GUIDANCE FOR THE

LEGAL SECTOR:

AML/CFT/CPF/TFS

Version 2.2
January 2021

Version	Date	Purpose/Change
1.0	September 2019	Issued
2.0	January 2020	Sections updated to include elements of the new Terrorism Financing Risk Assessment and a section on identifying proliferation financing risks.
2.1	October 2020	Formatting review and grammatical corrections
2.2	January 2021	Section 4.6 Ongoing Monitoring updated.

Cayman Attorneys Regulation Authority

Anti-Money Laundering, Counter Terrorist Financing, Proliferation Finance and Targeted Financial Sanctions

Guidance for the Legal Sector
2020

Contents

Glossary

Term	Meaning
AIM	Alternative Investment Market
AML/CFT/CPF	Anti-Money Laundering/Counter the Financing of Terrorism/Counter Proliferation Financing
AMLSG	Anti-Money Laundering Steering Group
CARA	Cayman Attorneys Regulation Authority
CDD	Client Due Diligence
CFATF	Caribbean Financial Action Task Force
CIMA	Cayman Islands Monetary Authority
DNFBP	Designated Non-Financial Businesses and Professions
DPL	Data Protection Law
FATF	Financial Action Task Force
FRA	Financial Reporting Authority
FSP	Financial Service Provider
IBA	International Bar Association
LLP	Limited Liability Partnership
LPP	Legal Professional Privilege
MLRO	Money Laundering Reporting Officer
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
NRA	National Risk Assessment
PEP	Politically Exposed Person
PFPL	Proliferation Financing (Prohibition) Law (2017 Revision)
POCL	Proceeds of Crime Law (2020 Revision)
SAR	Suspicious Activity Report
TL	Terrorism Law (2018 Revision)
UN	United Nations

Definitions

Applicant	A person who wishes to become a client of a Practice, but has not yet been accepted by the Practice as such
Beneficial Owners	See chapter 4
Business Relationship	Any arrangement between two or more persons where: - the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis; and - the total amount of any payment or payments to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made
Constable	Has the meaning assigned to it in the Police Law (2017 Revision)
Criminal Conduct	Conduct which constitutes an offence in any part of the Cayman Islands, or would constitute an offence in any part of the Cayman Islands if it occurred there. See Section 144(2) of the POCL
Criminal Property	Property which constitutes, or represents, a person's benefit from criminal conduct (in whole or part and whether directly or indirectly), where the alleged offender knows or suspects that it is such and includes terrorist property. See Section 144(3) of the POCL and the definition of property
CDD	See chapter 4
Disclosure/SAR	A report made to the FRA in accordance with Sections 136 and 137 of the POCL
Dollar or $	Cayman Islands dollars
Inter Vivos Trust	A trust which takes effect while a person is alive. Also referred to as a Living Trust
LPP	See chapter 7.4
Nominated Officer/MLRO	A person nominated within the Practice to make disclosures to the FRA under the POCL
One-Off Transaction	A transaction (carried out other than in the course of an established business relationship formed by a person conducting relevant financial business ("**RFB**")) amounting to CI$15,000 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 Cayman Islands. It is not necessary that the original ML/TF/PF offence from which the proceeds stem was committed in the Cayman Islands, if the conduct contravenes the law of the country in which it occurred and would also constitute an offence had it taken place within the Cayman Islands. There is no duty imposed on a financial service provider ("**FSP**") (such as a Practice) to inquire into the criminal law of another country in which the conduct may have occurred. However, an FSP (such as a Practice) should be aware of and understand the laws of those jurisdictions in which it operates. The question is whether the conduct amounts to an indictable offence in the Cayman Islands or would if it took place in the Cayman Islands. An FSP (such as a Practice) is not expected to know the exact nature of criminal activity concerned or that the particular funds in question are definitely those which flow from the crime.
PEP	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
Privileged Circumstances	See chapter 6.7.2
Property	Includes money and all other property, whether real or personal, including things in action and other intangible or incorporeal property. See Section 2 of the POCL
Regulated Sector	Activities, professions, and entities regulated for the purposes of AML/CFT/CPF obligations - see chapter 1
Regulations	Anti-Money Laundering Regulations (2020 Revision), as amended
Tax Adviser	A Practice which 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 from the commission of acts of terrorism or which has been used or is reasonably suspected to have been used, directly or indirectly, in the commission of an act of terrorism

Trust or Company Service Provider	A Practice or person licenced or regulated in the Cayman Islands to provide any of the following services to other persons: - forming companies or other legal persons; - 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 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; or - 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 another person other than a company listed on a regulated market when providing such services

Acknowledgements

This Guidance draws heavily on the work of the Legal Sector Affinity Group in the UK.

Further, reliance is placed on CIMA Guidance Notes, the Cayman Islands National Risk Assessment (as updated) and the CFATF Mutual Evaluation Report 2019.

Chapter 1 - Overview

1.1 Who should read this Guidance?

All independent legal professionals and other staff in a Practice who secure compliance in the fields of anti-money laundering, counter terrorist financing, counter proliferation finance and targeted financial sanctions ("**AML/CFT/CPF/TFS**").

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 by a sole practitioner, or in a self-employed capacity or operates under another structure. For attorneys in a law firm, the term 'practice' refers to their firm or business as a whole and not a practice group within a firm.

As used in this Guidance, “you” means independent legal professionals. There is no distinction made between "lawyers" or "attorneys" in the Cayman Islands.

1.2 What is the issue?

Independent legal professionals are key actors in the business and financial world, facilitating vital transactions that underpin the Cayman Islands economy. 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, terrorist financing and proliferation financing ("**ML/TF/PF**") are serious threats to society, causing a loss of revenue, endangering life, and fuelling other criminal activity.

This Guidance aims to assist independent legal professionals to meet their obligations under the Cayman Islands’ AML/CFT/CPF/TFS regime.

Summary of Vulnerabilities Faced by Attorneys

This Guidance takes note of the National Risk Assessment (as updated) ("**NRA**") and Caribbean Financial Action Task Force ("**CFATF**") Mutual Evaluation Reports.

Some of the vulnerabilities present in the Cayman Islands legal sector include:

- directly participating in problematic transactions or using their client accounts for improper purposes;
- attorneys being sought to provide a cover of respectability to problematic legal arrangements and entities by acting as trustees or directors for those entities;
- playing the key role in forming and structuring legal entities and arrangements, such that they effectuate the mechanisms by which criminals and terrorists can facilitate and obscure their activities through these vehicles;
- effectuating the transfer of properties, funds and assets, especially in those markets such as real estate and luxury goods which are well-known targets of money-launderers;
- the prevalence of corporate and private wealth practice areas where the purpose and the beneficiaries of asset transfers can be obscured by the involvement of complex chains of transactions, vehicles and intermediaries; and
- participating in 'sham litigation' where a seemingly contentious matter is actually a contrivance for the transfer of funds between parties.

1.3 Definition of money laundering

ML is the process by which the direct or indirect benefit of crime is channelled through the economy/financial system to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the funds/proceeds in the financial system without arousing any suspicion, moves it in a series of complex transactions to disguise its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately.

The definition of ML in the POCL is sufficiently broad that it includes not only committing the offences considered in this Guidance, but also an attempt, conspiracy or incitement to commit such an offence, as well as aiding, abetting, counselling or procuring the commission of such an offence. Finally, overseas conduct which would constitute an offence (or an attempt, conspiracy or incitement to commit such an offence, as well as aiding, abetting, counselling or procuring the commission of such an offence) if committed in the Cayman Islands, will also constitute money laundering. See Section 144(10) of the POCL.

There is no single method of ML. However, there are acknowledged phases to ML: placement, layering and integration.

1.3.1 Placement

Proceeds generated from criminal activity are placed in the financial system. This is the point when proceeds of crime are most apparent and easiest to detect. Because banks and financial institutions have developed AML procedures, criminals often look for other ways of placing cash into 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 separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. 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 by layering, the criminal is able to make the funds appear legitimate. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. For example, this can be done by investing funds in legitimate businesses or other forms of investment, often 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 ML.

1.4 Legal framework and other requirements

1.4.1 Financial Action Task Force

The FATF was created in 1989 at 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, the FATF released its 40 recommendations for fighting ML. Between October 2001 and October 2004, it released nine further special recommendations to prevent TF. The recommendations were revised in February 2012. The revised recommendations now fully integrate CFT measures with AML controls and, among other things, seek to address new and emerging threats better and to clarify and strengthen many of the existing obligations, including PF, the laundering of the proceeds of corruption and tax crimes.

The CFATF has associate status with FATF and is made up of states and territories of the Caribbean Basin that have agreed to implement measures against ML/TF/PF, including the Cayman Islands.

1.4.2 Proceeds of Crime Law (2019 Revision)

Scope

The POCL establishes a number of ML offences including:

- the principal ML offences;
- the offences of failing to report suspected ML; and
- the offence of tipping off.

See Chapter 6 for further discussion of ML offences.

Application

The POCL applies to all persons, although certain offences only apply to nominated officers. See Section 137 of the POCL.

Under Schedule 6 of the POCL, key activities which may be relevant to independent legal professionals are legal services provided in the course of business relating to:

- the sale, purchase or mortgage of land or interests in land on behalf of clients;
- management of client money, securities or other assets;
- organisation of contributions for the creation, operation or management of companies;
- management of bank, savings or securities accounts; and
- the creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

Chapters 6, 7 and 9 of this Guidance provide more details on the obligations of independent legal professionals under the POCL.

1.4.3 Terrorism Law (2018 Revision)

Scope

The TL establishes several offences about engaging in or facilitating terrorism and raising or possessing funds for terrorist purposes. It contains duties similar to those found under the POCL, in Sections 23 and 25 (and Schedule 1), which apply where a person knows, suspects or has reasonable grounds to suspect that someone has committed an offence under the TL (i.e. has had dealings with terrorist property). However, because the term "criminal property" under the POCL now includes "terrorist property" and the term "money laundering" under the Anti-Money Laundering Regulations (2018 Revision) (as amended) ("**Regulations**") includes terrorism offences, reports in relation to terrorism or dealings with terrorist property can be

made under the POCL regime.

Read about these provisions in Chapter 8.

Application

Section 23 of the TL relates to persons in an unregulated business knowing or suspecting (subjective) and Schedule 1 relates to persons in regulated business knowing, suspecting (subjective) or having reasonable grounds to suspect (objective) a TL offence (e.g. using terrorist property or arranging for property to be used for terrorist purposes).

Disclosure (i.e. a report) should be made to the FRA and will not be treated as a breach of any statutory or civil duty of confidentiality.

Chapters 8 and 9 provide more detail on the obligations of independent legal professionals under the TL.

1.4.4 The Regulations and Guidance Notes

Scope

The Regulations came into force on 31 December 2019 and repealed the prior Regulations. The Regulations were promulgated under the POCL and therefore have the force of law. They set out administrative requirements for the AML regime within the regulated sector and outline the scope of Client Due Diligence ("**CDD**").

The Regulations aim to limit the use of professional services for ML by requiring professionals to know their clients and to monitor the use of their services by clients.

The Regulations and the POCL both permit the creation of guidance in order to assist in the implementation of procedural obligations. The Cayman Attorneys Regulation Authority ("**CARA**"), in its capacity as an independent regulatory arm established by CILPA, subsequently issued this Guidance in accordance with Section 55D of the Regulations, which state that a supervisory authority may issue guidance, directives and procedures to be followed by DNFBPs, in order to promote compliance with the Regulations.

Application

The Regulations apply to persons carrying out RFB. What constitutes RFB is set out under Section 2 of the POCL and includes the following:

1. banking or trust business carried on by a person who is licensed under the Banks and Trust Companies Law (2020 Revision) (as amended);
2. acceptance by a building society of deposits (including the raising of money from members of the society by the issue of shares);
3. business carried on by a co-operative society within the meaning of the Co-operative Societies Law (2020 Revision) (as amended);

4. insurance business and the business of an insurance manager, an insurance agent, or an insurance broker within the meaning of the Insurance Law, 2010 (as amended);

5. mutual fund administration or the business of a regulated mutual fund within the meaning of the Mutual Funds Law (2020 Revision) (as amended);

6. company management business as defined by the Companies Management Law (2018 Revision) (as amended); and

7. activities falling within Schedule 6 of the POCL, which include:

    (i) acceptance of deposits and other repayable funds from the public;

    (ii) lending;

    (iii) financial leasing;

    (iv) money or value transfer services;

    (v) issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money);

    (vi) financial guarantees and commitments;

    (vii) trading in:

        a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);

        b) foreign exchange;

        c) exchange, interest rate and index instruments;

        d) transferable securities; or

        e) commodity futures trading;

    (viii) participation in securities issues and the provision of financial services related to such issues;

    (ix) advice to undertakings on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings;

    (x) money broking;

    (xi) individual and collective portfolio management advice;

    (xii) safekeeping and administration of cash or liquid securities on behalf of other persons;

    (xiii) safe custody services;

    (xiv) financial, estate agency (including real estate agency and real estate brokering), legal and accounting services provided in the course of business relating to:

        a) the sale, purchase or mortgage of land or interests in land on behalf of clients;

        b) management of client money, securities or other assets;

        (ba) organisation of contributions for the creation, operation or management of companies;

        c) management of bank, savings or securities accounts; and

        d) the creation, operation or management of legal persons or arrangements, and buying and selling of business entities;

    (xv) undertaking property development within the meaning set out in Section 2 of the

Trade and Business Licensing Law (2019 Revision) and the subsequent sale of that property without using a real estate agent or broker;

(xvi) undertaking property investment without using a real estate agent or broker;

(xvii) the services of listing agents and broker members of the Cayman Islands Stock Exchange ("**CSX**") as defined in the CSX Listing Rules and the Cayman Islands Stock Exchange Membership Rules respectively;

(xviii) the conduct of securities investment business (as defined under the Securities Investment Business Law (2020 Revision);

(xix) dealing in precious metals or precious stones, when engaging in a cash transaction that is equivalent to fifteen thousand United States dollars or more;

(xx) the provision of registered office services to a private trust company by a company that holds a Trust licence under Section 6(5)(c) of the Banks and Trust Companies Law (2020 Revision);

(xxi) otherwise investing, administering or managing funds or money on behalf of other persons; and underwriting and placement of life insurance and other investment related insurance;

(xxii) providing virtual asset services; and

(xxiii) operating a single family office.

Application

This Guidance applies to firms of attorneys at law regulated by CARA. The Guidance is also intended to assist legal professionals more generally in respect of their wider obligations relating to TF, PF, reporting suspicious activity and TFS. In particular, the Guidance will assist when a legal professional participates in financial or real property transactions concerning:

- the sale, purchase or mortgage of land or interests in land on behalf of clients;
- management of client money, securities or other assets;
- management of bank, savings or securities accounts;
- the creation, operation or management of legal persons or arrangements, and buying and selling of business entities; and
- organisation of contributions for the creation and operational management of companies.

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 and this Guidance must be applied by attorneys when they carry out the above listed activities for third parties. It is noted that litigation is not an activity listed and therefore the Regulations do not apply to litigation-only clients.

The Regulations and this Guidance do not apply where a person provides legal services 'in house' as an employee of an entity that does not provide legal services.

The Regulations also clearly state that 'firms of attorneys at law' do not include persons who provide legal services to the Government.

Activities covered by the Regulations

In terms of the activities covered, you should note that:

- managing client money is a narrower concept than handling it;
- opening or managing a bank account is different to simply opening a client account;
- it is likely that "management of bank, savings or securities account" will cover a legal professional acting as a nominee shareholder, trustee, receiver, or acting pursuant to a power of attorney; and
- it is likely that management of client money, securities or other assets will cover safe custody services and safety deposit box services.

Activities not covered by the Regulations

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.

1.5 Status of this Guidance

This Guidance contains best practice guidance on complying with AML/CFT/CPF obligations.

This Guidance is issued by CARA which is the AML Supervisor for the legal sector, under a formal delegation from CILPA.

This Guidance is not legal advice and does not necessarily provide a defence to complaints of misconduct or inadequate professional service.

CARA will consider whether a legal professional has complied with this Guidance when undertaking its role as supervisor of professional conduct, and as a supervisory authority for the purposes of the Regulations.

Pursuant to Regulation 55S, this Guidance will be considered when deciding whether to impose a fine and the amount of the fine.

In determining compliance with the Regulations, a court will consider regulatory guidance such as the Guidance.

While care has been taken to ensure that this Guidance is accurate, up to date and useful, neither the staff nor Board of CARA will accept any legal liability in relation to this Guidance.

1.6 Terminology in this Guidance

Must

A specific requirement in legislation: you must comply unless specific exemptions or defences are provided in relevant legislation.

Should

Outside of a regulatory context, good practice for most situations in CARA'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 or your practice. However, if you do not follow the suggested route, you should be able to justify to CARA 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 by CARA to justify why this was an appropriate option.

Chapter 2 - Risk-based approach

2.1 General comments

The possibility of being used, including unwittingly, as a conduit for money laundering and terrorist financing or proliferation 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; and
- damage to reputation leading to a loss of business.

These AML/CFT/CPF risks must be appropriately identified, assessed and mitigated, just as you would 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 ("**RBA**") to preventing ML/TF/PF means that you can 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 ML/TF/PF methods change.

The RBA does not apply to reporting suspicious activity, because the POCL, the TL and the Proliferation Financing (Prohibition) Law (2017 Revision) ("**PFPL**") 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 RBA still applies to ongoing monitoring of clients and retainers and this will enable you to identify suspicions.

ML/TF/PF 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 members of the Practice are subject; and
- the susceptibility of the activities of your Practice to ML/TF/PF in the particular countries in which your Practice operates.

2.2 Requirement to undertake and maintain a Practice-wide risk assessment

Under Regulation 8(1), an independent legal professional's Practice is required to carry out and maintain a documented Practice-wide risk assessment to identify, assess and understand the risk of ML/TF to which the business is subject.

You must:

- take appropriate steps to identify, assess and understand the ML/TF risks your business faces;
- apply an RBA to compliance with CDD obligations, and to the monitoring of financial activities which would include categories of activities that are considered to be of a high risk;

- have documented policies, controls and procedures that enable the Practice to manage, monitor and mitigate effectively the different risks that have been identified; and
- ensure the residual risk is acceptable for the Practice.

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.

Although Regulation 8(1) does not currently make explicit reference to PF, you need to assess these risks with a view to implementing appropriate ongoing monitoring procedures for the purposes of preventing, countering and reporting PF as required under Regulation 5.

2.3 Assessing your Practice's risk profile

In carrying out your practice-wide risk assessment you must consider:

- risk factors relating to:
  - your clients;
  - the countries or geographic areas in which your clients operate;
  - your products or services;
  - your transactions; and
  - your delivery channels;
- the nature of any issues raised in suspicious activity reports ('**SARs**') made by your Practice's MLRO (consult the key contact in your Practice to understand any risks he/she may have identified).
- the NRA (the Cayman Islands Government conducted an NRA in 2014/2015 and published a summary of the results which can be found at:

  http://www.gov.ky/portal/page/portal/cighome/help/features/Summary%20Results%20of%20the%20CINRA%20relating%20to%20MLTFPF.pdf)
- the FATF Risk-based Approach Guidance for Legal Professionals;
- sector risk assessments produced by CARA;
- if you provide services in any other jurisdictions, any relevant FATF mutual evaluations, NRAs, 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.

Red Flags with Warning Signs for Attorneys:

a) The transaction is unusual if, for example:
   - the nature of the instruction is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting; or
   - there are remarkable and highly significant differences between the declared price and the actual values in accordance with any reference which could give an idea of this value, or in the judgement of the legal professional there is an obvious disparity.

b) 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.

c) The source of funds is unusual:

- funds received from or sent to a foreign country when there is no apparent connection between the country and the client; or
- funds received from or sent to high-risk countries.

d) Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

e) 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.

f) The collateral being provided for the transaction is currently located in a high-risk country.

g) 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.

h) There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.

i) 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, with no logical explanation.

j) 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.

k) Large financial transactions, especially if proposed 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.

Having assessed the ML/TF/PF 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.

The risk and vulnerabilities relating to the activities of attorneys have been assessed in relation to the following areas outlined in the FATF 40 recommendations:

- purchase and sale of real estate;
- management 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
- purchase and sale of business entities.

2.3.1 Client risk factors

When assessing risk factors relating to your clients 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 versus stable client base

Although not determinative, you should consider 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 ML issues, which may mean your Practice is at a lower risk of being subject to ML/TF/PF (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 ML/TF/PF risks your Practice faces. Where your clients or the beneficial owners of your clients are based or operate their business in high-risk jurisdictions, this should be reflected in your risk assessment.

High-risk country or geographic area risk factors include the following:

- countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF and MoneyVal, as not having adequate AML/CFT/CPF systems;
- countries subject to sanctions, embargos or similar measures issued by, for example, the UN or EU;
- countries identified by credible sources as having significant levels of corruption or other criminal activity; and/or
- countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country or the geographic area.

Conversely, where your clients or the beneficial owners of your clients are based or operate their business in low risk jurisdictions this should be considered in your risk assessment.

Low-risk country or geographic area risk factors include:

- countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT/CPF systems; and/or
- countries identified by credible sources as having a low level of corruption or other criminal activity.

The 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 ML/TF/PF 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/CFT/CPF 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).

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, UN or EU sanctions.

You should pay particular attention to the level of risk assigned to the relevant sector by the NRA or relevant supervisory authority including CARA. While not all work in such sectors will represent higher risk, 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.

The NRA results assessed the following sectors as follows:

Sector	**Vulnerability Level**
Insurance	Medium
Banking	Medium High
Securities	Medium High
Other Financial Institutions	Medium
Lawyers	Medium
Accountants	Medium Low
Real Estate	Medium
Dealers of Precious Metals and Precious Stones	Medium
Trust and Corporate Service Providers	Medium

2.3.1.4 Acting for politically exposed persons

An independent legal professional's exposure to politically exposed persons ("**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, if any, 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 certain firms 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
- management of assets
- 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 Practice 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 Practice so that you can put in place additional controls where necessary to minimise the risk of ML/TF/PF.

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 ML 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 ML. 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 and companies

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 ML. 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 registry, 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 (i.e. there is no actual claim and the litigation is 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 an RBA and avoiding 'tick the 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 as set out in the Code of Conduct for Cayman Islands Attorneys-at-Law.
- Prohibit the use of your client account without 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 from an account in their name, from the Cayman Islands or from 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 ML. 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 ML taking place and whether it is a circumstance requiring a disclosure to the FRA.
- Monitor, through accounts staff (where applicable), 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 are 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 file a **SAR**. 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.
- Remain vigilant. Information overload can be a warning sign. Money launderers may attempt to inundate the legal professional with information to reduce the chances that the professional spots the issue or to convince the professional that the transaction is legitimate.

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 that you 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 and proposed uses of the structure to be created.

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 ML 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 ML warning signs.

2.5 Assessing individual client and retainer risk

Under Part IV of the Regulations, how 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 client; and
- the regularity and duration of the business relationship.

You should also consider whether:

- your client is within a high-risk category, including whether:
    - it is based or conducts its business in high-risk jurisdictions and/or sectors; and
    - 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);
- you may need to consider (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 ML compliance):
    - 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; and
    - 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 its identity;
- you can be satisfied that you understand the client's ownership and control structure (particularly if the client or entities in its 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 ML/TF/PF;
- 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; or
    - transactions with an unexplained cross-border element.

This assessment will help you determine 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. For example:

- 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

You must 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 5 requires the regulated sector to have procedures in place to mitigate and manage the AML/CFT risks identified in the Practice's risk assessment.

These procedures need to be proportionate to the size and nature of your Practice. They must include:

1. identification and verification procedures in accordance with Part IV of the Regulations;
2. procedures to screen employees to ensure high standards when hiring;
3. record-keeping procedures in accordance with Part VIII of the Regulations;
4. adequate systems to identify risk in relation to persons, countries and activities which shall include checks against all applicable sanctions lists;
5. risk-management procedures concerning the conditions under which a client may utilise the business relationship prior to verification;
6. internal reporting procedures in accordance with regulation 34 of the Regulations, except where your Practice is comprised of one individual who, in the course of RFB, does not employ or act in association with any other person;
7. procedures for the ongoing monitoring of business relationships or one-off transactions for the purposes of preventing, countering and reporting ML/TF/PF and such procedures allowing for the identification of assets subject to TFS applicable in the Cayman Islands;
8. procedures to ensure compliance with TFS obligations applicable in the Cayman Islands; and
9. such other procedures of internal control, including an appropriate effective risk-based independent audit function and communication as may be appropriate for the ongoing monitoring of business relationships or one-off transactions for the purpose of forestalling and preventing ML/TF/PF;

and reflect:

10. an RBA as set out in Part III of the Regulations to monitor financial activities, which would include categories of activities that are considered to be high risk; and
11. awareness of the lists of countries, published by any competent authority, which are non-compliant, or do not sufficiently comply with the recommendations of the FATF.

In general, procedures should provide for:

1. the identification and scrutiny of matters which can arise in the context of legal practice, for example 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; or
- there appears to be no apparent economic or legal purpose, or the commercial rationale is unclear, and a high risk of ML 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 to remember that anyone carrying out RFB shall not use anonymous accounts, or accounts in fictitious names; you must be 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 level of 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)); and

3. identification and assessment of the risk that may arise in relation to the development of new products and new business practices, including by new technology/legal service delivery methods adopted by the Practice, and the use of new or developing technologies for both new and pre-existing products.

Effective management of AML/CFT/CPF risks are the responsibility of senior management. As such, all procedures and written policies must be approved by senior management.

Those operating in the regulated sector must ensure their procedures are documented and that relevant employees (if any) are aware of these procedures.

You must regularly review and update your procedures to ensure that they remain current and align with the level of risk facing your business. You should ideally record these reviews and/or updates in writing. You should maintain a written record of the steps that you have taken to communicate your procedures, and any changes to your procedures, to your relevant employees (where applicable).

It is vital that, where staff make decisions in line with the procedures identified by the Practice, they record their decisions and, where appropriate, the decision-making process either on the client record, matter file or compliance file.

3.3 Group-wide application

Practices must consider the application of the Regulations to their wider group, if any. Where a Practice in the Cayman Islands operates branches or controlled subsidiaries, agencies or representative offices in any other jurisdiction, it must have group-wide compliance programmes and comply with the relevant requirements under the Regulations.

In relation to branches and majority owned subsidiaries, before relying on group-wide programmes you should consider conducting a gap analysis between your group-wide AML/CFT/CPF programmes and the Cayman Islands AML/CFT/CPF legislation and regulatory requirements to ensure that they, at a minimum, comply with the applicable Cayman Islands requirements. You should also conduct a gap analysis as and when there are any changes to applicable AML/CFT/CPF obligations, or to group-wide programmes.

Where any gaps are identified during the gap analysis you should address those by amending your AML/CFT/CPF programme as appropriate, subject to legislative limitations (if any) for doing so in the countries in which the other group entities operate.

The group-wide policies should be appropriate to all branches and majority-owned subsidiaries of your Practice, and should include:

1. policies and procedures for sharing information required for conducting CDD;
2. AML/CFT/CPF risk management policies and procedures; and
3. adequate safeguards on the confidentiality and use of information exchanged.

As with your Practice-wide procedures, you must regularly review and update your group-wide procedures and should maintain a written record of any changes that you make to them following such a review. You should also maintain a written record of the steps that you have taken to communicate your group-wide procedures, and any changes to them, to your relevant employees.

3.4 Areas to cover

Practices must ensure they have procedures which include:

1. CDD identification and verification procedures;
2. employee screening procedures;
3. record-keeping procedures in accordance with Part VIII of the Regulations;
4. adequate systems to identify risk in relation to persons, countries and activities which shall include checks against applicable sanctions lists;
5. risk-management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification;
6. internal controls or reporting procedures in accordance with regulation 34 of the Regulations;
7. procedures for ongoing monitoring to prevent ML/TF/PF and identification of assets subject to TFS;
8. procedures to comply with TFS obligations applicable to the Practice;
9. other procedures of internal control, including an appropriate effective risk-based independent audit function and communication as may be appropriate for the ongoing monitoring of business relationships or one-off transactions for the purpose of forestalling and preventing ML/TF/PF;
10. a procedure for disclosures to the FRA (and the recording of decisions not to make disclosures to the FRA); and
11. a procedure for the monitoring and management of compliance with the procedures;

and reflect:

- an RBA and risk management practices; and
- awareness of any list of countries, published by any competent authority, which are non-compliant, or do not sufficiently comply with the recommendations of the FATF.

3.4.1 Risk management practices

Practices must ensure that they have documented their understanding of the key AML/CFT/CPF risks that they face.

They should keep a record of the sources used in completing their AML/CFT/CPF risk assessment.

It is important that decisions taken in relation to the application of the policies and procedures 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 (where applicable) 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 and for how long;
- when cash payments will be accepted;
- when payments will be accepted from or made to third parties; and
- the manner in which disclosures are to be made to the nominated officer.

3.4.2 Internal controls

Internal controls are expected to be adopted that are comprehensive and proportionate to the nature, scale and complexity of their activities and the AML/CFT/CPF risks identified. Factors you may consider when determining the measures you take which are 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; and
- the level of visibility and control that senior management has over client matters.

You should consider each of the controls set out in Regulation 5. The type and extent of measures to be taken should be appropriate to the AML/CFT/CPF risks, and to the size of the Practice.

The controls to be considered are set out below:

1. Appointment of an individual as the officer responsible for the Practice's compliance with the Regulations, the Anti-Money Laundering Compliance Officer ("**AMLCO**").

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 ML/TF/PF risk exposure and sufficient authority to take decisions affecting that risk exposure.

The requirement to appoint an AMLCO is additional to the requirement to appoint an MLRO. However, your AMLCO may also be your MLRO.

2. An audit function to test the AML/CFT/CPF systems, policies and procedures.

This should be conducted on a regular basis, the frequency being commensurate with the nature, size and complexity of your Practice, as well as the risks identified during the risk assessments.

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; and
- the extent of the policies and procedures in place to manage the risks identified in your Practice's risk assessment.

The audit function should:

a. test the overall integrity and effectiveness of the AML/CFT/CPF systems and controls;

b. assess the adequacy of internal policies and procedures, including:

    1. CDD measures;
    2. record-keeping and retention;
    3. third party relationships (e.g. eligible introducers) and supporting documentation; and
    4. transaction monitoring;

c. assess compliance with the relevant laws and regulations;

d. test transactions in all areas of your Practice, with emphasis on high-risk areas, products and services;

e. assess employees' knowledge of the laws, regulations, guidance and policies and procedures;

f. assess the adequacy, accuracy and completeness of training programmes; and

g. assess the adequacy of your process of identifying suspicious activity, including screening lists.

You should take an RBA 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.

1. Maintenance of policies and procedures in relation to outsourcing arrangements, in particular in relation to AMLCO and MLRO (refer to Section 10 (c) of the Guidance Notes for further information).

2. Adoption of procedures for employee screening to ensure high standards when hiring employees, and periodically after hiring (at least annually and any time where a suspicion has arisen as to the conduct of the employee).

   The extent of employee screening should be proportionate to the potential risk associated with your Practice, and the risks associated with individual employees, to ensure that employees are fit and proper to discharge their responsibilities and duties. In screening an employee, you may verify:

   a. references provided by the prospective employee at the time of recruitment;

   b. the employee's employment history, professional membership and qualifications;

   c. details of any regulatory actions or actions taken by a professional body;

   d. details of any criminal convictions; and

   e. whether the employee has any connections with the sanctioned countries or parties which may include doing checks against screening databases (e.g. World- Check).

3. Adoption of an appropriate employee training programme.

   You should ensure that all appropriate staff (if any) receive training on ML/TF/PF prevention on a regular basis, and ensure all staff fully understand that they will be committing criminal offences if they contravene the provisions of the Cayman Islands AML regime.

   This training should:

   a. be provided at least annually, or more frequently where there are changes to the Cayman Islands AML/CFT/CPF regime, in the recognition and treatment of suspicious activity;

   b. ensure that staff are aware of the serious nature of the background against which the Regulations have been issued, and ensure staff are fully educated on your AML/CFT/CPF systems, policies and procedures;

   c. be given to new employees;

   d. contain focus appropriate for operations staff who have roles where they are particularly important in combatting ML/TF/PF activities;

   e. provide appropriate training to ensure the level of knowledge required is provided to supervisors, managers and senior management, as well as the AMLCO and MLRO;

   f. be refreshed through refresher training on a regular, on-going basis to ensure relevant staff fully appreciate the importance their employer places on AML/CFT/CPF and their compliance obligations; and

g. be appropriate to level of employee (e.g. frontline staff might need more in-depth training).

3.4.3 Nominated Officers

Regulation 33(1) requires that all practices within the regulated sector must have a Nominated Officer/MLRO to receive disclosures under Part V of the POCL and the TL, and to make disclosures to the FRA.

You will need to inform CARA 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 CARA of any subsequent appointments to either of those positions within 14 days.

Who should be a Nominated Officer?

Your Nominated Officer/MLRO should be a natural person who is autonomous, independent, has and shall have access to all relevant material in order to make an assessment as to whether the activity is or is not suspicious, and who can dedicate sufficient time for the efficient discharge of the MLRO function, particularly where the MLRO or Deputy MLRO has other professional responsibilities. He or she should also be well versed in the different types of transactions you handle, and in a position of sufficient responsibility to be able to have access to all of your Practice's client files and business information, when necessary, so as to be able to make the required decisions on the basis of all information held by the Practice.

Role of the Nominated Officer

Your Nominated Officer/MLRO 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 ML/TF/PF 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 FRA 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/MLRO delegating certain duties regarding the practice's AML/CFT/CPF 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/MLRO is absent.

Responding to enquiries from law enforcement agencies

Although the task of detecting crime falls to law enforcement agencies, practices will be called upon to assist law enforcement agencies in the avoidance and detection of ML/TF/PF activities, and to react in accordance with the law in the reporting of knowledge or suspicion of such.

3.4.4 Client 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 cover instructions as to:

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 based on 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 ("**SDD**") may occur;
5. what steps need to be taken for enhanced due diligence ("**EDD**");
6. what steps need to be taken to ascertain whether your client is a PEP and subsequent controls that will be put in place in respect of a PEP;
7. when CDD needs to occur and under what circumstances delayed CDD is permitted and for how long;
8. how to conduct CDD on existing clients and how often CDD information will be reviewed to ensure that it is up to date; and
9. what ongoing monitoring is required.

For further information on conducing CDD, see Chapter 4.

3.4.5 Reliance and Record Keeping

Reliance

Your policies and procedures should cover reliance, which is discussed further in Section 4.4. You should consider including in your policies and procedures the fact that before relying on a third party for meeting your AML/CFT/CPF obligations, you will:

- assess the AML/CFT/CPF and other relevant procedures of a person; and
- satisfy yourself that that person's policies and procedures would enable you to comply with the AML/CFT/CPF obligations of the Cayman Islands (i.e. have an equivalent outcome).

Record keeping

Your policies and procedures should set out how your business complies with the record keeping obligations contained in the Regulations, which are discussed further in Section 4.8.

3.4.6 Monitoring compliance with policies and procedures

Practices must ensure that they regularly review their risk assessment and policies and procedures.

Monitoring compliance will assist you to assess whether the policies and procedures that you have implemented are effective in identifying and preventing ML/TF/PF 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; and
    - AMLCO/MLRO's logs of situations brought to his or her 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; and

4. how lessons learnt will be communicated back to staff and fed back into the risk profile of the Practice.

3.5 Disclosures

Practices must have a system clearly setting out the requirements for making a disclosure under the POCL and the TL. 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/MLRO or his or her 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 FRA; and
- 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 in order to comply with the Regulations and defend any allegations against the Practice in relation to ML/TF/PF 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.

The Regulations require that you keep records of CDD material and supporting evidence and records in respect of the relevant business relationship or one-off transaction. Adapt your standard archiving procedures for these requirements.

3.6.1 CDD material

You may keep either a copy of CDD material, or a record that indicates the nature of evidence of the CDD obtained. You may keep it for five years after the relevant business it relates to is completed, the business relationship ends, or the one-off 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 and this also reduces the risk of the material being inadvertently transferred to the client at the end of the business relationship or on completion of the one-off transaction.

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; and
- 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; and
- all identity details recorded on the document.

Where you are relied upon by another person for the completion of CDD measures, you must keep the relevant documents for five years from the date on which you were first relied upon.

3.6.2 Risk assessment notes

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 in demonstrating they have applied an RBA in a reasonable and proportionate manner. Contemporaneous notes have greater evidentiary value 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 a one-off 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/MLRO regarding concerns;
- advice sought and received regarding concerns;

- why the concerns did not amount to a suspicion and a disclosure was not made;
- any disclosures made;
- conversations with the FRA, law enforcement agencies, insurers and supervisory authorities regarding disclosures made; and
- decisions not to make a report to the FRA which may be important for the Nominated Officer in justifying 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 Law ("**DPL**") came into force in September 2019 and apply to you. It allows clients or others to make subject access requests for data held by you. Such requests could cover any disclosures made.

The DPL 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. This exception could 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 exception applies, document steps taken to assess this, to respond to any enquiries by the Ombudsman.

Under the DPL 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 the DPL (interpretation of data protection principles) and a privacy notice containing a statement that any personal data received from the client will only be processed for the purposes of preventing ML/TF/PF and any other purposes to which they have consented.

3.7 Communication and training

Your staff members (if any) are the most effective defence against launderers, terrorist financiers and proliferation financiers who would seek to abuse the services provided by your Practice.

Regulation 5 and other laws require that you ensure relevant employees:

- are made aware of both the laws relating to ML/TF/PF and the requirements of data protection which are relevant to the implementation of the Regulations, as well as your Practice's policies and procedures related to ML/TF/PF and data protection; and
- are regularly provided with training in how to recognise and deal with transactions and other activities which may be related to ML/TF/PF.

Professional regulatory requirements may also oblige you to train your relevant 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 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;
- whether the training will include a test;
- how often training and refreshers should take place; and
- how relevant staff will be kept up to date with emerging risk factors for the Practice and changes to applicable laws.

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/CFT/CPF conferences;
- participation in dedicated AML/CFT/CPF forums;
- review of publications on current AML/CFT/CPF issues; and
- practice or practice group meetings for discussion of AML/CFT/CPF issues and risk factors.

Providing an AML/CFT/CPF policy manual is useful to raise staff awareness and can be a continual reference source between training sessions.

3.7.2 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 and regulatory requirements; and
- changing criminal methodologies.

You should take an RBA to determining how often training should take place. Some type of training every year or two is preferable.

3.7.3 Communicating with your clients

While not specifically required by the Regulations, we recommend that you advise your client of your AML/CFT/CPF obligations. Clients are 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; and
- the requirement to report suspicious transactions (without tipping off).

Consider the manner and timing of your communications, for example, whether the information will be provided in the standard client engagement letter or otherwise.

Chapter 4 – Client due diligence

Note: Section 4.12.2.3 (senior management approval) of this Chapter may not apply to attorneys who are practising 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 client and understand the reasoning behind the client's instructions given to you.

4.2 Application

You must apply CDD on those clients who retain you for services regulated under the Regulations. See section 1.4.4 for further guidance on the scope of the regulated sector.

4.3 CDD in general

4.3.1 When is CDD required?

Regulation 11 requires that you apply CDD when:

- establishing a business relationship;
- carrying out a one-off transaction valued in excess of ten thousand dollars, whether it is executed in a single operation or in several operations which appear to be linked;
- carrying out a one-off transaction that is a wire transfer;
- you suspect ML/TF; or
- you doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

The distinction between one-off transactions and long-lasting business relationships is relevant to the timing of CDD and the question of when the time period for record-keeping begins to run.

Where a one-off 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, procedures must ensure Practices remain compliant with the relevant standard.

There is no obligation to conduct CDD in accordance with the Regulations for retainers involving non-regulated activities (i.e. activities within your Practice that do not constitute RFB). 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 'passported' easily between a Practice's non-regulated and regulated departments.

4.3.2 What is CDD?

Regulation 12 requires that you:

- identify the client and verify its identity on the basis of documents, data 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 any person purporting to act on behalf of the client and verify that person's identity and his or her authority to act on the client's behalf;

- 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 the client or other 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; and
- maintain ongoing due diligence on a business relationship, including:
    - having a risk-based overview of transactions undertaken to ensure transactions are broadly consistent with your understanding of the client, the client's business and risk profile, including, where necessary, on an RBA, the client's source of funds; and
    - ensuring that documents, data or information collected under the CDD process are kept current and relevant, by reviewing existing records at appropriate times and taking into account whether CDD measures have been undertaken previously, particularly for higher risk clients.

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 name and address.

Verification is obtaining some evidence which supports this claim of identity.

A risk-based approach/RBA

Regulation 8 means that, in practise, 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 8, and
- your assessment of the level of risk arising in any particular case.

You cannot avoid conducting CDD, but you can use an RBA 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 based on documents or information which come from a reliable source, independent of the client. There are a number of ways in which you can verify a client's identity including:

- obtaining or viewing original documents (or certified copies where appropriate);
- conducting electronic verification;
- obtaining information from other regulated persons; and
- 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. In verifying a client, you may use independent sources such as company registries, World-Check (or similar internationally accepted screening databases), Regulatory Data Corp ('RDC') and Google.

Consider the cumulative weight of information you have on the client and the risk levels associated with both the client and the retainer.

You may need to use a wider range of sources when verifying the identity of the beneficial owner and understanding the ownership and control structure of any client that is not an individual. Sometimes only the client or its 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.

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 may accept CDD documents in electronic form provided your Practice has taken an RBA and has suitable documented policies and procedures in place to ensure the authenticity of an electronic document. You should, for example, check the type of electronic file and ensure that it is tamper resistant.

You should consider whether any electronic verification system you use properly establishes the client'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 who they say they are.

For further guidance, you may refer to CIMA's Statement of Guidance on the 'Nature, Accessibility and Retention of Records', where applicable.

4.4 Reliance and outsourcing

Reliance has a specific meaning within the Regulations and relates to the process under Regulation 3(2) where, in certain circumstances, you may rely on another person to conduct CDD for you.

Before you rely on a third party to conduct CDD on your behalf, you must (as set out in 3.4.5):

- assess the AML/CFT/CPF and other relevant procedures of the third party; and
- satisfy yourself that the third party's policies and procedures would enable you to comply with the AML/CFT/CPF and CDD specific obligations of the Cayman Islands (i.e. have an equivalent outcome).

4.4.1 Relying on a third party

In order to rely on another regulated person to apply CDD measures, you must ensure your arrangement with the third party:

- enables you to obtain from the third party, immediately on request, copies of any identification and verification data and any other relevant documentation on the identity of the client or its beneficial owner; and
- requires the third party to retain copies of the data and documents in accordance with the record-keeping obligations under Parts IV and VIII of the Regulations.

You should note that you remain liable for any non-compliance with CDD requirements when you rely on another person.

You should ensure that any 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 on you 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).

4.5 Timing

4.5.1 When must CDD be undertaken?

Regulation 11 requires you to verify your client's identity, the identity of any person purporting to act on the client's behalf and that of any beneficial owner, before you establish a business relationship or carry out any transaction valued in excess of ten thousand dollars.

Regulation 15 provides that, if permitted by the Regulations, it will be possible to complete verification after the establishment of a business relationship, provided that:

- verification occurs as soon as reasonably practicable;
- the delay is essential so as not to interrupt the normal conduct of business; and
- the ML/TF risks are effectively managed.

Regulation 18 provides that if you are unable to complete CDD as required, you cannot open an account, commence business relations, or carry out a transaction with or for the client.

You must also:

- terminate the business relationship; and
- consider making a disclosure in respect of the client to the FRA.

Although you must consider making a disclosure to the FRA 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 FRA if you have a reportable suspicion or knowledge of ML/TF/PF 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.

4.5.2 Exceptions to the timing requirement

As noted above, 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 FRA.

Normal conduct of business

Regulation 15(2) 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 ML/TF. This exception does not apply if

your matter is a one-off transaction.

Consider your risk profile when assessing which work can be undertaken on a retainer prior to verification being completed.

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.

The Guidance Notes provide examples of types of circumstances in which it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business. These include:

- non-face to face business;
- securities transactions (as in the securities industry companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the client is contacting them, and performance of the transaction may be required before verification can be completed); and
- instances of telephone or electronic business where payment is or is expected to be made from a bank or other account, you should:
    - satisfy yourself that such account is held in the name of the applicant at or before the time of payment; and
    - not remit the proceeds of any transaction to the applicant or to his/her order until verification of the applicant’s identity has been completed.

These are only examples, and you should adopt risk management procedures with respect to the conditions under which an applicant may utilise the business relationship prior to verification. You should not postpone verification where the ML/TF/PF risks are high and EDD measures are required to be performed.

If you are unable to conduct full verification of the client and beneficial owners, then the prohibition in Regulation 18 will apply.

4.6 Ongoing monitoring

Regulations 12(e) and 17A require that you conduct ongoing monitoring of a business relationship. Ongoing monitoring is defined as including:

- 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, its business, and the risk profile; and

- at appropriate times, undertaking reviews of existing relationships to ensure that the documents, data, or information obtained for the purpose of applying CDD are kept up to date, relevant and adequate, particularly for higher risk categories of clients.

Regulation 5 requires, inter alia, that there are procedures in place for the ongoing monitoring of business relationships for the purposes or preventing, countering, and reporting money laundering, terrorism financing, proliferation finance and to ensure compliance with targeted financial sanctions applicable in the Cayman Islands. This includes ongoing monitoring/scrubbing against sanctions lists.

You must also be aware of obligations to keep clients' personal data updated under the Data Protection Law 2017.

Practices must operate a system of regular review and renewal of CDD. The frequency of review and updating should be risk-based, reflecting your knowledge of the business relationship and any changes in its circumstances. You must also have robust systems and controls in place for transaction monitoring and trigger-based review (refer to 4.6.1).

The application of SDD does not exempt you from your obligation to conduct ongoing monitoring or from your duty to report suspicious activity. Where you have applied SDD in low-risk relationships, you may choose to adjust the extent of regular review commensurate with the lower risks. Where the risk is deemed higher, you should apply enhanced monitoring, increasing the frequency and intensity.

Ongoing monitoring will normally be conducted by legal professionals handling the retainer and involves staying alert to suspicious circumstances which may suggest ML/TF/PF or the provision of false CDD material. A high degree of professionalism and scrutiny is expected from legal professionals. Legal professionals are expected to fulfil 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. The client may then instruct you in the purchase of a holiday home, the value of which appears to be outside the client’s financial means 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 provided, 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 FRA or with your Nominated Officer.

4.6.1 Trigger-based monitoring

Practices must make sure that documentation, data, and information obtained for CDD purposes is kept up-to-date and is adequate. Events prompting a due diligence update should include, but are not limited to:

a. a change in the client's identity information;

b. a change in beneficial ownership or control of the client;

c. a material change in the service provided to the client;

d. information being obtained that is inconsistent with your knowledge of the client; and/or

e. a change in the risk or factors affecting the risk rating.

A review may also be triggered by:

a. the start of a new engagement;

b. planning for recurring engagements;

c. a previously stalled or paused engagement restarting;

d. a significant change to key office holders;

e. the identification or participation of a PEP;

f. adverse information from sources such as media reports or other relevant sources;

g. a significant change in the client's business activity (this would include new operations in new jurisdictions); and/ or

h. the presence of knowledge, suspicion, or cause for concern (for example where you doubt the veracity of information provided). If a SAR has been made, care must also be taken to avoid making any disclosures which could constitute tipping off.

You should consider whether an event affects the risk associated with the business relationship. Where the basis of a relationship has changed, you must re-evaluate the risk rating of the client and associated matter(s). Ongoing monitoring procedures must take into account changes in the client and/or client’s matter risk rating. If the risk changes significantly, for example is deemed higher risk, then EDD should be applied.

In circumstances where no subsequent action was taken or 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 decided to take 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

The CDD requirements under Part IV of the Regulations do not imply that you need to repeatedly identify and verify the identity of each client whenever it undertakes a transaction. You are entitled to rely on identification and verification steps you have already undertaken unless you have doubts about the information's veracity. If however you become aware that you lack sufficient information about a client, or develop a suspicion of ML/TF, you should take steps to ensure that all relevant information is obtained as quickly as possible.

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 the client's personal details.

4.8 Records

Parts IV and VIII of the Regulations require you to keep records of your CDD documents and information and sufficient supporting records in respect of a transaction (whether or not a one off transaction) which is the subject of CDD or ongoing monitoring to enable the transaction to be reconstructed.

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 one off transaction was complete or the business relationship had come to an 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; or
- the client has given consent to the retention.

Many Practices will wish to retain the complete file of papers, including CDD records, for a period exceeding that which is specified in the Regulations. 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 is any variation on the period prescribed in the Regulations, the client's consent should 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 (based on an RBA) as to what evidence is appropriate to verify the identity of your clients. Verification of identity is a cumulative process. We outline a number of identification information, verification documentation and associated requirements for different types of applicants/clients below 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, permanent address (including postal code), date of birth, place of birth, nationality, occupation, physical appearance, employment and financial history, and family circumstances. Their identity must be verified in accordance with Part IV of the Regulations, based on 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 photo-card driving licences. Identification documents which do not have photographs or signatures or are easy to obtain (such as birth certificates, credit cards or non-Cayman Islands provisional driving licences), are not normally appropriate as the sole evidence of identity.

In most cases of face-to-face verification, producing a valid passport or photo-card identification should enable most clients to meet the AML/CFT/CPF identification requirements.

The name and address of the applicant should be verified by one or more of the following methods:

- obtaining a reference from a respected professional (e.g. a lawyer, accountant, minister or teacher);
- checking the register of electors;
- making a credit reference agency search;
- checking a current local telephone directory;
- requesting sight of an original or certified copy of a recent rates or utility bill, or a statement from a recognised financial institution, i.e. bank account statement, mortgage statement, credit card statement etc. or insurance policy; or
- making a personal visit to the home of an applicant client.

The form in Appendix B of the Guidance Notes may be used for verification of identity to supplement the identification documentation already held (however it is not intended to be used as the sole means of obtaining evidence of identity of an applicant, but is designed to be a standardised means by which verification can be obtained concerning identification evidence already held).

Identification documents should be certified, or originals either provided or sighted.

If documents are in a foreign language, other than the English language, such documents shall be translated into the English 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. If the usual types of evidence of identity cannot be obtained (for example certain classes of clients like the elderly, students or minors may find these difficult to obtain), flexibility is recommended (though without compromising sufficient AML/CFT/CPF procedures). 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 ML/TF/PF. 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 ML/TF is occurring or intended.

If standard documentation cannot be obtained, a request may be made to another institution for confirmation of identity (for example, entities that qualify under Regulation 22(d) of the Regulations).

Persons acting on behalf of the client

In accordance with Regulation 12(1)(b) 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; or
- 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 Corporate clients

With respect to a legal person you should identify the beneficial owners of the applicant, and take reasonable measures to verify their identity through the following information:

- the identity of the natural person who is the beneficial owner (if any);
- to the extent that there is any doubt as to whether there is a natural person considered a beneficial owner, or whether the person(s) with the controlling ownership interest are the beneficial owner(s), the identity of the natural persons (if any) exercising control of the legal person through any other means; and
- where no natural person is identified by either of the above enquiries, then the relevant natural person holding the position of the general partner, president, chief executive officer, director(s), manager(s) or other person in an equal senior management position who is exercising control over the legal person.

The following documents are acceptable for corporate (legal persons) clients. You are required to take an overarching RBA to determine the scope of the documentation required, and may need several or all types of documentation and information listed below, depending on the specifics/type of corporate applicant and the risks posed:

- certificate of incorporation or equivalent, and details of the registered office;
- explanation of the applicant’s business, reason for relationship being established and a copy of the latest available financial statements (where appropriate);
- satisfactory evidence of each of the legal owners, beneficial owners and a copy of the register of members or its equivalent;
- in the case of a bank account, satisfactory evidence of the account signatories, details of their relationship with the company and (if they are not employees) an explanation of the relationship;
- evidence of authority to enter into the relationship (e.g. board resolution);
- copies of any powers of attorney or other authority affecting the operation of the account given by the directors in relation to the company;
- verification of names and addresses of any individuals with such powers of attorney;
- a copy of the register of directors and officers or its equivalents;

- evidence of directors' identity;
- certificate of good standing or a similar document confirming that the applicant or client is listed in the company registry of its place of formation, and has not been dissolved, struck-off, wound up or terminated; and
- a copy of the constitutional documents, i.e. memorandum and articles of association, by-laws, or equivalents, of the applicant/client.

4.9.3 Partnerships and unincorporated businesses

In the case of a Cayman Islands limited partnership and other unincorporated businesses or partnerships, you should obtain, where relevant:

- identification evidence for at least two partners/controllers, the general partner and/or authorised signatories, in line with requirements for personal clients;
- evidence of the trading address of the business or partnership and copy of the latest financial report and accounts (audited where applicable); and
- an explanation of the nature of the business or partnership, to ensure this has a legitimate purpose.

4.9.4 Other arrangements or bodies

Trusts and fiduciary clients

Overview

The scope of due diligence that should be conducted on the parties to a trust will depend on the circumstances of the matter, such as whether the trust is being considered for due diligence because it is part of the ownership chain of another client or whether it relates to legal advice in relation to that trust and, if so ,what the advice entails and for whom is it being provided.

CDD shall usually be required for all material parties to the trust, where the trust sits atop a beneficial ownership chain. By contrast, considerations are more nuanced when legal advice is being provided. Specifically, in the context of legal advice, you will need to consider whether or not you need to collect CDD on all of the parties of the trust, which will usually only be the case when you are effectively acting for the trust as a whole. This may include when you are setting up the trust for the settlor or advising the trustee as to matters which involve changes to trust parties or the structure of the trust. By contrast, if you are advising a specific party as to their rights and obligations as to the trust, then you would only have to collect CDD as to that party, provided that the matter qualifies as RFB.

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 either:

- the settlor;
- the trustee(s);
- the protector(s); or
- one or more of the beneficiaries.

You shall identify the beneficial owners and verify their identity through the following information: the settlor, the trustee(s), the protector (if any), the enforcer (if any), the

beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

In the event the client is a settlor and a trustee, in its capacity as trustee, you should take the necessary steps to verify the identity of the trustee and the identity and source of funds of the settlor of the trust from which the assets originated.

You should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

- enquire as to the general nature of the trust and source of funds;
- obtain identification evidence for the settlor(s), i.e. the person(s) whose property was settled on the trust; and
- in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s) if different to the settlor(s).

In some cases, it may be impractical for you to obtain all of the information above (for example, if the settlor has died), or you may need additional information depending on risks identified. In such case, you shall take an RBA in determining what identification and verification documentation should be obtained.

Practical considerations

Applying CDD where you act in relation to an existing trust will usually involve you having sight of the trust deed and any document which relates to it. You should consider whether, if it is not provided, you 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 ML.

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 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 in relation to which you act lacks legal personality, you should approach CDD as you would where you act for a client in relation to a trust. '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.

Non-Profit Organisations (including charities)

Non-profit organisations (‘**NPOs**’) may pose a potential risk of ML/TF. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of funds.

If the applicant is an NPO you should normally obtain the following documentation:

- an explanation of its purposes and operations; and
- the identity of at least two signatories and/or anyone who gives instructions on behalf of the entity.

If the NPO is registered in an overseas jurisdiction, it may be useful to contact the appropriate charity commission or equivalent body to confirm the charity's registration.

If the NPO is operating locally, it may be useful to review the list of non-profit organisations maintained by the Cayman Islands Registry (www.ciregistry.ky) to confirm the charity's registration.

It will not be practical to obtain documentary evidence of identity of all donors. However you should undertake a basic 'vetting' of foreign NPOs and NPOs established overseas through a reasonable search of public information; verifying that the NPO does not appear on any terrorist lists, sanction lists nor have associations with ML, or a high-risk country. Identification information on representatives or signatories should be obtained.

Pension funds

Regulation 22 provides that the CDD required under Part IV regarding verification of the identity of a client or an applicant for business is not required where the identity of the client is known to you, you know the nature and intended purpose of the business relationship or one-off transaction, you have not identified any suspicious activity and the client or applicant for business is a pension fund for a professional association, trade union or is acting on behalf of employees of:

- an entity required to comply with Regulation 5 or is a majority-owned subsidiary of such relevant financial business
- a central or local government organisation, statutory body or agency of government in a country which is a lower risk jurisdiction
- an entity acting in the course of business, or which is a majority-owned subsidiary of the business, in relation to which an overseas regulatory authority exercises regulatory functions, and is based or incorporated in, or formed under the law of, a country which is a lower risk jurisdiction :or
- a company that is listed on a recognised stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or majority-owned subsidiary of such a company.

In applying an RBA, the risk factors to be considered include product and service factors. Where the product is:

- an insurance policy for pension schemes with no early surrender option, and where the policy cannot be used as collateral; or
- 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. This will be considered a low risk classification factor. In that case, you will need evidence that the product is such a scheme and so qualifies for SDD. Such evidence may include:
    - a copy of a page showing the name of the scheme from the most recent definitive deed; or

- 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.

Government agencies and councils

Regulation 22 provides that the CDD required under Part IV regarding verification of the identity of a client or an applicant for business is not required where the identity of the client is known to you, you know the nature and intended purpose of the business relationship or one-off transaction, you have not identified any suspicious activity and the client or applicant for business is a central or local government organisation, statutory body or agency of government in a country which is a lower risk jurisdiction.

The ML/TF 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; and
- extract from official government website.

In applying an RBA, the risk factors to be considered include client factors. Where the client or applicant for business is a central or local government organisation, statutory body or agency of government in a country which is a lower risk jurisdiction, this will be considered a low risk classification factor.

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.

The breadth of the definition is linked to the RBA, as the multiplicity of vehicle types means that the determination of beneficial ownership will be situational and it is incumbent on Practices to identify those parties that the requirement is meant to address, namely those who have the capacity to control or influence the client in the context of the transaction or the advice that is being provided. Practices will be expected to focus on those parties who are in a position to direct the activities of the client, such that those who could potentially be engaging in the activities of ML/TF/P through the law firm's services are identified.

To identify the beneficial owner, obtain at least the person's 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 RBA. 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;
- register of members or shareholder details from an online registry;
- the passport of, or electronic verification on, the individual; and
- other reliable, publicly available information.

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/CFT/CPF 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; and
- whether (and if so, 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; and
- identify the specific individuals as required in 4.9, in accordance with the Guidance Notes, above.

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 from your client directly, its website or its 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 its 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 2(1) states that a beneficial owner generally means a natural person who ultimately owns or controls the client or on whose behalf a transaction or activity is being conducted, and includes but is not restricted to:

- in the case of a legal person other than a company the securities of which are listed on a recognised stock exchange, to a natural person who ultimately owns or controls, whether through direct or indirect ownership or control, 10% or more of the shares or voting rights in the legal person; or
- in the case of any legal person, to a natural person who otherwise exercises ultimate effective control over the management of the legal person; or
- in the case of a legal arrangement, to the trustee or other person who exercises ultimate effective control over the legal arrangement.

In these cases, it is presumed that the client is the beneficial owner, unless the features of the transaction indicate that the client is acting on someone else's behalf. In that case you do not have to proactively search for beneficial owners but should 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 where that person is:

- 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); or
- 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.

You cannot rely solely on the information contained in the company's register of members or its equivalent to identify persons with significant control. Where the holder of the requisite level of shareholding of a company is another company, apply the RBA 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 10 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 ML as it is often difficult to identify beneficial owners and such companies are often incorporated in jurisdictions with lower AML/CFT/CPF 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; and
- getting an assurance that either such a regulated person or the holder of the shares will notify you of any change of registered particulars 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.

4.11 Simplified due diligence/SDD

Part V of the Regulations permits SDD to be undertaken where you determine that the business relationship or transaction presents a low risk of ML/TF/PF taking into account your risk assessment, and simplified CDD is commensurate with the lower risk factors identified by the country (i.e. the NRA or similar assessments conducted by the Cayman Islands) or the relevant supervisory authority.

4.11.1 What is SDD?

You have to obtain evidence that the transaction and client or products provided are eligible for SDD. The simplified measures should be commensurate with the low risk factors. Examples of possible SDD measures are:

- verifying the identity of the client and the beneficial owner after the establishment of the business relationship;
- reducing the frequency of client identification updates;
- reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold, which in any event should be based on the client profile; and
- relying on a third party to conduct verification of identity of applicant/client/beneficial owner(s).

Where you decide to take simplified CDD measures on an applicant/client, you should document the full rationale behind the decision and make the documentation available to the relevant supervisory authority on request.

4.11.2 Who are acceptable candidates under Regulation 22?

You are required to conduct verification of the identity of applicants at the time of establishing the business relationship, however regulation 22 of the Regulations allows you not to conduct verification where:

- you know the identity of the applicant/client;
- you know the nature and intended purpose of the business relationship or one-off transaction;
- there is no suspicious activity; and
- the applicant/client is a person who or which:
    a. is required to comply with Regulation 5 or is a majority-owned subsidiary of that relevant financial business;
    b. is a central or local government organisation, statutory body or agency of government in a lower risk country
    c. is acting in the course of a business or is a majority-owned subsidiary of the business in relation to which an overseas regulatory authority exercises regulatory functions and is based or incorporated in, or formed under the law of, in a lower risk country;
    d. is a company that is listed on a recognised stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership or majority owned subsidiary of such a company; or
    e. is a pension fund for a professional association, trade union or is citing on behalf of employees of an entity referred to in points a. to d. above.

If the applicant/client falls into one of the eligible categories (such as being regulated in a low risk jurisdiction or listed on a recognised stock exchange) then the extent of required due diligence under Regulation 22 only entails verifying and documenting that basis, i.e. proving that in fact the client is so regulated or listed.

For further details on the requirements for qualification for SDD, see Part 5 of the Regulations, in particular the amended regulations 24 in respect of nominees and 25 in respect of Eligible Introducers.

4.12 Enhanced due diligence/EDD

Regulation 27 provides that you will need to apply EDD in addition to the CDD measures required in Part IV, on a risk-sensitive basis:

- where a higher risk of ML/TF/PF has been identified pursuant to Part III;
- where, through supervisory guidance, a high risk of ML/TF/PF has been identified;
- where a client or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its AML/CFT/CPF regime or a prevalence of corruption;

- in relation to correspondent banking relationships, pursuant to Part XI;
- where the client is a PEP, or a family member or known close associate of a PEP; or
- in the event of any unusual or suspicious activity.

In applying the RBA to a specific 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

You should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships and transactions. Where a client is a natural person and is not physically present for identification purposes, you must take this into account when assessing whether there is a high risk of ML/TF/PF 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 EDD 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 CIMA 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

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 measures 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), you must take the following steps to deal with the heightened risk:

- have appropriate risk management systems to determine whether the client is a PEP;
- have senior management approval for establishing a business relationship with a PEP or an entity beneficially owned by a PEP;

- take reasonable measures to establish the source of wealth and source of funds which are involved in the business relationship or one-off transaction; and
- conduct closer ongoing monitoring of the business relationship.

In assessing the ML/TF/PF risks of a PEP, you should consider whether the client:

- is from a high-risk country;
- has prominent public functions in sectors known to be exposed to corruption; and/or
- has business interests that can cause conflict of interests (with the position held).

Other red flags that you should consider include (in addition to red flags you consider for other applicants):

- information provided by the PEP that is obviously inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
- funds repeatedly moved to and from countries to which the PEP does not seem to have ties; and
- use by the PEP of multiple bank accounts for no apparent commercial or other reason.

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 is a PEP, you should consider on an RBA what extra measures, if any, you need to take when dealing with that client.

4.12.2.1 Who is a PEP?

A PEP includes:

a. a person who is or has been entrusted with prominent public functions by a foreign country, for example a head of state or government, a senior political or government, judicial or other official, or a senior executive of a state-owned corporation;

b. a person who is or has been entrusted domestically with prominent public functions, for example a head of state or of government, senior politician, senior government, judicial or military official, senior executive of a state owned corporation and important political party official; or

c. a person who is or has been entrusted with a prominent function by an international organisation like a member of senior management, such as a director, a deputy director and a member of the board or equivalent functions.

Middle ranking and junior officials are not PEPs. Only those who hold truly prominent positions should be treated as PEPs and the definition should not be applied to more junior members of the civil service or military officials other than those holding the most senior ranks.

In addition to the primary PEPs listed above, a PEP also includes:

- family members of a PEP: spouse, child, sibling, and parent; and
- close associates of a PEP: persons with whom joint ownership or control of a legal entity or legal arrangement is held, with whom there are close business or personal relationships, or who are owners of a legal entity or arrangement known to have been established to the benefit of a 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 Part III of the Regulations, the level of risk of ML/TF/PF 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; and
- 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 beyond doubt, 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 EDD 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 ML).

4.12.2.3 Senior management approval

'Senior management' is not defined. However, in the context of a Practice, 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; or
- 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, in order to ensure appropriate monitoring of the Practice's risk profile and compliance.

4.12.2.4 Establishing source of wealth and funds

Generally, establishing sources of wealth and funds simply involves asking questions of the client about its source of wealth and the source of the funds to be used with each retainer. When you know a person is a PEP, his or her 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, you should 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 where the funds received from or on behalf of the client's funds come from (e.g. a Cayman Islands bank account). Source of wealth is a more general question and relates to how the client came to have the funds in question (e.g. via inheritance, sale of property or business, or investment windfall). Source of wealth is fundamental to ML risk assessment. If you are clear about the legitimacy of a client's source of wealth, the risk of ML is significantly reduced.

4.12.2.5 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 country'.

You are encouraged to consult publicly available information to ensure that you are aware of the high-risk countries/territories. While assessing risk of a country, you're encouraged to consider, among the other sources, sanctions issued by the UN and EU, the FATF high-risk and non-cooperative jurisdictions, the FATF and its regional style bodies ('**FSRBs**'), and the Transparency International corruption perception index.

4.12.4 Other situations of higher risk of ML/TF/PF

EDD is also required where there is a higher risk of ML/TF/PF identified pursuant to Part III of the Regulations. In determining whether there is a higher risk of ML/TF/PF in a given case, you must take into account the risk factors set out in Regulation 8(1). 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 ML/TF/PF.

See Chapters 2 and 12 for factors and warning signs you should consider in determining

whether a high risk of ML/TF/PF is present in a given case.

4.13 Sanctions and other restrictions

Your CDD measures should, following an RBA, enable you to ascertain whether your client is subject to the restrictions or directions listed below.

You should also be able to ascertain whether any key beneficial owners or the intended recipient of funds from a transaction you are undertaking is subject to the restrictions or directions listed below, where there is a higher risk of ML/TF/PF.

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 TF; and
- persons from jurisdictions which are subject to sanctions.

The sanctions orders applicable in the Cayman Islands are published by the Cayman Islands Government in the Gazettes. Generally, the sanctions lists in force in the UK (HM Treasury) are extended to the Cayman Islands. The lists issued in the United Kingdom might be different from lists issued in other countries, such as the United States (OFAC). While the OFAC sanctions might have no legal effect in the Cayman Islands, because of the extra-territorial effect of the US measures, and their implications for international banking transactions in US dollars, you should take note of them. You should carefully select the sanctions lists as lists that do not include at least all the sanctions applicable in the Cayman Islands may cause your sanctions compliance programme and monitoring to be deficient.

Chapter 5 – Counter Terrorist Financing, Proliferation Finance and Targeted Financial Sanctions/CFT/PF/TFS

5.1 Counter the Financing of Terrorism and Proliferation Financing

Comparison of Proliferation Financing to Money Laundering and Terrorist Financing (from CIMA Guidance 2020 Section 14 E.)

	Money Laundering	Terrorist Financing	Proliferation Financing
Flow of Funds	Circular – money eventually ends up with the person that generated it	Linear – money generated is to propagate terrorist groups and activities	Linear – money is used to purchase goods and parts, technology from brokers and manufacturers. Shipping and insurance also part of money trail
Conduits	Favours - formal financial system	Favours - cash couriers or informal systems such as hawala and currency exchange firms	Favours - formal financial system
Detection Focus	Suspicious transactions - deposits uncharacteristic of customer's or the expected activity	Suspicious relationships, such as wire transfers to seemingly unrelated parties	Goods and materials, activities, countries, individuals
Transaction Amounts	Large, but often structured to avoid reporting requirements	Small, usually below reporting thresholds	Moderate amounts – transactions appear legitimate with transaction profile
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares and countries with lax financial services regulations	Varied methods, including formal banking system, informal value transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide origin of funding

Terrorism is an unlawful action which is intended to compel a government or an international organisation, or intimidate the public to do or abstain from doing any act for the purpose of advancing a political, religious, racial, or ideological cause.

These actions include serious violence against a person, endangering a person's life, serious damage to property, creating serious risk to public health and safety, or serious interference with or disruption to the provision of emergency services, or essential infrastructure, or to an electronic or computer system. By contrast, financial gain is the main objective of other types of financial crimes. Nonetheless, terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts.

For the purpose of these Guidance Notes, Practices shall refer to the meaning of terms 'terrorism' and 'terrorist financing' in the TL.

Sources of funding for terrorism could be unlawful sources such as kidnapping, extortion, smuggling, various types of fraud (e.g. through credit cards or charities), theft and robbery, and narcotics trafficking. Practices must be aware however, that funding for terrorist groups, unlike for criminal organisations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal and legitimate sources is a key difference between terrorist groups and traditional criminal organisations.

Terrorist groups find ways of laundering the funds in order to disguise links between them and their funding sources, and to be able to use the funds without drawing the attention of authorities. Some of the particular methods detected with respect to various terrorist groups include cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, and money orders/money transfers), use of credit or debit cards, and wire transfers.

The Cayman Islands National Risk Assessment on Terrorism Financing indicates that the Islands face a risk level of medium and that the jurisdiction and the entities and activities affiliated with it could be misused for terrorism financing purposes. While it should be noted that there is very little direct evidence that any significant movements of terrorism-related funds take place through the jurisdiction, it was concluded that the overall size of the jurisdiction's international financial sector and the general difficulties in detecting TF make it inherently vulnerable. The vulnerability primarily arises from the high levels of cross border business and financial transactions and activities, with the attendant possibility of the services and products offered or assets channelled through the Cayman Islands being used to fund terrorism abroad.

The jurisdiction has mitigated such inherent vulnerabilities by virtue of its comprehensive legislative framework and upgraded supervisory and law enforcement mechanisms. A critical component of this are the steps that regulated institutions, such as law firms, take to identify and address terrorism risks by the application of the RBA. Successful application of the RBA requires a realistic understanding of these vulnerabilities, so that resources can be applied appropriately. The evidence collected to date (such as domestic investigations, SARs, intelligence reports or requests for assistance from other jurisdictions), all seem to indicate that while terrorism financing is quite rare in the jurisdiction it can have incredibly serious consequences when it does occur. This means that firms need to apply an RBA that efficiently excludes the vast majority of cases where there is no potential connection to TF and then focus on those rare instances where there is a possible danger.

A starting point are the typologies defined in the NRA and consideration of their applicability to the jurisdiction, and to each firm's practice.

Typology A: The Cayman Islands is used as a transit country for funds that are intended to be used for terrorism purposes abroad, with funds being sent via the Cayman Islands either through banks, other payment channels such as money services businesses ("**MSBs**"), or being physically moved through the Cayman Islands territory.

There is no evidence to indicate that any sums of material amounts transit through Cayman financial institutions, primarily based on data highlighting that fund flows from countries with terrorism issues is limited to .03%, with the bulk of that amount coming from countries like India and the Philippines which are well-represented within the local population. Further, the majority of this activity will be limited to simple transactions through banks and other financial institutions, which will not involve legal advice.

Typology B: The Cayman Islands regulated service providers knowingly or unknowingly facilitating the movement of funds for terrorism purposes but without the funds actually entering or moving through the Cayman Islands, for example, Cayman lawyers providing services to customers that support foreign terrorism.

Given the affiliations present in the jurisdiction between law firms and corporate service providers ("**CSPs**"), these risks should be closely considered by any firm operating this sort of business model, with special focus being paid to understanding the client's business and which jurisdictions it operates in. That being said, all available evidence indicates that only a tiny fraction of CSP clients in the jurisdiction are involved in business lines or jurisdictions where there could be a potential concern.

Typology C: Cayman Islands legal entities are abused for TF purposes.

While there is little available evidence that Cayman entities have been misused, the potential always exists that a Cayman vehicle could be used to obscure TF. As with the RBA more broadly, firms should understand their client's underlying activities and also note when they have connections to higher-risk jurisdictions or activities. Also, firms need to understand how new technologies could potentially facilitate such financing, although the NRA indicates that so far cryptocurrencies have proven to be a poor tool for TF although closed initial coin offerings have been utilized. Attorneys forming such entities need to take a robust approach to reviewing potential risk.

Beyond these typologies, law firms should have an understanding of: those jurisdictions with connections to terrorism, those businesses and entity types that might be used as covers for TF (such as certain foundations and charities) and apply broader risk consideration, such as transactions that fail to make economic sense, to identifying potential TF.

Countering Proliferation Financing

Proliferation is the manufacture, acquisition, possession, developing, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services, and expertise.

PF is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible. In other words, it is the financing of the proliferation activities described above. PF refers to more than simply the payment for goods and includes any financial service provided in support of any part of the procurement process (even if it is not directly connected to the physical flow of goods). Financing can include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation.

PF facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items poses a risk to global security and stability and may ultimately result in loss of life.

The PFPL makes it an offence for any person to provide funds and economic resources to fund

unauthorised proliferation activities, or to enter into or become concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund unauthorised proliferation activities.

A person who acts in the course of a business in the financial sector may be committing an offence, even if the offence takes place wholly or partly outside the Islands.

Considerations for attorneys

The RBA demands that all firms develop a substantive understanding as to the business activities of their clients and the specifics of any transaction that is facilitated by their legal advice. While it is very unlikely that law firms will be directly involved in the operational aspects of PF or development, or the shipment of goods that could be used for those purposes, their clients may well be and may need legal advice with respect to the purchase, sale and transport of such goods. Certainly, law firms with trade finance, asset finance, structured finance and maritime practices should be especially mindful of clients from jurisdictions where proliferation is a concern, as well as the identity of goods being purchased and sold. Even more specifically, law firms servicing the shipping sector should be generally cognizant of their clients' trade routes, products being transported and purpose behind such services as the purchase of shipping insurance or discounted foreign accounts receivable and provisions of guarantees to or on behalf of exports. While the RBA will be linked to the advice they are providing, as a firm cannot reasonably be expected to have visibility over every aspect of a client's business, firms should always be able to justify their level of inquiry and the risk factors that were identified and considered.

Prohibited goods: If firms are providing legal advice as to the purchase, sale or transport of goods they should take steps to determine whether those goods are listed on export control lists or are identifiable as "dual-use goods".

Customers: firms should always understand the nature of their customer's business, including whether those clients are exposed to the manufacture, trade or provision of expertise or consulting services relating to sensitive or dual-use goods or technology. Given the jurisdiction's predominant focus on traditional financial services, the majority of clients will likely be easily discounted from a PF perspective. Firms should therefore apply further research and inquiry to those clients that remain.

Geography: While most of the countries directly tied to proliferation should likely be considered higher-risk in any event because of the presence of sanctions, terrorism and corruption, firms should address this risk-factor from a proliferation-specific perspective. It would be insufficient to simply note the presence of geographic risk as one of many factors to consider without directly identifying proliferation risks if they are in fact present. While it is perfectly reasonable to classify a matter as 'standard risk' if there is only one risk factor present, that is not the case where that risk factor, in the wider context of the transaction, reveals a substantive risk of proliferation financing.

Further, there are some jurisdictions (such as Singapore) that are not considered higher risk in a general sense but may be in the specific context of PF because of their potential use as a ‘conduit country’. For certain types of advice, firms should consider shipments made to the countries surrounding noteworthy proliferation hot-spots, such as Iran, to determine whether there is a chance that these hot-spots may be the ultimate destination. The RBA must always be contextual.

Products and Services: While it is unlikely that Cayman Islands law firms will directly offer products and services that will be used to facilitate PF, firms should be aware that entities involved in proliferation may seek shipping insurance or loans or credit facilities to facilitate export transactions. These include the purchase of discounted foreign accounts receivable and

provisions of guarantees to or on behalf of exporters.

Red Flags

Geographic Factors:

• Transactions involving a country of proliferation concerning Examples: North Korea and Iran
• Transactions involving countries of diversion concern. Examples: China (particularly Liaoning and Jilin provinces), Hong Kong, Singapore and Malaysia
• Transactions involving countries that are known to trade with North Korea. Examples: Syria, Egypt, the United Arab Emirates, Yemen and Iran
• Trade finance transaction shipment route through jurisdictions with weak export controls or enforcement
• Transaction involves shipment of goods inconsistent with normal geographic trade patterns, where goods are shipped through several countries for no clear reason
• Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped
• Transaction involves financial institutions with known deficiencies in AML/CFT/CPF controls

Documentation:

• Based on the documentation obtained in the transaction, the declared value shipment was obviously under-valued vis-à-vis shipment cost
• Inconsistencies between information contained in trade documents and financial flows, or changes in shipment location or goods shipped
• Freight forwarding company listed as final destination
• Obvious alterations to third party documents or the documentation appears illogical, altered, fraudulent or is absent

Customers:

• Customer is involved in the supply, sale, delivery or purchase of dual-use good, or is a military or research body connected to a high-risk jurisdiction
• Customer activity does not match business profile, especially in terms of types of goods shipped
• Order for goods placed in a country different than that of the expected end-user. There are obviously circumstances though where this is easily explainable
• New customer requests letter of credit while awaiting opening of account
• Customer is vague or inconsistent in the information it provides and is resistant to providing additional information when queried.
• The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions

Transaction Structure

• Transaction concerns dual-use goods or military goods
• Transaction demonstrates links between representatives of companies exchanging goods
• Transaction involves possible shell companies
• Pattern of wire transfers or payment activity show unusual patterns or no apparent purpose, or payment instructions are illogical or contain last minute changes
• Circuitous route of shipment and/or circuitous route of financial transactions

Implementation of a holistic RBA

- Ensure that PF is incorporated into wider compliance policies and procedures
- Train staff as to incorporation of PF into the RBA
- Require staff to understand their client's business and the specifics of the transaction (including counterparties where appropriate) before any client is on-boarded
- Require staff to consider red flags during the on-boarding process
    - This should include familiarity with sanctions and export control lists, as well UN Panel reports and general familiarity with dual-use goods and technology
- Adopt appropriate screening solutions to identify listed individuals or otherwise subject to adverse press
- Ensure that senior management is informed when there are credible linkages to PF

Freezing and Reporting Obligation

The PFPL requires that any person that has in its possession, custody or control any funds or economic resources that relate to a designated person to immediately freeze such funds and resources and ensure that no funds or resources are made available for the benefit of the designated person.

In addition, any person must, as soon as reasonably practicable, disclose to the FRA, using the form issued for that purpose, details of any frozen funds or economic resources or actions taken in compliance with relevant Security Council measures. This includes attempted transactions.

Any person who fails to comply with the freezing and reporting requirement faces civil penalties and criminal prosecution.

5.2 Targeted Financial Sanctions/TFS

Sanctions are used as a foreign policy tool to influence target countries, regimes, sectors and/or groups to make desired changes. Types of sanctions include: (a) targeted asset freezes, (b) restrictions on a wide variety of financial markets and services; and (c) directions to cease all business.

Practices should make their sanctions compliance programme an integral part of their overall AML/CFT/CPF compliance programme and accordingly should have documented policies, procedures, systems and controls in relation to sanctions compliance.

Practices should provide adequate sanctions-related training to their appropriate staff. Official sanctions orders applicable in the Cayman Islands are published by the Cayman Islands Government in the Gazettes. Sanctions-related information and applicable orders are posted on CIMA's website accessible at www.cima.ky.

When conducting risk assessments, Practices should take into account any sanctions that may apply (to applicants/clients or countries). Practices should manually or electronically screen applicants, clients, beneficial owners, transactions, service providers and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, Practices may discover that certain sanctions are applicable to one or more of their clients, existing or new.

For the purposes of supervision by CARA, Practices must document screening results (including a time stamp) to evidence that screening has been conducted without delay. The

phrase ‘without delay’ means, ideally, within a matter of hours.

Where there is a true match or suspicion, Practices shall take steps that are required to comply with the sanctions obligations including reporting pursuant to the POCL, Regulations, TL and PFPL. Separately, Practices must file a SAR with the FRA if they discover a relationship that contravenes a sanctions order or a direction under the PFPL. Practices shall document and record all the actions that were taken to comply with the sanctions regime, and the rationale for each such action.

Practices are expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed. Practices can submit contact email addresses of staff to the FRA, to ensure receipt of email notifications when the sanction lists are updated.

Generally, the sanctions lists in force in the UK (HM Treasury) are extended to the Cayman Islands pursuant to Overseas Orders in Council. These sanctions apply to all individuals and entities in the Cayman Islands. The lists issued in the United Kingdom (HM Treasury) might be different from lists issued by other countries, such as the United States (OFAC). While the OFAC sanctions may have no legal effect in the Cayman Islands, because of the extra-territorial effect of the US measures, and their implications for international banking transactions in US dollars, Practices should take note of them. It is important that Practices carefully select the sanctions lists as lists that do not include at least all the sanctions applicable in the Cayman Islands may cause a Practice’s sanctions compliance programme and monitoring to be deficient.

In respect of TFS notices, your headline obligations as set out by the FRA are to 'Freeze and Report’:

In relation to freezing and reporting, you must:

i. check whether you maintain any accounts or hold any funds or economic resources for the persons set out in consolidated sanctions list assessable at www.fra.gov.ky and any domestic lists (if applicable);

ii. freeze such accounts, and other funds or economic resources without delay;

iii. refrain from dealing with the funds or economic resources or making them available to such persons unless licensed by the Governor;

iv. report any findings to the FRA at financialreportingauthority@gov.ky, together with any additional information that would facilitate compliance with the applicable sanctions as set out in the Overseas Orders in Council; and

v. provide any information concerning the frozen assets of designated persons to the FRA at financialreportingauthority@gov.ky by completing and submitting a TF/PF Asset Freeze Report Form. Information reported to the FRA may be passed on to other regulatory authorities or law enforcement.

In the event that any person/entity is officially delisted, the obligation to freeze no longer exists. The funds or assets that have been frozen must therefore be unfrozen.

In relation to unfreezing and reporting, you must:

i. check whether you have frozen assets of any person or entity removed from the sanctions list and verify that the person or entity is no longer subject to an asset freeze;

ii. remove the person or entity from your Practices’ list of persons/entities subject to financial sanction;

iii. unfreeze the assets/accounts of the person or entity and where necessary re-activate all relevant accounts;

iv. send advice to the person or entity that the assets are no longer subject to an asset freeze; and

v. advise the FRA of the actions taken as soon as practicable.

Failure to comply with financial sanctions legislation or to seek to circumvent its provisions is a criminal offence.

Offences under the Overseas Orders in Council relating to UN/EU financial sanctions carry a maximum of seven years' imprisonment on indictment and, on summary conviction, to a maximum of six months' imprisonment or a maximum fine of £5,000 or its equivalent in the Cayman Islands.

Similarly a person who commits an offence under Schedule 4A of the TL is liable on summary conviction, to a fine of $4,000, or to imprisonment for a term of twelve months, or to both, or on conviction on indictment, to a fine or to imprisonment for a term of seven years, or to both.

Under the PFPL the FRA has the power to impose civil penalties of such amount as it considers appropriate (not exceeding $40,000) on a person who fails to comply with freezing and reporting obligations of any frozen funds or economic resources. A person who fails to comply with a freezing obligation is also liable on summary conviction to a fine of $50,000, or on conviction on indictment, to a fine of $70,000, or imprisonment for a term of three years, or to both. A person who fails to comply with a reporting obligation is liable on summary conviction to a fine of $10,000.

Chapter 6 – Money laundering offences

6.1 General comments

The POCL created a single set of ML offences applicable throughout the Cayman Islands to the proceeds of crime. It also creates a disclosure regime, which makes it an offence not to disclose knowledge or suspicion of criminal conduct, but also permits persons to be given consent in certain circumstances to carry out activities which would otherwise constitute an offence under the POCL.

In this Guidance, there are references to decisions of English courts, which technically do not constitute binding precedent in the Cayman Islands. Only where the decisions set out common law principles (or statutes where the Cayman Islands statute has the same or similar wording) are they regarded as highly persuasive by the courts of the Cayman Islands.

6.2 Application

The POCL 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 V of the POCL 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 ML offences. A person will have a defence to a principal offence if he or she knows or believes on reasonable grounds that the criminal conduct involved was exempt overseas criminal conduct.

For the principal offences of ML, 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, you must disclose if you have knowledge, suspicion or reasonable grounds for suspicion.

These terms for the mental elements in the offences are not terms of art; they are not defined within POCL 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 wilfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the English criminal courts is that nothing less than actual knowledge will suffice.

6.3.2 Suspicion

The term 'suspects' is one which the English courts have 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 ML 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 ML 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 ML, 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 ML?

6.4 Principal ML offences

6.4.1 General comments

ML offences assume that criminal conduct has occurred in order to generate the criminal property which is 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 ML offence.

The principal ML offences apply to ML activity which occurred on or after 30 June 2008. If the ML took place after 30 June 2008, the conduct giving rise to the criminal property can occur before that date.

When considering the principal ML 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 ML.

6.4.2 Section 133 – concealing

A person commits an offence if he or she conceals, disguises, converts, or transfers criminal property, or removes criminal property from the Cayman Islands.

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 134 - 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 V of the POCL. The arrangement must exist and have practical effects relating to the acquisition, retention, use or control of criminal 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 'arranging' under the relevant English law offence 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 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 the client may commit upon coming into possession of the property after completion of the settlement.

The recovery of property by a victim of an acquisitive offence will not amount to committing an offence under either Section 134 or Section 135 of the POCL.

Sham litigation

Sham litigation created for the purposes of ML remains within the ambit of Section 134. 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, ML for the purposes of the POCL 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 English court in *Bowman v Fels* did not directly consider the conduct of transactional work, its approach to what constitutes an arrangement under English law 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 criminal property will not constitute the making of an arrangement under Section 134 of the POCL.

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; and
- if no arrangement exists, whether one may come into existence in the future and, if so, whether you may become concerned in it.

6.4.4 Section 135 - 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 ML offences

You will have a defence to a principal ML offence if:

- you intended to make a required disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence); or
- you are a professional legal adviser or other relevant professional adviser and the information or other matter came to you in privileged circumstances; or
- you do not know or suspect that another person is engaged in ML and you have not been provided by your employer with such training as is required by the Regulations and this Guidance; or
- you know, or believe on reasonable grounds, that the criminal conduct is occurring in a particular country or territory outside the Cayman Islands, and the criminal conduct is:
    - not unlawful under the criminal law applying in that country or territory; and

- is not of a description prescribed in an order made by the Attorney General of the Cayman Islands.

In relation to Section 135 of the POCL you will also have a defence if you gave adequate consideration for the criminal property (the adequate consideration defence).

6.5.1 Required disclosures

Making a required disclosure regarding suspicion of ML under Section 136 of the POCL will mean liability for the principal ML offences will not arise.

You may make a required disclosure either:

- before ML has occurred;
- while it is occurring but as soon as you suspect it; or
- after it has occurred, if you had good reason for not disclosing earlier and you make the disclosure as soon as practicable.

A disclosure is required so long as 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/MLRO. The Nominated Officer/MLRO will consider your disclosure and decide whether to make an external disclosure to the FRA. If your Practice does not have a Nominated Officer/MLRO, you should make your disclosure directly to the FRA.

Reasonable excuse defence

This defence applies where a person intended to make a required 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 ("**LPP**").

You will have a defence against a principal ML offence if you make a required 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 CARA's view that you will have a reasonable excuse for not making a required disclosure and will not commit a ML 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 Cayman Islands or elsewhere) is already aware of the suspected criminal conduct or ML and the non-reporter does not have any additional information which might assist the regulator or enforcement authority;
- if the only information that a reporter would be providing for the purposes of a required disclosure is information entirely within the public domain; or
- if all the suspected predicate offending and all the suspected ML occurs outside the Cayman Islands and there is otherwise no Cayman Islands nexus to the suspected criminality.

This is not intended to be an exhaustive list. Moreover, non-reporters should be aware that it will ultimately be for a court to decide if an excuse for not making a required disclosure was a reasonable excuse. You should clearly document your reasons for concluding that you 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. It may be that certain steps have already taken place which you now suspect facilitated ML; while further steps are yet to be taken which you also suspect will facilitate further ML.

You may be required to make a disclosure in these circumstances if:

- at the time the initial steps were taken they did not amount to a ML 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 should fully document 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 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 ML offence if you know or suspect the money is criminal property. In that case, you must make a required disclosure.

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 135 of the POCL in line with the English 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, unbeknownst to that party, is given criminal property in settlement for that debt; and
- a person provides goods or services as part of a legitimate arm's length transaction but unbeknownst to that person is paid from a bank account which contains the proceeds of crime.

6.6 Failure to disclose offences – ML

6.6.1 General comments

The failure to disclose provisions in Sections 136 and 137 of the POCL apply where the information on which the knowledge or suspicion is based came to a person on or after 30 June 2008, or where a person or a Nominated Officer/MLRO in the regulated sector has reasonable grounds for knowledge or suspicion on or after that date.

If the information came to a person before 30 June 2008, the old law (i.e. the Proceeds of Criminal Conduct Law (2007 Revision) or any other law relating to ML)applies. In both sections, the phrase 'knows or suspects' is used, referring to actual knowledge or suspicion - a subjective test. The phrase ‘or has reasonable grounds for knowing or suspecting’ is also used - an objective test. On this basis, the person may be guilty of the offence under Sections 136 or 137 of the POCL if he or she should have known or suspected ML.

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 136 – failure to disclose

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 criminal conduct;
- the information on which his suspicion is based comes in the course of business inthe regulated sector, or other trade, profession, business or employment; and
- he or she fails to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a Nominated Officer/MLRO or the FRA.

Making a required disclosure or being party to a joint disclosure report will both be treated as satisfying any requirement to disclose.

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 137 – failure to disclose: Nominated Officer

A Nominated Officer in the regulated sector commits a separate offence if, as a result of an internal disclosure under Section 136 of the POCL or information which comes to him or her in the course of business in the regulated sector, he or she knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct and he or she fails to disclose as soon as practicable to the FRA.

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 for not making the required disclosure;
- you are a professional legal adviser or a relevant professional adviser and the information or other matter came to you in privileged circumstances; or

- you did not receive appropriate training from your employer.

Both failure to disclose sections also reiterate that the offence will not be committed if the property involved in the suspected ML 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 LPP is not excluded by the crime/fraud exception. It is CARA's view that on this basis you will have a reasonable excuse for not making a required disclosure and will not commit a ML 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 Cayman Islands or elsewhere) is already aware of the suspected criminal conduct or ML and the non-reporter does not have any additional information which might assist the regulator or enforcement authority, or
- if the only information that you would be providing for the purposes of a required disclosure under Section 136 or 137 of the POCL is information entirely within the public domain, or
- if all the suspected predicate offending and all the suspected ML occur outside the Cayman Islands and there is otherwise no Cayman Islands nexus to the suspected criminality.

This is not intended to be an exhaustive list. Moreover, non-reporters should be aware that it will ultimately be for a court to decide the excuse for not making a required disclosure under Sections 136 or 137 of the POCL constituted a reasonable excuse. You should clearly document your reasons for concluding that you 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 LPP. It is a creation of the POCL and has an autonomous meaning.

Privileged circumstances mean information communicated:

- by a client, or a representative of a client, in connection with the giving of legal advice to the client,
- 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.

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 and nominated officers who have no knowledge or suspicion of ML, 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 adequately.

6.8 Tipping off

The offences of tipping off for ML are contained in the POCL. There are also tipping off offences for terrorist property in the TL.

6.8.1 Offences

6.8.2 Tipping off

A person commits the offence of tipping off if he or she knows or suspects that an activity in relation to which a disclosure (the original disclosure) must be made under the POCL is about to take place, is taking place or has taken place (whether or not a disclosure has been or is likely to be made), and he or she makes a subsequent disclosure to (or to the representative of) a client in connection with the giving of legal advice to the client or to any person in connection with legal proceedings or contemplated legal proceedings which is likely to prejudice any investigation which might be conducted following the disclosure (whether or not the investigation is conducted).

6.9 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 the POCL 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.

It is not tipping off to include a paragraph about your obligations under the AML/CFT/CPF legislation in your Practice's standard client engagement letter.

Chapter 7 – Legal professional privilege/LPP

7.1 General comments

Legal professionals are under a duty to keep the affairs of their clients confidential, and the circumstances in which they can disclose client communications are strictly limited.

However, Sections 133 to 137 of the POCL contain provisions for disclosure of information to be made to the FRA.

Legal professionals also have a duty of full disclosure to their clients. However, Section 139 of the POCL prohibits disclosure of information in circumstances where a SAR is required to be made (whether or not it has been or is likely to be in relation to the activity in question).

This Chapter examines the tension between a legal professional's duties and these provisions of the POCL. Similar tensions also arise with respect to the TL.

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 the POCL.

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 or her staff (if any) 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 LPP.

7.4 LPP

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 without the client’s consent. It recognises the client's fundamental human right to be candid with his or her legal adviser, without fear of later disclosure to his or her 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 records has not been the subject of a legal decision and is an evolving area of law. Attorneys 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 or her legal skills and which are directly related to the performance of the legal professional's professional duties [*Passmore on Privilege 2nd edition 2006*].

English 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]; and
- 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 or 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]; and
- 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 or her 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:

- seeking or giving advice in relation to it;
- obtaining evidence to be used in it; or
- 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 an employee 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 a client 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 you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia* [1986] 1 Lloyds 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 are 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 ML 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].

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, the POCL recognises another type of communication, one which is received in 'privileged circumstances'. This is not the same as LPP but is merely an exemption from certain provisions of the POCL, although in many cases the communication will also be covered by LPP.

The privileged circumstances exemption is found in the following legislation:

- POCL – Sections 136(2)(c) and 137(2)(b)
- TL – Sections 17(2), 23(6), Schedule 1, 1(5) Schedule 5, 1(4), 3(5), 8, 11(3), and 13(2).

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 its representative in connection with you giving legal advice;
    - by the client or its representative in connection with its seeking legal advice from you; or
    - by any person for the purpose of or 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.

Consider the crime/fraud exception when determining what constitutes the furthering of a criminal purpose.

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 that employee 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 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 or her information which is subject to LPP, 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 or her information which is privileged as between client B and his or her 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 that professional in connection with the giving by him of legal advice to that client. However, if it was given to him or her 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 POCL 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 you disclose?

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under the POCL.

If the communication was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of the POCL, which include making a disclosure to the FRA.

If neither of these situations applies, the communication will still be confidential. However, the material is disclosable under the POCL and is required to be disclosed.

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 TL 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 TL. The principal terrorist property offences in Sections 19 to 22 of the TL apply to all persons and therefore to all legal professionals. There are two specific offences of failure to disclose: Section 23, which applies to information coming to a person otherwise than in the course of a business in the regulated sector, and Section 25 of the TL (and Schedule 1) which applies to persons in the regulated sector.

The definition of regulated sector in the TL is extensive, and broadly aligns with the definition of regulated sector in the POCL.

8.3 Principal terrorist property offences

8.3.1 Section 19 – soliciting

It is an offence to knowingly provide or collect terrorist property, or attempt to do so, whether directly or indirectly, if you intend or if you have knowledge that the money or other property may be used for terrorist purposes. You can commit the offence:

- even if the act of terrorism does not actually occur or is not attempted;
- even the property is not actually used to commit or to attempt the act of terrorism, nor is linked to a specific act of terrorism;
- regardless of whether the property is from a legitimate or illegitimate source; and
- regardless of the country or territory in which the act of terrorism is intended to or does occur.

8.3.2 Section 20 – 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 it may be used for these purposes.

8.3.3 Section 21 – 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 22 – ML

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 by methods including, but not limited to the following:

- concealment;
- removal from the jurisdiction; and
- 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 ML under the POCL in Chapter 6.

8.4 Defences to principal terrorist property offences

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 26 of the TL. You do not commit an offence under Sections 19 to 22 of the TL in the following further circumstances:

- you are acting with the express consent of a constable, including civilian staff at the FRA; or
- you disclose your suspicion or belief to a constable or the FRA 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 FRA 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 23 of the TL provides that anyone, whether he or she is a nominated officer or not, must disclose as soon as reasonably practicable to a constable, or the FRA, if he or she knows or suspects that another person has committed one of the principal offences based on information which came to him or her in the course of a trade, profession, business or employment otherwise than in the course of business in the regulated sector. The test is subjective.

It is a defence, however, if

- 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.

It is also a defence under Section 23 if you made an internal report in accordance with your Practice's reporting procedures.

8.5.2 Regulated sector

Section 25 (and Schedule 1) provides that a person must disclose as soon as reasonably practicable to a constable or nominated officer if they know or suspect, or have reasonable grounds for knowing or suspecting, that another person has committed one of the principal offences based on information which came to them in the course of a trade, profession or employment in the regulated sector.

It is a defence however if you received the information on which the belief or suspicion is based in privileged circumstances, without an intention of furthering a criminal purpose.

In deciding whether or not a person has committed an offence, the court must consider whether the person followed relevant guidance.

8.6 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.

Chapter 9 – Making a disclosure

9.1 General comments

The disclosure regime for money laundering and terrorist financing is run by the FRA. The FRA began as the Financial Investigation Unit in the early 1980s, operating within police headquarters. In 2000 it underwent a name change to become the Financial Reporting Unit ("**FRU**"), with the head of unit becoming a civilian post and there being an appointed legal advisor. Line management for operational work was undertaken by the office of the Attorney General. Throughout this period, the role of the unit was to receive, analyse and investigate SARs, in addition to gathering evidence to support prosecutions.

In January 2004, with the introduction of the Proceeds of Criminal Conduct Law ("**PCCL**"), the FRU became the FRA. The PCCL mandated that the FRA become a full-fledged civilian body and that its function change from being an investigative to an analytical type financial investigation unit. Accordingly, its mandate was restricted to the receipt and analysis of financial information coupled with the ability to disseminate this intelligence to agencies, where authorised to do so by the PCCL. The FRA's existence and independence were further enshrined in the POCL, which repealed and replaced the PCCL and came into force on 30 September 2008.

For full details on the FRA and its activities view its website at: www.fra.gov.ky.

9.2 Application

All persons within the regulated sector and nominated officers/MLROs have obligations under the POCL and the TL, to make disclosures of suspicions of ML/TF and terrorist property offences.

In addition, any person may need to make a required disclosure about criminal and terrorist property.

All persons are required to make disclosures to the FRA of suspected TF.

9.3 Suspicious activity reports/SARs

9.3.1 What is a SAR?

A SAR is the name given to the making of a disclosure to the FRA under either the POCL or the TL.

9.3.2 Who discloses?

Where a Practice has a nominated officer/MLRO, either they or their deputy will make the SAR to the FRA.

9.3.3 When?

You must make a SAR as soon as practicable after you have formed a reportable suspicion or know of ML/TF (subject to privilege considerations).

9.3.4 How to disclose

Forms

The FRA has issued a preferred form to be completed when making a SAR. We encourage you to use the preferred form to enhance the FRA's ability to assess your SAR quickly.

The FRAs preferred method for institutions and individuals is to submit their suspicion on the SAR Form available on the FRA's website (http://www.fra.gov.ky/contents/page/4),. On completion, the report can be delivered by hand to the Cayman Islands Government Administration Building or faxed to 345 945 6268.

9.3.5 No option of getting consent from the FRA to proceed

NOTE: There are no 'consent' or Defence Against Money Laundering ("DAML") SARs in the Cayman Islands. Keep the FRA informed of your approach.

9.3.6 Confidentiality of SARs

The FRA is required to treat your SARs confidentially. Where information from a SAR is disclosed for the purposes of supervision or law enforcement, care is taken to ensure that the identity of the reporter and his or her Practice are not disclosed to other persons.

If you have specific concerns regarding your safety if you make a SAR, you should raise this with the FRA either in the report or through its helpdesk. If you have concerns about your immediate safety following the making of a SAR, or that the confidentiality of a SAR you have made has been breached, you should contact the Royal Cayman Islands Police Service.

Chapter 10 – Enforcement

10.1 General comments

The Cayman Islands' AML/CFT/CPF regime is robust. 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

The Regulations define a Supervisory Authority as CIMA or any other body that may be assigned the responsibility of monitoring compliance with ML regulations made under the POCL in relation to persons carrying out RFB, who are not otherwise subject to such monitoring by CIMA.

CILPA has been designated as the AML supervisor for firms of attorneys in the Cayman Islands. Its supervisory functions have been delegated to a body formed as CARA. CARA has operational independence and employs professional regulatory staff. For more information, please visit www.cara.ky.

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 should:

- identify and assess the international and domestic risks of ML/TF 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 disclosure obligations under Part XII of the Regulations;
- take appropriate measures, in accordance with an RBA, to review Practices' risk assessments and policies, controls and procedures;
- report to the FRA any suspicion that a person it is responsible for has engaged in ML/TF;
- make up to date information on ML/TF available to the persons it supervises;
- co-operate and co-ordinate their activities with other supervisory authorities, and law enforcement authorities; and
- collect certain information about the persons it supervises, and any other information it considers necessary for exercising its supervisory function.

10.2.1 Enforcement powers under the Regulations

The Regulations give supervisory authorities a variety of powers for performing their functions under the Regulations, including the ability to request that information from persons carrying out RFB be provided without delay.

The Regulations also provide for fines and enforcement powers in relation to DNFBPs, in Part XIIA.

10.3 Disciplinary action against legal professionals

Conduct which fails to comply with AML/CFT/CPF obligations may also be a breach of professional obligations under the Cayman Islands Code of Conduct for Attorneys.

10.4 Offences and penalties

Not complying with AML/CFT/CPF 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 POCL - relevant offences and penalties

Section	Description	Penalty
133	Concealing, disguising, converting, transferring or removing criminal property	On summary conviction – up to two years' imprisonment or a fine of five thousand dollars, or both
134	Entering into or becoming concerned in an arrangement regarding criminal property	On indictment – up to 14 years' imprisonment or a fine, or both
135	Acquiring, using or having possession of criminal property	
136	Failing to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering	On summary conviction – up to two years' imprisonment or a fine of up to five thousand dollars or both
137	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – nominated officer where the information came to him or her either in the course of business in the regulated sector or in consequence of a disclosure made under section 136	On indictment – up to five years' imprisonment or a fine or both
139	Tipping off	

10.4.2 Regulations - relevant offences and penalties

A person who breaches the Regulations commits an offence and is liable:

- on summary conviction, to a fine of five hundred thousand dollars; or
- on conviction on indictment, to a fine and to imprisonment for two years.

In determining whether a breach has occurred the court will consider compliance with this Guidance.

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 the Practice and the individual can be jointly liable.

Chapter 11 – Civil liability

11.1 General comments

The POCL 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 advisers 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 it has 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 his or her own 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 is 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 English 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 wilful 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 he or she is 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 wilful blindness by deliberately failing to make the enquiries that a reasonable and honest person would make.

11.5 Making a disclosure to the FRA

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 its retainer.

English 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 English 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 English 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 the UK's Proceeds of Crime Act as an exception to the tipping off provisions.

The position in England and Wales is slightly different as the consent regime applies to ML as well as TF. However, this case law is still considered relevant and informative.

NOTE: As mentioned, there are no 'consent' or DAML SARs in the Cayman Islands. Keep the FRA informed of your approach.

In continuing with a transaction, you must ensure that either:

- although you had sufficient suspicion to justify a disclosure to the FRA, 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 AML/CFT/CPF 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 English Courts have provided limited assistance in this area. *Bank of Scotland v A Limited* [2001] 1 WLR 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 English 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.

Chapter 12 – ML warning signs

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 ML/TF risks.

The POCL 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 be 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 being asked 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 AML/CFT/CPF 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 be a cause for concern:

- 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; or
- 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 or a law enforcement agency;
- settlements paid in cash, or paid directly between parties (e.g. 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 ML. 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 ML. 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 ML taking place and whether it is a circumstance requiring a disclosure to the FRA.

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 enable someone to deposit money 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 the client's name, from the Cayman Islands 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 country or territory

A retainer involving countries or territories which do not have comparable AML/CFT/CPF ML 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.

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 ML 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 ML 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 the POCL and the provisions relating to overseas criminal conduct; and
- where estate assets have been earned or are located in a suspect country or 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 135 of the POCL may lead to a ML offence being committed at an early point in the administration. The Section 134 offence under the POCL of arranging 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. 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 he or she does 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 his or her lifetime.

If, for example, you know or suspect that the deceased person improperly claimed welfare benefits or had evaded the due payment of tax during his or her lifetime, criminal property will be included in the estate and so a ML 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, under UK law, by failing to disclose gifts received from the deceased fewer than seven years before death). Although these matters may not actually constitute ML (because no criminal conduct has yet occurred so there is no 'criminal property'), attorneys should carefully consider their position with respect to their professional obligations.

Grant of probate

A Cayman Islands grant of probate may be required before Cayman Islands 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 country or territory.

If the deceased person is from another jurisdiction and a legal professional is dealing with the matter in that jurisdiction, 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 ML 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 ML 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 trustee(s), the nature of the work may already require information which will help in assessing ML 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 ML procedures, may increase the risk profile of the retainer.

If you think a ML 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 134 arrangement offence under the POCL. If they do, consider the options for making a disclosure.

Consider also whether a Section 136 disclosure obligation under the POCL 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 ML/TF vehicles.

If you are acting for a charity, consider its purpose and the organisations with which it is aligned. A charity which is registered 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. See also the FRA's website and OFSI's Financial Sanctions Guidance.

https://www.gov.uk/government/publications/financial-sanctions-faqs

12.3.4 Powers of attorney

Whether acting as, or on behalf of, an attorney-in-fact, you should remain alert to ML risks.

Consider also your obligations to identify the authority of attorney-in-fact to act on behalf of the client and verify his or her identity.

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 FRA.

If you discover or suspect that a donee has already completed an improper financial transaction that may amount to a ML suspicion, a disclosure to the FRA may be required (depending on whether LPP 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 ML vehicles to disguise the true owner and/or confuse the audit trail. You will need to identify the property-owning vehicle's beneficial owners where it is your client.

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 100% private funding 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; or
- payments from several individuals or sources.

If you are concerned:

- ask your client to explain the source of the funds. Assess whether you think its explanation is valid (for example, the money may have been received from an inheritance or from the sale of another property); and
- 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 into 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.

Where you act for a vendor, you will also typically receive funds from the buyer or its solicitors, which you may hold on the buyer's behalf, pending an exchange or completion process. Where

funds come direct to you from an unrepresented buyer you will need to undertake CDD on the buyer.

Direct payments between buyers and sellers

If you suspect that there has been a direct payment between a seller and a buyer, consider whether there are any reasons for concern or whether the documentation will include the true purchase price.

12.4.3 Valuing

An unusual sale price (an evident overvalue or undervalue) can be an indicator of ML. While you are not required to get independent valuations, if you become aware of a significant discrepancy between the sale price and any valuation provided, 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 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 the POCL.

If you discover or suspect that a mortgage advance has already been improperly obtained, consider your disclosure obligations under the POCL.

If you are acting in a re-mortgage and discover or suspect that a previous mortgage has been improperly obtained, you may need to consider making a disclosure to the FRA as there is criminal property (the improperly obtained mortgage advance).

Tipping off offences

In relation to asking further questions of your client and discussing the implications of the POCL, there is a specific defence for tipping off for legal advisers who are seeking to dissuade their client from engaging in a ML offence.

For further advice on tipping off, see Section 6.8.

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 134 arrangements offence under the POCL.

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 at 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 ML/TF.

If the company is being formed in a foreign jurisdiction, you should clarify why this is the case. In countries where there are few AML/CFT/CPF requirements, you should make particularly careful checks.

Refuse the retainer if you have doubts or suspicions and consider your disclosure obligations under the POCL.

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/entity acting on its behalf.

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 individual 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 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 new vehicle/entity, you will need to obtain documentation evidencing the establishment of the new vehicle/entity and consider the issue of beneficial ownership.

Generally private equity work will be considered at low risk of ML/TF for the following reasons:

- a private equity firm in the Cayman Islands is also covered by the Regulations as a financial institution;
- investors in private equity funds may be large institutions, some of which will also be regulated for ML purposes;
- where the private equity sponsor or fund manager is regulated in the Cayman Islands or a comparable jurisdiction, 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; and
- 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 ML to a standard which is equivalent to the Cayman Islands;
- where the investor is either an individual or an investment vehicle itself (a private equity fund of funds); or
- where the private equity sponsor is seeking to raise funds for the first time.

You may wish to consider the Guidance Notes.

The following points should be considered when undertaking CDD measures in relation to private equity work:

- where your client qualifies for SDD, you do not have to identify beneficial owners unless there is a suspicion of ML; 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 SDD 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 that professional in accordance with the Regulations;
- 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;
    - its track record within the private equity sector; and
    - its 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, the source may simply confirm its 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; and
- 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 new vehicle/entity. However, once you start acting for a new vehicle/entity, you will need to consider identification for it, and its beneficial owner(s). 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; or
- a prospectus is issued to invite investment.

Factors which will increase the risks include circumstances where:

- the scheme is open to non-tax exempt investors;
- the scheme or any of its investors is located in any jurisdiction which is not regulated for ML to a standard which is equivalent to that of the Cayman Islands; or
- neither the scheme nor any of its investment managers is regulated and no CDD is conducted on the investors.

You should also consider the Guidance Notes.

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 through 11 of this Guidance worked through the theory of the law relating to when an 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 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 Sections 133 and 135 of the POCL are relatively straightforward to assess. However, an arrangement offence under Section 134 of the POCL may be more complicated, particularly with transactional matters.

13.2.1 Do I have an arrangement?

Under Section 134 of the POCL, 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 it in the purchase of a property, including the drafting of the contract and transfer documents. When you are instructed there will already be an arrangement between the vendor and the purchaser, but not yet an arrangement for the purposes of Section 134 of the POCL.

If an arrangement within Section 134 of the POCL 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 134 of the POCL 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 134 of the POCL, and possibly under Section 133 or 135 of the POCL.

Consider whether you need to make a required disclosure to provide yourself with a defence to the principal ML offences. Consider whether you risk committing a failure to disclose offence if you do not make a disclosure to the FRA.

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 the POCL:

- 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 the POCL.
- If the information was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of the POCL, which include making a disclosure to the FRA.

  If neither of these situations applies, the communication will still be confidential.

However, the material is disclosable under the POCL and a required disclosure should be made.

You have the option of withdrawing from the transaction rather than making a required disclosure, but you may still need to make a disclosure to avoid committing a failure to disclose offence.

NOTE: There are no 'consent' or DAML SARs in the Cayman Islands. Keep the FRA informed of your approach

What if you cannot disclose?

If you decide that either you cannot make a disclosure due to LPP or 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; 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 it agrees to waive privilege, you can make a disclosure to the FRA 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 FRA.

Refusal to waive privilege

Your client, whether sole or one of a number for whom you act, may refuse to waive privilege, either because it does not agree with your suspicions or because it 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 advise 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.

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 the POCL.

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 the POCL) is saved costs.

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 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 several 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 its 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 (e.g. 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 ML (which may simply mean they possess the benefits of a criminal offence contrary to Section 135 of the POCL). 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 ML offence may be committed:

- the vendor may commit a Section 133 offence under the POCL by transferring the criminal property;
- both the vendor and purchaser may be entering into an arrangement contrary to Section 134 of the POCL; or
- the purchaser may be committing a Section 135 offence under the POCL 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 135 possession offence under the POCL. 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 134 of the POCL?

It is a question of interpretation whether Sections 134 and 135 of the POCL should be read together such that, if the defence under Section 135 of the POCL applies, an offence will also not be committed by the vendor under Section 134 of the POCL. 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 their position after completion.

The purchaser will, after the transaction, have possession of the assets and may be at risk of committing a Section 135 offence under the POCL (subject to the adequate consideration defence outlined above).

The vendor will have the sale consideration in its 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 135 of the POCL.

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 ML 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.

When considering whether to advise your client about their disclosure obligations, remember the tipping off offence.

Are you 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, 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 ML 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 considerations that differ from those applicable 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 133 offence (for the vendor), or a Section 135 offence (for the purchaser) under the POCL.

However, the sale of shares could constitute a Section 134 offence under the POCL, depending on the circumstances, particularly if the criminal property represents a large percentage of the value of the target company. Disclosure may be required 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, i.e. 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 its directors may subsequently transfer, use or possess the assets for the purposes of the principal ML offences in Sections 133 and 135 under the POCL.

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 so that they may transfer, use or possess 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), 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 134 of the POCL.

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 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 134 of the POCL.

Firstly, consider whether the shareholders are, or may become, aware 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 ML 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.

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 FRA to ensure that there are no tipping off concerns if details of the risks are set out in a public circular.

Each shareholder's express authority to make a disclosure will be required. It may be simplest to ask the shareholders to authorise the board of the vendor to make a disclosure 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 Cayman Islands.

Even where the conduct is lawful overseas, in serious cases it will still be disclosable if the ML is taking place in the Cayman Islands and the underlying conduct would be criminal if it had occurred in the Cayman Islands.

In some cases the only ML activity in the Cayman Islands may be your involvement in the transaction as a Cayman Islands legal professional.

NOTE: There are no 'consent' or DAML SARs in the Cayman Islands. Keep the FRA informed of your approach.