrorist group, listed person or individual that owns or controls the property (or that the property is owned or controlled on behalf of). If it is an entity, complete field 3. If it is an individual, complete fields 3A-B-C.

3. Full name of terrorist group or listed person

3A. Surname of terrorist or listed person

3B. Given name of terrorist or listed person

3C. Other/Initial

4. Street address

5. City

6. Province or State

7. Country

8. Postal or Zip code

9. Phone number (with area code)

9A. Phone extension number

Information about anyone who owns or controls the property on behalf of the terrorist or listed person above (where applicable)

Name of entity or individual that owns or controls the property on behalf of the terrorist or listed person named in field 3 or fields 3A-B-C (above). If it is an entity, complete field 10. If it is an individual, complete fields 10A-B-C.

10. Full name of terrorist group or listed person

10A. Surname of individual

10B. Given name

10C. Other/Initial

11. Street address

12. City

13. Province or State

14. Country

15. Postal or Zip code

16. Phone number (with area code)

16A. Phone extension number

Terrorist Property Report



NOTE: Please copy this page for each additional property (if applicable).

PART C — Information about the property

Property of

1. Type of property*

<input type="checkbox"/> Cash	Indicate the type of currency in property identifier (field 2) below. Indicate the actual or approximate value of the cash in field 4 below and provide the currency code applicable in field 4A. Provide any additional information about the cash in the description of property (field 5) below.
<input type="checkbox"/> Bank account	Indicate the name of the financial institution in property identifier (field 2) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide the account number(s) and other account information in Part D. If you need to provide any additional information about the account, you can use the description of property (field 5) below.
<input type="checkbox"/> Insurance policy	Indicate the name of the insurance policy issuer in property identifier (field 2) below, and policy number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 below and provide the currency code applicable in field 4A. Provide any additional information about the insurance policy in the description of property (field 5) below, such as the names of beneficiaries, etc.
<input type="checkbox"/> Money order	Indicate the name of issuer in property identifier (field 2) below, and any number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the money order in the description of property (field 5) below, such as the name of the bearer, etc.
<input type="checkbox"/> Real estate	Indicate the type of real estate (such as single family home, condo, commercial, land only, etc.) in property identifier (field 2) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the real estate in the description of property (field 5) below, such as the municipal address and name of registered owner, and description of the property.
<input type="checkbox"/> Securities	Indicate the name of the securities issuer in property identifier (field 2) below, and any securities number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the type of securities (such as stocks, bonds, mutual funds, etc.) in the description of property (field 5) below. If the property involves an account, complete Part D to provide information about the account.
<input type="checkbox"/> Traveller's cheques	Indicate name of issuer of the traveller's cheques in property identifier (field 2) below, and any number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the traveller's cheques in the description of property (field 5) below, such as the currency, name of the bearer, etc.
<input type="checkbox"/> Other	<p>DESCRIPTION (OTHER)</p> <p>For example, this could include the commercial assets of a business or partnership. Indicate property identifier (field 2) below, and property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the property in the description of property (field 5) below. If the property involves an account, complete Part D to provide information about the account.</p>

2. Property identifier (see instructions above for type of property)

If there is not enough room to provide all the property identifier information for this property, attach a separate sheet to provide all the relevant information. Make sure to indicate that this information belongs in field 2 of Part C.

3. Property identifier number (see instructions above for type of property)

If there is not enough room to provide all the property identifier numbers for this property, attach a separate sheet to provide them all. Make sure to indicate that this information belongs in field 3 of Part C.

4. Property value (actual or approximate)*

4A. Currency code Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3: Submitting Reports to FINTRAC*.

5. Description of property

If there is not enough room to provide all the information to describe this property, attach a separate sheet to provide all the details. Make sure to indicate that this information belongs in field 5 of Part C.

NOTE: Please copy this page for each additional account (if applicable).

PART D — Account information (if property involves an account)

Property Account of

1. Branch or transit number* (where applicable) 2. Account number* (where applicable)

3. Type of account* (where applicable)
 A Personal **B** Business **C** Trust **D** Other DESCRIPTION (OTHER)

4. Currency code* (where applicable) Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3: Submitting Reports to FINTRAC*.

5. Full name of each account holder* (where applicable)
 A
 B
 C

6. Date opened 7. Date closed **2 | 0**

8. Status of the account* (if there was a transaction or a proposed transaction, please provide the status at the time the transaction was initiated or proposed.)
 A Active **B** Inactive **C** Dormant



NOTE: Please copy this page for each additional, related, disposition (per transaction) (if required).

PART E2 — Information about the transaction or proposed transaction disposition(s) (where applicable)

Property Transaction Disposition of

If there was a transaction related to the property, indicate how it was completed, i.e., where the money went. If there was a proposed transaction related to the property, indicate how it was proposed to be completed. If there was no transaction related to the property, do not complete this Part, or Parts E1, F, G or H.

Indicate on whose behalf this transaction was conducted.

On behalf of: **The individual who conducted the transaction** (described in PART F) **An entity (other than an individual)** (also complete PART G)
 Another individual (besides the individual who conducted it) (also complete PART H)

12. Disposition of funds how the transaction was completed* (where applicable)

<input type="checkbox"/> A Cash out	<input type="checkbox"/> E Outgoing electronic funds transfer	<input type="checkbox"/> H Purchase of diamonds	<input type="checkbox"/> K Purchase of precious stones (excluding diamonds)	<input type="checkbox"/> N Real estate purchase/deposit
<input type="checkbox"/> B Currency exchange	<input type="checkbox"/> F Purchase of bank draft	<input type="checkbox"/> I Purchase of jewellery	<input type="checkbox"/> L Purchase of money order	<input type="checkbox"/> O Securities purchase/deposit
<input type="checkbox"/> C Deposit to an account	<input type="checkbox"/> G Purchase of casino chips	<input type="checkbox"/> J Purchase of precious metals	<input type="checkbox"/> M Purchase of traveller's cheques	
<input type="checkbox"/> D Life insurance policy purchase/deposit	<input type="checkbox"/> P Other			

POLICY NUMBER DESCRIPTION (OTHER)

13. Amount of disposition* (where applicable)

14. Currency code* (where applicable) Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, see Appendix 1 in *Guideline 3: Submitting Reports to FINTRAC*.

Additional information about the funds described in field 12 above

15. Other institution, entity or person name and number* (where applicable)

16. Account number or policy number of other institution, entity or person* (where applicable)



NOTE: Please copy this page for each additional transaction (if applicable).

PART F — Information about the individual who conducted or proposed to conduct transaction(s) (where applicable)

Property Transaction

1. Surname _____ 2. Given name _____ 3. Other/Initial _____

1A. Alias Surname _____ 2A. Alias Given name _____ 3A. Alias Other/Initial _____

4. Client number assigned by reporting person or entity (where applicable)

5. Street address

6. City

7. Province or State _____ 8. Country _____

9. Postal or Zip code

10. Country of residence

11. Home phone number (with area code)

12. Individual's identifier

Driver's licence Birth certificate Provincial health card Passport Record of Landing or Permanent resident card
 Other _____
DESCRIPTION (OTHER)

13. ID number (from question 12) _____ 13A. Citizenship _____

14. Place of issue Province or State _____ 15. Place of issue Country _____

16. Individual's date of birth
YEAR MONTH DAY

17. Individual's occupation

18. Individual's business phone number (with area code) _____ 18A. Phone extension number _____

19. Individual's employer

20. Employer's street address

21. Employer's city

22. Employer's province or state _____ 23. Employer's country _____

24. Postal or Zip code

25. Employer's business phone number (with area code) _____ 25A. Phone extension number _____



NOTE: Please copy this page for each additional disposition (if required).

Property Transaction Disposition

PART G — Information about the entity on whose behalf transaction was conducted or proposed to be conducted (where applicable)

1. Name of corporation, trust or other entity

2. Type of business

3. Street address

4. City

5. Province or State

6. Country

7. Postal or Zip code

8. Business phone number (with area code)

8A. Phone extension number

9. Incorporation number (where applicable)

10. Place of issue Province or State

11. Place of issue Country

12. Individual(s) authorized with respect to the account (up to three (3))

A _____

B _____

C _____



NOTE: Please copy this page for each additional disposition (if required).

Property Transaction Disposition

PART H — Information about the individual on whose behalf transaction was conducted or proposed to be conducted (where applicable)

1. Surname _____ 2. Given name _____ 3. Other/Initial _____
 1A. Alias Surname _____ 2A. Alias Given name _____ 3A. Alias Other/Initial _____
 4. Street address _____
 5. City _____
 6. Province or State _____ 7. Country _____
 8. Postal or Zip code _____ 9. Home phone number (with area code) _____
 10. Office phone number (with area code) _____ 10A. Phone extension number _____ 11. Individual's date of birth _____
YEAR MONTH DAY

12. Individual's identifier
 Driver's licence Birth certificate Provincial health card Passport Record of Landing or Permanent resident card
 Other _____
DESCRIPTION (OTHER)

13. ID number (from question 12) _____
 14. Place of issue Province or State _____ 15. Place of issue Country _____
 16. Country of residence _____ 16A. Citizenship _____

17. Individual's occupation _____
 18. Individual's employer _____
 19. Employer's street address _____
 20. Employer's city _____
 21. Employer's province or state _____ 22. Employer's country _____
 23. Postal or Zip code _____
 24. Employer's business phone number (with area code) _____ 24A. Phone extension number _____

25. Relationship of the individual named in Part F to the individual named above (fields 1 to 3)
 Accountant Agent Legal counsel Borrower Broker
 Customer Employee Friend Relative Other _____
DESCRIPTION (OTHER)

The information on this form is collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* [the Act]. It will be used for analytical purposes and may also be used for the purposes of ensuring compliance with the Act. Any personal information is protected under the provisions of the *Privacy Act*. For more information, consult the Financial Transactions and Reports Analysis Centre of Canada chapter in the *Sources of Federal Government Information* publication, available on the Government of Canada Info Source Web site (<http://www.infosource.gc.ca>).

Source: www.fintrac-canafe.gc.ca/publications/guide/Guide5/5-eng.asp#s55

5. Instructions for Completing a Terrorist Property Report

The fields in this section refer to the numbered areas on the *Terrorist Property Report* form. As explained in subsection 3.3, these reports can only be completed and sent to FINTRAC on paper. There is no mechanism to report electronically.

Fields of this report are either mandatory, mandatory where applicable, or require "reasonable efforts" to complete, as follows:

- **Mandatory:** All fields of the report marked with an asterisk (*) **have to be completed.**
- **Mandatory where applicable:** The fields have both an asterisk and "where applicable" next to them have to be completed if they are applicable to you or to the property or the transaction or proposed transaction being reported.
- **Reasonable efforts:** For all other fields that do not have an asterisk, you have to make reasonable efforts to get the information. "Reasonable efforts" means that you tried to get the information requested on the report. If the information is available to you, you must provide it in the report. In the case of a transaction or a proposed transaction, if the information is not contained in your files or records, and it was not available at the time of the transaction, the field may be left blank.

Enter the date and time when you begin completing the report at the top of the form. If you have to file a correction to a report on paper, follow the instructions on the first page of the form. If you need to get a paper form, see section 3.

There are eight parts on the *Terrorist Property Report* form, but some are only to be completed if applicable. To make a terrorist property report, follow the following four steps:

- Step 1 - Complete Part A to provide information about you as the reporting entity.
- Step 2 - Complete Part B to provide details about the terrorist, terrorist group or listed person, and anyone who owns or controls the property on their behalf. Part B is also for you to explain what led you to file the report, as well as how you came to know that the property is owned or controlled by or on behalf of a terrorist or terrorist group or how you came to believe that the property is owned or controlled by or on behalf of a listed person.
- Step 3 - Complete Part C to provide details about the property. If the property involves an account, also complete Part D. If there were no transactions or proposed transactions related to the property, do not complete the rest of the report.
- Step 4 - If there was a transaction relating to the property, complete Parts E1 and E2 to provide information about how the transaction was initiated and completed. Provide the same information if there was a proposed transaction relating to the property. Complete Part F to provide information about the individual who conducted or proposed to conduct the transaction. If the transaction or proposed transaction was on behalf of an entity (such as a corporation or trust), also complete Part G or, if it was on behalf of an individual, complete Part H.

The rest of this section will cover each part of the *Terrorist Property Report* form.

Part A: Information about the person or entity filing this report

This part is for information about you, the reporting person or entity creating the report. If you have multiple branch or office locations, the information in this Part should be about the branch or office location where you possess or control the property.

Field 1* Reporting person or entity's identifier number (where applicable)

This is your institution or licence number, or other identification number as outlined below. If you have several branch locations, the identification number should refer to the branch or office where you possess or control the property.

- If you are an **accountant**, enter your provincial chartered accountant (CA), provincial certified management accountant (CMA), or provincial certified general accountant (CGA) number.
- If you are a **bank, caisse populaire, cooperative credit society or credit union**, enter your financial institution number issued by the Canadian Payments Association (CPA).
- If you are an **agent of the Crown that sells or redeems money orders**, enter your post office number.
- If you are a **life insurance broker or agent**, enter your provincial broker or agent licence number.
- If you are a **federally regulated life insurance company**, enter your institution code issued by the Office of the Superintendent of Financial Institutions (OSFI).
- If you are a **life insurance company that is not federally regulated**, enter your provincial licence number.
- If you are a **provincial savings office**, enter your financial institution number issued by the CPA.
- If you are a **real estate broker or sales representative**, enter your provincial broker number.
- If you are a **securities dealer**, enter your provincial dealer licence number.
- If you are a **trust and loan company**, enter your financial institution number issued by the CPA.
- If you are a **provincial trust and loan** that is not a member of the CPA, enter your registration number.
- If you are a **money services business**, enter your money services business registration number issued by FINTRAC.
- If you are a **dealer in precious metals and stones**, leave this field blank.
- If you are a **British Columbia public notary**, enter your membership number. If you are a **notary corporation of British Columbia**, enter your permit number.
- If you are a **real estate developer**, enter your provincial licence number if you have one. Otherwise, leave this field blank.

If there was a transaction or a proposed transaction relating to the property at a different location from where you possess or control the property, provide the details about that other location in field 1 of Part B.

Field 2* Reporting person or entity's full name

Enter the full legal name of your business or corporation. If you do not have a business name (for example, you are an individual), enter your full name.

Fields 3* to 6* Reporting person or entity's full address

Enter your civic address, town or city, province and postal code. If you have more than one location, this information should be about where the property is possessed or controlled.

Fields 7*, 8* and 9 Contact name

Enter the name of the individual FINTRAC can contact for clarification about this report.

Field 10* Contact telephone number

Enter the telephone number, including the area code, of the individual named in fields 7 to 9 (above). Include the extension if applicable at field 10A.

Field 11* Type of reporting person or entity

Enter the type of activity that best describes you. If you are involved in more than one activity type, indicate the one applicable to the property being reported. If there is more than one activity for one or more properties on the report, check only one box to indicate your principal type of activity, and provide additional details in Part B, field 1.

Part B: Reason for filing this report

This part is to provide details of why you are filing a report about property in your possession or control. You have to explain how you came to know or believe that the property is owned or controlled by or on behalf of a terrorist, terrorist group or listed person. This part is also for you to provide information about the terrorist, terrorist group or listed person and anyone (besides you) who possesses or controls the property on their behalf.

Field 1* Reason for filing this report

This section explains what led you to make this report. The more information that you provide to explain this, the more valuable your report will be.

Include a clear and complete description of the events that led you to make this report, with as many details as possible. Include an explanation of how you came to be in possession or control of the property.

If there is not enough room on the form, attach a separate sheet to provide all the relevant information. Make sure you indicate on the separate sheet that this information belongs in field 1 of Part B.

If you can use word-processing software to write out this information, attach the printed text to Part B. Make sure you indicate that it belongs in field 1 of Part B.

Field 2 How you came to know or believe that the property is terrorist property or believe that property is listed person

Provide as many details as possible about how you know this property is owned or controlled by or on behalf of a terrorist or a terrorist group or how you believe this property is owned or controlled by or on behalf of a listed person.

If there is not enough room on the form, attach a separate sheet to provide all the relevant information. Make sure you indicate on the separate sheet that this information belongs in field 2 of Part B.

Field 3 Full name of terrorist, terrorist group or listed person

Enter the full name of the terrorist, terrorist group or listed person that owns or controls the property, or on whose behalf the property is owned or controlled. As explained in subsection 3.1, a terrorist or a terrorist group can be an individual, a group, a trust, a partnership, or a fund. It can also be an unincorporated association or organization. A listed person can be an individual, a corporation, a trust, a partnership, a fund or an unincorporated association or organization.

If it is an entity (that is, not an individual), enter the complete name of the terrorist group or listed person in field 3. If it is an individual, enter the terrorist's or listed person's surname, given name, and other name or initial (if known) in fields 3A, 3B and 3C.

If the property is owned or controlled by an individual or entity other than the terrorist, terrorist group or listed person, provide the details at fields 10 through 16 below. For example, if you know you are dealing with a terrorist group through a front organization, provide information about the front organization in fields 10 through 16.

Fields 4 to 8 Terrorist, terrorist group or listed person address

Enter the civic address, town or city, province, country and postal code for the terrorist, terrorist group or listed person named in field 3 above.

Field 9 Telephone number

Enter the telephone number, including the area code, of the terrorist, terrorist group or listed person named in field 3 above. Include the extension, if applicable, at field 9A.

Field 10 Name of individual or entity that owns or controls the property on behalf of the terrorist, terrorist group or listed person

Enter the full name of the individual or entity that owns or controls the property on behalf of the terrorist, terrorist group or listed person named in field 3 above.

If it is an entity (that is, not an individual), enter the complete name of the entity in field 10. If it is an individual, enter the individual's surname, given name, and other name or initial (if known) in fields 10A, 10B and 10C.

Fields 11 to 15 Individual or entity address

Enter the civic address, town or city, province and postal code for the individual or entity named in field 10 above.

Field 16 Telephone number

Enter the telephone number, including the area code, of the individual or entity named in field 10 above. Include the extension if applicable at field 16A.

Part C: Information about the property

This part is for information about the property in your possession or control.

If there is more than one property associated with the terrorist, terrorist group or listed person named in field 3 of Part B, complete a separate Part C for each property. To do this, you can copy Part C. At the top of Part C, complete the "Property (number) of (total number of properties in Part C)" area to distinguish between each property. If there was a transaction or a proposed transaction related to a property described in Part C, provide the details of the transaction in Parts E1, E2 and F, as well as Part G or H, as applicable. For each of these, indicate to which property the transaction information applies.

Field 1* Type of property

Check the appropriate box to indicate which of the seven types listed best describes the property. Follow the instructions next to the applicable description on the form for the rest of the fields in Part C.

If none of the seven types is appropriate for the type of property, check the box for "Other". This would include, for example, commercial business assets (other than funds such as bank accounts). Provide a description in the space provided to the right. Follow the instructions underneath for the rest of the fields in Part C.

If the property involves an account, complete Part D to provide information about the account.

Field 2 Property identifier

Follow the instructions for the applicable property type in field 1. For example, if the property is "cash", indicate the type of currency in field 2.

If there is not enough room on the form to provide all the property identifier information for this property, attach a separate sheet to provide all the relevant information. It is very important that you indicate clearly on the separate sheet that this information belongs in field 2 of Part C.

Field 3 Property identifier number

Follow the instructions for the applicable property type in field 1. For example, if the property is an insurance policy, indicate the policy number in field 3.

If there is not enough room on the form to provide all the property identifier information for this property, attach a separate sheet to provide all the relevant information. It is very important that you indicate clearly on the separate sheet that this information belongs in field 3 of Part C.

Field 4* Actual or approximate value

Provide the actual or approximate value of the property. Provide the currency code applicable to this amount in field 4A. If the amount is in Canadian dollars, enter CAD as the currency code. If it is in United States dollars, enter USD. If the amount is in another type of foreign currency, see Appendix 1 in Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC for the code to use.

Field 5 Description of property

Provide any additional information about the property that is not already provided in the rest of the fields in Part C (and in Part D if the property involves an account).

If there is not enough room on the form to provide all the property identifier information for this property, attach a separate sheet to provide all the relevant information. It is very important that you indicate clearly on the separate sheet that this information belongs in field 5 of Part C.

Part D: Account information (if the property involves an account)

This part is for information about any account associated with the terrorist property. As explained earlier, it is possible to have more than one property per report. Provide the account information, where applicable, for each property included in the report.

If there is more than one account, complete a separate Part D for each one. To do this, you can copy Part D. Complete the "Account (number) of (total number of accounts in Part D)" area at the top to distinguish between each account, and identify the applicable property in the "Property (number)" area.

If none of the property in this report is associated to an account, do not complete Part D.

Field 1* Branch or transit number (if this Part is applicable)

Enter the branch number, transit number or other appropriate identifying number of the entity where the relevant account is held, if applicable to the property.

If the transaction being reported was proposed and, because of this, information for field 1 is not available, you can leave the field blank.

Field 2* Account number (if this Part is applicable)

Enter the number of the relevant account.

If the transaction being reported was proposed and, because of this, information for field 2 is not available, you can leave the field blank.

Field 3* Type of account (if this Part is applicable)

Indicate the type of the relevant account. If the selections provided do not cover this particular account, indicate "Other" and provide details in field 3D.

If the transaction being reported was proposed and, because of this, information for field 3 is not available, you can leave the field blank.

Field 4* Currency code (if this Part is applicable)

Enter the code for the type of currency for the relevant account. Enter CAD if Canadian dollars, or USD for United States dollars. If the account is another type of currency, see Appendix 1 in *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* for the currency code to use.

If the transaction being reported was proposed and, because of this, information for field 4 is not available, you can leave the field blank.

Field 5* Full name(s) of account holder(s) (if this Part is applicable)

Enter the full name of each account holder (up to three). If there are more than three, you do not need to provide more.

If the transaction being reported was proposed and, because of this, information for field 5 is not available, you can leave the field blank.

Field 6 Date opened

Enter the date (yyyy-mm-dd) the account was opened.

Field 7 Date closed

Enter the date (yyyy-mm-dd) the account was closed, if applicable.

Field 8* Status of the account (if this Part is applicable)

Indicate whether the account was active, inactive or dormant at the time you came to know that the property was terrorist property. If there was a transaction or a proposed transaction relating to the account, indicate the status of the account at the time the transaction was initiated or proposed.

The status of an account is determined by your policies and procedures. For example, your policy may be to assign inactive status to all accounts if there is no client activity for an account over a certain period of time, and dormant status if that inactivity is prolonged.

If you do not have such policies or procedures to assign inactive or dormant status to unused accounts, simply leave this field blank.

If the transaction being reported was proposed and, because of this, information for field 8 is not available, you can leave the field blank.

Part E1: Information about any transaction or proposed transaction (where applicable)

If there were any transactions or proposed transactions related to the terrorist property, you will have to complete Parts E1, E2 and F. Part E1 is for information about how the transaction was initiated or proposed to be initiated (that is, where the money or property came from). Part E2 is for information about how the transaction was completed or proposed to be completed (that is, where the money went). Part F is for information about the individual who conducted the transaction or proposed to conduct the transaction.

If the transaction was completed or proposed to be completed on behalf of anyone other than the individual in Part F, you will also have to complete Part G or H, as appropriate.

If there is more than one property in this report, you will have assigned a number to each property at the top of Part C. In this case, indicate to which one each transaction applies by completing the "Property (number)" area at the top of Part E1.

If there is more than one transaction to report, complete a separate Part E1 for each one. To do this, you can copy Part E1. Complete the "Transaction (number) of (total number of transactions in Part E)" area at the top of Part E1 to distinguish between each transaction. When you complete Parts E2 and F, as well as Part G or H, as applicable, indicate to which transaction that information applies.

If there was no transaction or proposed transaction related to any of the property described in Part C, Part E1 is not applicable. In this case, Parts E2, F, G and H would not be applicable either.

Field 1* Date of the transaction (if this Part is applicable)

Enter the date (yyyy-mm-dd) of the transaction. If the transaction was not completed, enter the date that the transaction was proposed.

The date of transaction field is mandatory. If the transaction was outside normal business hours, and you are not certain of the date, use the night deposit indicator field below (field 3).

Field 2 Time of transaction

Enter the time (hh:mm) of the transaction. If the transaction was not completed, enter the time that the transaction was proposed. The time of transaction field can be left blank if it is not available after reasonable efforts have been made.

Field 3* Night deposit indicator (if this Part is applicable)

If the transaction was outside normal business hours and you cannot provide the date in field 1, use the night deposit indicator field.

Field 4 Date of posting

Enter the date (yyyy-mm-dd) the transaction cleared, if this differs from the date of the transaction provided in field 1.

Field 5* Type of funds or other property involved in initiating transaction (if this Part is applicable)

Check the appropriate box to show the type of funds or other property involved in the transaction or the proposed transaction. For example, if your client brought in cash, "cash" is the type of funds or, if your client wanted to cash a life insurance policy, "negotiated life insurance policy" is the description of funds.

If none of the selections provided cover the particular transaction, indicate "Other" and provide details in field 5P. For example, if annuities were involved in initiating the transaction, indicate "Other" and provide information about the type of annuity in field 5P.

If there was more than one type of funds, indicate the one that best represents how the transaction was initiated or proposed to be initiated. Provide information about the rest of the types of funds on a separate sheet attached to the report. It is very important that you indicate clearly that this information belongs in field 5 of Part E1.

If the transaction being reported was proposed and, because of this, information for field 5 is not available, you can leave the field blank.

If you are a dealer in precious metals and stones, select the type of funds in field 5S that best describes what you received in the transaction, or what you were supposed to receive in a proposed transaction. If you were buying precious metals or stones, indicate the type of funds that best describes what you bought or proposed to buy. The same would apply if you were to receive precious metals or stones from a client for a trade-in sale. If you were selling precious metals or stones to a client, indicate the type of funds based on how the client paid or proposed to pay. For example, if the client paid cash, indicate "cash" or if the client paid by debit card or credit card, indicate "Other" and provide details in field 5P.

Field 6* Amount of transaction (if this Part is applicable)

Enter the total of funds or value of the property involved in the transaction. This is the total amount received to initiate the transaction. If this amount was not in Canadian funds, you do not have to convert it but you must provide the currency information in field 7.

You will provide details about what happened or was proposed to happen to that amount (that is, the disposition(s) of the transaction) in Part E2.

If the transaction being reported was proposed and, because of this, information for field 6 is not available, you can leave the field blank.

Field 7* Currency code (if this Part is applicable)

Enter the code for the currency of the transaction, even if it was in Canadian funds. Enter CAD if Canadian dollars, or USD for United States dollars. If the account is another type of currency, see Appendix 1 in Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC for the currency code to use.

If the transaction being reported was proposed and, because of this, information for field 7 is not available, you can leave the field blank.

Fields 8* and 9* Other institution, entity or individual name, number and account number (if this Part is applicable)

Provide the name (including the identification number, if applicable) and account number of any other institution or individual related to the funds or other property described in field 5, if applicable. For example, if cheques were involved in initiating the transaction, you would provide the name and number of the financial institution in field 8, and the chequing account number in field 9.

If more than one other individual or institution was involved, attach a separate sheet with the information for fields 8 and 9 for each additional individual or institution. It is very important that you indicate clearly on the separate sheet that this information belongs in Part E1, and clearly indicate what applies to field 8 and what applies to field 9.

Field 10* How was the transaction conducted? (if this Part is applicable)

Check the appropriate box to indicate how the transaction was conducted, or proposed to be conducted. For example, if the transaction was done through an automated banking machine, check the "Automated bank machine" box. If none of the selections provided cover this particular transaction, indicate "Other" and provide details in field 10G.

Field 11 ID number of the individual initially identifying a transaction for terrorist property

Enter the identification number of the individual who first identified the transaction relating to property owned or controlled by or on behalf of a terrorist or a terrorist group. If that individual does not have an ID number, this field may be left blank.

Part E2: Information about the transaction or proposed transaction disposition(s) (where applicable)

This Part is for information about how the transaction was completed or proposed to be completed.

If there is more than one transaction in this report, indicate to which property and which transaction this disposition applies in the "Property (number) Transaction (number)" area at the top of Part E2. These numbers should be the same as the ones assigned to the transaction in Part E1.

There could be more than one disposition for a particular transaction. For example, your client could propose to initiate a transaction in cash, send half of it as an electronic funds transfer (EFT) (disposition 1), and use the rest to purchase a bank draft (disposition 2). In that case, make sure you include the information for each disposition. If there is more than one disposition to report for any transaction, complete a separate Part E2 for each one. To do this, you can copy Part E2. Complete the "Disposition (number) of (total number of dispositions in this transaction)" area at the top of Part E2 to distinguish between each disposition.

You have to provide information about the individual conducting or proposing to conduct the transaction in Part F. If the disposition was on behalf of that same individual, check that box at the top of this Part.

If the disposition was on behalf of an entity (other than an individual), such as a partnership, corporation, trust or other entity, check that box and complete Part G to provide the information about the entity. If the disposition was on behalf of another individual, check that box and complete Part H to provide the information about the individual.

Field 12* Disposition of funds (if this Part is applicable)

This describes what happened, or what was proposed to happen, to the funds involved in the transaction.

Check the appropriate box to indicate how the transaction was completed, or proposed to be completed. If the disposition of funds was a life insurance policy purchase or deposit, check that box and provide the life insurance policy number in field 12D.

If none of the selections provided cover this particular disposition, indicate "Other" and provide details in field 12P. For example, if annuities were involved in the disposition of funds, indicate "Other" and provide information about the type of annuity in field 12P.

If the transaction being reported was proposed and, because of this, information for field 12 is not available, you can leave the field blank.

If you are a dealer in precious metals and stones, select the disposition of funds in field B12 that best describes what you paid or sold (or what you proposed to pay or sell) to the conductor of the transaction. If you were buying precious metals or stones, select the disposition of funds that best describes how you paid or proposed to pay for them. For example, if you paid in cash, indicate "cash out" or if you paid by cheque, indicate "Other" and provide details in field 12P. If you were selling precious metals or stones (including a trade-in sale), select the disposition of funds that best describes what your client purchased or proposed to purchase.

Field 13* Amount of disposition (if this Part is applicable)

Enter the amount of funds involved in the disposition. If the amount was not in Canadian funds, you do not have to convert it but you must provide the currency information in field 14.

If the transaction being reported was proposed and, because of this, information for field 13 is not available, you can leave the field blank.

Field 14* Currency code (if this Part is applicable)

Enter the code for the currency of the transaction, even if it was in Canadian funds. Enter CAD if Canadian dollars, or USD for United States dollars. If the account is another type of currency, see Appendix 1 in *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* for the currency code to use.

If the transaction being reported was proposed and, because of this, information for field 14 is not available, you can leave the field blank.

Fields 15* and 16* Other institution, entity or individual name, number and account number (where applicable, if this Part is applicable)

Provide the name (including the identification number, if applicable) and account number of any other institution or individual related to the disposition of funds described in field 12, if applicable. For example, if cheques were involved in the transaction's disposition, you would provide the name and number of the financial institution in field 15, and the chequing account number in field 16.

Also provide any policy number related to the other institution, entity or individual, in field 16, if applicable.

If more than one other individual or institution was involved, attach a separate sheet with the information for fields 15 and 16 for each additional individual or institution. It is very important that you indicate clearly on the separate sheet that this information belongs in Part E2, and clearly indicate what applies to field 15 and what applies to field 16.

If the transaction being reported was proposed and, because of this, information for fields 15 and 16 is not available, you can leave them blank.

Part F: Information about the individual who conducted or proposed to conduct transaction(s) (where applicable)

This part is for information about the individual who conducted the transaction, or who proposed to conduct the transaction.

If there is more than one transaction in this report, indicate to which property and which transaction this information applies by completing the "Property (number) Transaction (number)" area at the top of Part F. These numbers should be the same as the ones assigned to the transaction in Part E1. If there is more than one transaction to include in this report and they were not all conducted or proposed to be conducted by the same individual, complete a separate Part F for each individual. To do this, you can copy Part F. Complete the "Property (number) Transaction (number)" area at the top of Part F to distinguish between each individual who conducted or proposed to conduct a transaction.

If you are a dealer in precious metals and stones, the individual who conducted or attempted to conduct the transaction is the one from whom you were buying or to whom you were selling precious metals or stones.

Fields 1 to 3 Individual's full name

Enter the surname, given name and other name or initial (if known) of the individual who conducted or proposed to conduct the transaction.

Fields 1A to 3A Alias

Enter any alias that you know is used by the individual named in fields 1 to 3.

Field 4 Entity client number (where applicable)

Enter the client number you issued to the individual named in fields 1 to 3, if applicable.

Fields 5 to 9 Individual's full address

Enter the civic address, town or city, province or state, country and postal code of the individual named in fields 1 to 3.

Field 10 Country of residence

Enter the country of permanent residence of the individual named in fields 1 to 3.

Field 11 Home telephone number

Enter the home telephone number, including the area code, of the individual named in fields 1 to 3.

Field 12 Individual's identifier

Check the appropriate box to show the document used to identify the individual named in fields 1 to 3.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in field 12F.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field 12, but do not provide the number in field 13.

Field 13 ID number

Enter the number of the document described in field 12 that was used to identify the individual named in fields 1 to 3. Remember that a Social Insurance Number is not acceptable for this purpose, and neither is a health card number in some provinces.

Field 13A Citizenship

Enter the name of the country of citizenship of the individual named in fields 1 to 3.

Fields 14 and 15 Place of issue

Enter the province or state and country of issue of the document used to identify the individual named in fields 1 to 3.

Field 16 Date of birth

Enter the date (yyyy-mm-dd) of birth of the individual named in fields 1 to 3.

Field 17 Individual's occupation

Enter the occupation of the individual named in fields 1 to 3.

Field 18 Individual's business telephone number

Enter the business telephone number, including the area code, of the individual named in fields 1 to 3. Include the extension, if applicable, at field 18A.

Field 19 Individual's employer

Enter the name of the entity or individual who is the employer of the individual named in fields 1 to 3.

Fields 20 to 24 Employer's business address

Enter the civic address, town or city, province or state, country and postal code of the employer of the individual named in fields 1 to 3.

Field 25 Employer's business telephone number

Enter the business telephone number, including the area code, of the employer of the individual named in fields 1 to 3. Include the extension if applicable at field 25A.

Part G: Information about the entity on whose behalf the transaction was conducted or proposed to be conducted (where applicable)

This part only applies if the transaction's disposition was conducted, or proposed to be conducted, on behalf of a third party other than an individual, as you indicated in Part E2, above field 12. This includes an entity such as a business, corporation or trust, or any other entity that is not an individual.

Complete a separate Part G for each entity on whose behalf a disposition was conducted or proposed to be conducted. To do this, you can copy Part G. Complete the "Property (number) Transaction (number) Disposition (number) " area at the top of Part G to distinguish between each disposition, based on the number you assigned the disposition in Part E2.

Field 1 Name of corporation, trust or other entity

Enter the full name of the corporation, trust or other entity (such as a partnership, etc.) on whose behalf the transaction was conducted or proposed to be conducted.

Field 2 Type of business

Describe the type of business for the entity named in field 1.

Fields 3 to 7 Full address of entity

Enter the civic address, town or city, province or state, country and postal code of the entity named in field 1.

Field 8 Business telephone number

Enter the telephone number, including the area code, of the entity named in field 1. Include the extension, if applicable, at field 8A.

Fields 9 to 11 Incorporation information (where applicable)

Provide the incorporation number, where applicable, for the corporation named in field 1. Also provide the province or state and country of the incorporation number's place of issue.

Field 12 Signing authority names

Provide the names of up to three individuals who have authority to conduct transactions through the account of the entity (if an account is involved in the transaction).

Part H: Information about the individual on whose behalf the transaction was conducted or proposed to be conducted (where applicable)

This part only applies when the transaction's disposition was conducted, or proposed to be conducted, on behalf of a third party that is an individual, as you indicated in Part E2, above field 12.

If the individual conducted or proposed to conduct the transaction's disposition on his or her own behalf, this part does not apply. In that case, information about the individual should be provided in Part F. If the transaction's disposition was conducted on behalf of an entity (that is, not an individual), Part G should be completed.

Complete a separate Part H for each individual on whose behalf a disposition was conducted or proposed to be conducted. To do this, you can copy Part H. Complete the "Property (number) Transaction (number) Disposition (number)" area at the top of Part H to distinguish between each disposition, based on the number you assigned the disposition in Part E2.

Fields 1 to 3 Individual's full name

Enter the last name, first name and middle initial (if applicable) of the individual on whose behalf the transaction was conducted or proposed to be conducted.

Fields 1A to 3A Individual's alias (where applicable)

Enter any alias that you know is used by the individual named in fields 1 to 3.

Fields 4 to 8 Individual's full address

Enter the civic address, town or city, province or state, country and postal code of the individual named in fields 1 to 3.

Field 9 Home telephone number

Enter the home telephone number, including the area code, of the individual named in fields 1 to 3.

Field 10 Office telephone number

Enter the office telephone number, including the area code, of the individual named in fields 1 to 3. Include the extension if applicable at field 10A.

Field 11 Date of birth

Enter the date (yyyy-mm-dd) of birth of the individual named in fields 1 to 3.

Field 12 Individual's identifier

Check the appropriate box to show the document used to identify the individual named in fields 1 to 3.

You can refer to an individual's provincial health card, provided there is no provincial or territorial legislation preventing you from using or requesting it.

If the selections provided do not cover the identifier used, indicate "Other" and provide details in field 12F.

Please note that although a Social Insurance Number (SIN) card can be used for identification purposes for transactions such as the opening of an account, the SIN (i.e., the number) should not be provided on this form. If you used a SIN card and no other identifying document for the individual, indicate **SIN card** in the "Other" area of field 12, but do not provide the number in field 13.

Field 13 ID number

Enter the number of the document described in field 15 that was used to identify the individual named in fields 1 to 3. Remember that a Social Insurance Number is not acceptable for this purpose, and neither is a health card number in some provinces.

Fields 14 and 15 ID place of issue

Enter the province or state and country of issue of the document used to identify the individual named in fields 1 to 3.

Field 16 Country of residence

Enter the country of permanent residence of the individual named in fields 1 to 3.

Field 16A Citizenship

Enter the name of the country of citizenship of the individual named in fields 1 to 3.

Field 17 Individual's occupation

Enter the occupation of the individual named in fields 1 to 3.

Field 18 Individual's employer

Enter the name of the entity or individual who is the employer of the individual named in fields 1 to 3.

Fields 19 to 23 Employer's business address

Enter the civic address, town or city, province or state, country and postal code of the employer of the individual named in fields 1 to 3.

Field 24 Employer's business telephone number

Enter the business telephone number, including the area code, of the employer of the individual named in fields 1 to 3. Include the extension if applicable at field 24A.

Field 25 Relationship of the individual named in Part F to the individual named above (fields 1 to 3)

Check the appropriate box to indicate the relationship of the individual who conducted or proposed to conduct the transaction (that is, the individual named in fields 1 to 3 of Part F) to the individual named in fields 1 to 3 (of Part H).

If none of the selections provided cover the relationship, indicate "Other" and provide details in field 25J.

CHAPTER 20

Appendix N— Self-Review Checklist

Part A: Compliance Framework Evaluation

Requirements	Status	Comments
Compliance Officer		
Has the Compliance Officer been appointed, in writing, to their role?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is the Compliance Officer independent of operations?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is the job description of the Compliance Officer described in writing, in sufficient detail, with documented accountability for AML/ATF program content and design?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the Compliance Officer have: <ol style="list-style-type: none"> 1. appropriate qualifications 2. knowledge of regulatory requirements 3. money laundering subject matter expertise and reference to policies 4. adequate resources to achieve program objectives 5. documented unfettered access to Senior Management, the Board, and all information and individuals throughout the organization 	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is there a substitute Compliance Officer in case of absence by the primary?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Requirements	Status	Comments
Policies and Procedures		
Do policies incorporate all the objectives and responsibilities imposed by the legislation, including a risk management mandate?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do procedures address the nature, timing, responsibilities, process and persons involved for all legislative requirements applicable to the organization, including: <ol style="list-style-type: none"> 1. record keeping 2. client identification (personal and non-personal) and prohibitions on accepting or dealing with clients where identification does not occur 3. risk based approach measures required mandated by law, and elected by your organization 4. suspicious transaction reporting 5. tipping-off prohibitions 6. large cash transaction reporting 7. compliance program requirements (including RBA documentation, the appointment of a compliance officer; the maintenance of up-to-date policies and procedures; the requirement for a bi-annual compliance review; the requirement for ongoing training for all employees and agents) 	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Have the policies and procedures been approved by a senior officer of the organization?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Risk Assessment & Risk Based Approach		
Has an inherent risk assessment been conducted and include the following prescribed factors: <ol style="list-style-type: none"> 1. clients and business relationships 2. products and delivery channels 3. geographic location of the activities 4. other relevant factors 	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Based on the above inherent risk assessment, are all areas classified into respective risk levels?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the Risk Based Approach (RBA) documentation contain the minimum required components? <ol style="list-style-type: none"> 1. documented inherent risk assessment 2. risk mitigation strategy 	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Requirements	Status	Comments
Does the documented risk mitigation strategy address all higher risk areas identified in the inherent risk assessment to a level acceptable by the organization, with at least the minimum standards imposed by the legislation (ongoing monitoring and client identification updates)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are risk mitigation measures integrated into policies and procedures?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Have the relevant employees been trained appropriately in the reason and application of risk mitigation measures?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are policies and procedures adopted for risk mitigation strategies being followed?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are risks being managed within organizational tolerance levels (are controls meeting their objective/ resulting in the expected outcome)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are resource allocations appropriate given inherent risk assessment findings and risk mitigation experience?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Training		
Does the organization have a documented training program which specifies: 1. Who is to be trained 2. With what frequency will the training occur to satisfy the ongoing nature of the program 3. How will the content be used for training 4. What restrictions, if any, will be placed on staff prior to successfully completing the training 5. How will content retention be evaluated and documented 6. On what basis will employees and agents be exempted from training	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the training content include at least: 1. background on money laundering risks 2. AML/ATF requirements including identifying reportable transactions 3. consequences of non-compliance and potential fines/penalties 4. organizational policies and procedures	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are there enhanced training requirements for the Compliance Officer?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Requirements	Status	Comments
Effectiveness Review		
Has an effectiveness review been conducted within two years of the previous review?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is the effectiveness review conducted by a person or firm independent of the organization's operations?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is the effectiveness review conducted by a person or firm with expertise in the AML/ATF Regulations, money laundering risks, and an understanding of the organization's operations?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the effectiveness review document specify a definition for effectiveness, the standards against which it evaluates effectiveness, its scope, methodology, findings, recommendations, and management undertakings to the recommendations?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Has the effectiveness review evaluated the effectiveness of: <ol style="list-style-type: none"> 1. policies and procedures (conformance to relevant standards and operational adherence) 2. the risk assessment and risk-based approach 3. the risk mitigation program 4. training 	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Has the effectiveness review report been presented to a senior officer within 30 days after the assessment along with any updates, if applicable, made to policies and procedures within the reporting period and the status of implementing any changes, if applicable, to policies and procedures?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Part B: Operational Compliance Evaluation

Requirements	Status	Comments
Client Identification		
Are legislative and internal standards being adhered to for the acceptance of personal clients (e.g. valid identification with details recorded)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are legislative and internal standards being adhered to for the acceptance of business clients (e.g. timing, extent of documentation)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are legislative and internal standards being adhered to for the acceptance of not-for-profit clients?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are enhanced identification processes being followed for higher risk clients?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are non-face-to-face standards being adhered to in cases where the client or their signing authority is not physically present when identifying themselves?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is client information being updated for higher risk clients?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Is third party determination conducted and documented in the required circumstances?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Large Cash Transaction Reporting (LCTR)		
Does the organization have an effective system in place to detect individual transactions, and combinations of transactions (24 hour rule) which require reporting?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are all reportable transactions reported within the prescribed time-frame and with all the required details (timing and quality of reporting)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Suspicious And Attempted Suspicious Transaction Reporting (STR)		
Does the organization have effective systems and training in place for the detection of transactions, attempted transactions and combinations of transactions which require reporting?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the organization have an effective system in place to evaluate and document unusual transactions, whether attempted or completed, put forward by employees and technology?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Requirements	Status	Comments
Is the rationale from the evaluation of unusual transactions fully documented? For both reported suspicious transactions and unreported transactions not deemed to be suspicious?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are all reportable transactions reported within the prescribed timeframe and with all the required details (Timing and Quality of reporting)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Have reasonable measures been taken to ascertain the identification of the subjects within all STRs?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Have suspicious and attempted suspicious transactions been linked to risk assessment and risk mitigation measures?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Terrorist Property Reporting (TPR)		
Does the organization have effective systems and training in place for the detection of transactions and property which require reporting?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does the organization have an effective system in place to evaluate and document potentially reportable transactions and property?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are all reportable transactions and properties reported to FINTRAC, CSIS and the RCMP within the prescribed timeframe and with all the required details?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Record-Keeping and Retention		
Are the prescribed records retained for a period of at least five years, in a way that allows for their retrieval within 30 days of a request by FINTRAC?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are sufficient details kept about the following transactions and situations at the prescribed thresholds: <ol style="list-style-type: none"> 1. large cash transaction records 2. receipt of funds records 3. copies of official corporate records 4. copies of suspicious transaction reports 	<input type="checkbox"/> YES <input type="checkbox"/> NO	

About the Author

Matthew McGuire, MAcc, CPA, CA, DIFA, CAMS, AMLP

Matthew McGuire is a Chartered Professional Accountant who leads the National Anti-Money Laundering (AML) Practice and the Investigative and Forensic Services Group in Ontario for MNP LLP. He is also the founder and Director of Seneca College's Canadian Institute for Financial Crime Analysis, a member of the Department of Finance's Public/Private Sector Advisory Committee on AML/ATF (Anti-Terrorist Financing), Chair of CPA Canada's AML Committee and a member of the Credit Union Central of Canada's AML Committee.

Together with his team of full-time dedicated AML specialists in offices across Canada, Matthew leverages his regulatory and investigative experience to empower companies and governments with regulatory compliance and financial crime risk mitigation strategies, guide them through regulatory exams and interventions, assist them with financial crime investigations, and provide them with litigation support.

Since his time as an intelligence analyst with FINTRAC, Matthew has been speaking regularly on the topic of money laundering and financial crime to reporting entities, law enforcement, prosecutors, financial intelligence units, universities, conferences, and authors articles for periodicals.

He holds an Honours Bachelor of Arts and a Master of Accounting degree from the University of Waterloo. In 2005, he completed the 2-year Diploma in Investigative and Forensic Accounting program at the University of Toronto. He is certified as an Anti-Money Laundering Specialist (CAMS) by the Association of Certified Anti-Money Laundering Specialists, and is accredited as an Anti-Money Laundering Professional (AMLP) by the Bank Administration Institute. Matthew has been qualified and admitted by the Ontario Superior Court of Justice as an expert witness in forensic accounting and money laundering, and has testified before Senate committees and the House of Commons Finance Committee on matters related to money laundering legislation.



CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA