THE LAW SOCIETY
OF SINGAPORE

PREVENTION OF MONEY LAUNDERING (INCLUDING PROLIFERATION FINANCING) AND FINANCING OF TERRORISM

PRACTICE DIRECTION [3.2.1]

[Formerly Practice Direction (Para 1 of 2015)]

Date: 3 October 2023

Contents

DEFINITIONS AND GLOSSARY OF TERMS USED IN THIS PRACTICE DIRECTION

Definitions

Definition in the Legal Profession Act (Cap 161, 2009 Rev Ed)	
Relevant matter	Means any of the following matters - (*a*) acquisition, divestment or any other dealing of any interest in real estate; (*b*) management of client's moneys, securities or other assets, or of bank, savings or securities accounts; (*c*) creation, operation or management of any company, corporation, partnership, society, trust or other legal entity or legal arrangement; (*d*) acquisition, merger, sale or disposal of any company, corporation, partnership, sole proprietorship, business trust or other business entity; (*e*) any matter, in which a legal practitioner or law practice acts for a client, that is unusual in the ordinary course of business, having regard to — (i) the complexity of the matter; (ii) the quantum involved; (iii) any apparent economic or lawful purpose of the matter; and (iv) the business and risk profile of the client.
Definitions in the Legal Profession (Prevention of Money Laundering And Financing of Terrorism) Rules (S 307/2015)	
Beneficial owner	In relation to an entity or a legal arrangement — (*a*) means — (i) an individual who ultimately owns or controls the entity or legal arrangement; or (ii) an individual on whose behalf the entity or legal arrangement conducts a transaction concerning a relevant matter (being a transaction for which a legal practitioner or law practice is engaged); and (*b*) includes an individual who exercises ultimate effective control over the entity or legal arrangement.
Client	Includes — (*a*) in relation to contentious business, any person who, as a principal or on behalf of another person, retains or employs, or is about to retain or employ, a legal practitioner or law practice; and (*b*) in relation to non-contentious business, any person who, as a principal or on behalf of another person, or as a trustee, an executor or an administrator, or in any other capacity, has power, express or implied, to retain or employ, and retains or employs or is about to retain or employ, a legal practitioner or law practice.
Close associate	In relation to a politically-exposed individual, means an individual who is known to be closely connected to the politically-exposed individual, either socially or professionally, such as, but not limited to — (*a*) a partner of the politically-exposed individual; (*b*) an employee or employer of the politically-exposed individual; (*c*) a person accustomed or under an obligation, whether formal or informal, to act in accordance with the directions, instructions or wishes of the politically-exposed individual; or

	(*d*) a person whose directions, instructions or wishes the politically-exposed individual is accustomed or under an obligation, whether formal or informal, to act in accordance with.
Commercial Affairs Officer	Means a Commercial Affairs Officer appointed under section 64 of the Police Force Act (Cap 235).
Countermeasure	Means a measure to prevent, or to facilitate the prevention, of money laundering or the financing of terrorism in a country or jurisdiction other than Singapore.
Domestic politically-exposed individual	Means an individual who is or has been entrusted with a prominent public function in Singapore.
Entity	Means a sole proprietorship, a partnership, a limited partnership, a limited liability partnership, a corporation sole, a company or any other association or body of persons corporate or unincorporate.
Family member	In relation to a politically-exposed individual, means a spouse, child (including an adopted child or a stepchild), sibling or parent of the politically-exposed individual.
Foreign politically-exposed individual	Means an individual who is or has been entrusted with a prominent public function in a country or jurisdiction other than Singapore.
Legal arrangement	Means any express trust or other similar legal arrangement.
Politically-exposed individual	Means — (*a*) a foreign politically-exposed individual; (*b*) a domestic politically-exposed individual; or (*c*) an individual who has been entrusted with a prominent function in an international organisation.
Prominent function	In relation to an international organisation, means the role held by a member of the senior management of the international organisation (including a director, deputy director or member of a board of the international organisation, or an equivalent appointment in the international organisation).
Prominent public function	Includes the role held by a head of state, a head of government, a senior politician, a senior government, judicial or military official, a senior executive of a state-owned corporation or a senior political party official.
Relevant Singapore financial institution	Means — (*a*) a bank in Singapore licensed under section 7 of the Banking Act (Cap 19); (*b*) a merchant bank approved under section 28 of the Monetary Authority of Singapore Act (Cap 186); (*c*) a finance company licensed under section 6 of the Finance Companies Act (Cap 108); (*d*) a financial adviser licensed under section 13 of the Financial Advisers Act (Cap 110), except one which is licensed only in respect of the financial advisory service specified in item 2 of the Second Schedule to that Act (namely, advising others by issuing or

	promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product); (*e*) a holder of a capital markets services licence granted under section 86 of the Securities and Futures Act (Cap 289); (*f*) a fund management company registered under paragraph 5(7) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Cap 289, Rg 10); (*g*) a person who is exempt from holding a financial adviser's licence under section 23(1)(f) of the Financial Advisers Act read with regulation 27(1)(d) of the Financial Advisers Regulations (Cap 110, Rg 2), except one who is exempt only in respect of the financial advisory service specified in item 2 of the Second Schedule to that Act (namely, advising others by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product); (*h*) a person who is exempt from holding a capital markets services licence under section 99(1)(h) of the Securities and Futures Act read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations; (*i*) a trustee approved under section 289 of the Securities and Futures Act for a collective investment scheme authorised under section 286 of that Act; (*j*) a trust company licensed under section 5 of the Trust Companies Act (Cap 336); or (*k*) a direct insurer licensed under section 8 of the Insurance Act (Cap 142) to carry on life business.
Suspicious transaction report or STR	Means a report by which a person — (*a*) discloses, under section 39(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A), any knowledge or suspicion referred to in that provision, or the information or other matter on which that knowledge or suspicion is based, to a Suspicious Transaction Reporting Officer; or (*b*) informs, under section 8(1) of the Terrorism (Suppression of Financing) Act (Cap 325), a police officer or Commercial Affairs Officer, of any fact or information referred to in that provision.
Suspicious Transaction Reporting Officer	Has the same meaning as in section 2(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.
Definitions in the Trustees Act, Part VI; Trustees (Transparency and Effective Control) Regulations 2017	
Connected individual	(a) In relation to an entity that is a partnership, means any partner or manager; (b) In relation to a trust or other similar arrangement, means any individual having executive authority in the trust or other similar arrangement; and (c) In relation to any other entity, means any director, or any individual having executive authority, in the entity.
Effective controller	Effective controller in relation to a relevant trust party of a relevant trust, means – (a) the individual who ultimately owns or controls the relevant trust

	party; or (b) the individual on whose behalf a transaction is being conducted by the relevant trust party in the relevant trust party's capacity as such, and includes an individual who exercises ultimate effective control over the relevant trust party;
Prescribed transaction	A transaction that has an aggregate value or amount of more than S$20,000, whether the transaction is carried out in a single operation or multiple operations that appear to be linked.
Relevant party	In relation to a relevant trust, means a relevant trust party of the relevant trust.
Relevant trust party	In relation to a trust, means all or any of the following: (a) a settlor; (b) a trustee; (c) a protector; (d) a beneficiary; and/or (e) a person who has any power over the disposition of any property that is subject to the trust.
Service supplier	An agent of, or a service provider to, the relevant trust (including any investment adviser or manager, accountant, or tax adviser).
Specified person	(a) a financial institution as defined in section 27A(6) of the Monetary Authority of Singapore Act (Cap. 186), read with section 27A(7) of that Act; (b) a casino operator as defined in section 2(1) of the Casino Control Act (Cap. 33A); (c) a licensed operator as defined in section 3(1) of the Estate Agents Act (Cap. 95A); (d) a dealer in precious stones or precious metals as defined in regulation 2 of the Corruption, Drug Trafficking and Other Serious Crimes (Cash Transaction Reports) Regulations 2014 (G.N. No. S 692/2014). (e) an advocate or solicitor who (i) has in force a practicing certificate; or (ii) is a director, a partner, a consultant, or an employee of a law practice, whether or not the advocate and solicitor has in force a practicing certificate; (f) a regulated foreign lawyer as defined in section 2(1) of the Legal Profession Act; (g) a foreign lawyer registered under section 36P of the Legal Profession Act; (h) a notary public as defined in section 2 of the Notaries Public Act (Cap. 208); (i) a public accountant as defined in section 2(1) of the Accountant Act (Cap. 2); or (j) a person (not being a person mentioned in paragraph (e) or (f) or a public accountant) who provides one or more of the following services: (i) acting as an agent for the formation of entities; (ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a person holding a similar position in any other entity;

	(iii) providing a registered office, any business address or any accommodation, correspondence, or administrative address for an entity; (iv) acting as (or arranging for another person to act as) a trustee of an express trust, or performing (or arranging for another person to perform) a function equivalent to the function of a trustee in any other similar arrangement; (v) acting as (or arranging for another person to act as) a nominee shareholder for another person.

Glossary

AML	Anti-Money Laundering
CDD	Customer Due Diligence or Client Due Diligence
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A, 2000 Rev Ed)
CPF	Countering Proliferation Financing, i.e. possible breaches or evasion of targeted financial sanctions as imposed by the United Nations Security Council, in particular in respect of North Korea and Iran.
CTF	Countering Terrorism Financing
DNFBP	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence or Enhanced Client Due Diligence
FATF	Intergovernmental body known as the Financial Action Task Force created in 1989
LPA	Legal Profession Act
MER 2016	Singapore Mutual Evaluation Report September 2016
ML	Money laundering
PCR	Legal Profession (Professional Conduct) Rules 2015
PF	Proliferation financing for nuclear and other weapons of mass destruction
Rules	Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules
TF	Terrorism financing
TSOFA	Terrorism (Suppression of Financing) Act (Cap 325, 2003 Rev Ed)
WMD	Weapons of Mass Destruction

Part 1 - Introduction

Legal practitioners are often, for good and legitimate reasons, the holders of large sums of money involved in commercial transactions and this means that fewer questions are liable to be asked when the lawyers pay out such sums to their clients or to third parties on their clients' instructions. Lawyers are also subject to confidentiality obligations which appeal to those who engage in money laundering activities and wish to hide their identities and activities under the cloak of legal privilege. There is thus a real risk that proceeds of crime could flow into Singapore via local law firms under the pretense of being moneys from legitimate transactions with the remitters wishing to give an appearance of legitimacy to any activity that the money is used for after being "cleansed" through the lawyer's client accounts. Given Singapore's reputation as a jurisdiction with strict controls aimed at eliminating illicit activities, it is all the more important for our solicitors, as potential fiduciary recipients of large sums of money, to understand and comply with obligations that aim to avoid exposing the profession to the risk of unintentionally assisting in the conduct of criminal activity." Judith Prakash JA in Re Chan Chun Hwee Allan [2018] SGHC 21, [35]

In respect of, inter alia, lawyers "The sector presents higher ML/TF vulnerability given that AML/CFT measures and their implementation are not as strong as those in the financial sector." MER 2016 page 19

"…many law practices did not have specific policies or procedures on how to deal with situations where they have to file an STR and the consequential consideration in relation to a client whom they have filed an STR against." MER 2016 page 94

This Practice Direction of the Council of the Law Society of Singapore ('Council') supersedes Practice Directions 1 of 2015 and 3.2.1 of 2020. It takes into the consideration the developments in law and practice since 2020.

1.1 Scope of Practice Direction

Part VA of the Legal Profession Act (Cap 161, 2009 Rev Ed) ('Part VA') on the "Prevention of Money Laundering and Financing of Terrorism" and the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015 (S 307/2015) ('Rules') applies to all legal practitioners in Singapore, whether a Singapore admitted advocate and solicitor or foreign law practitioner (section 70A Legal Profession Act).

The Rules are made in accordance with section 70H of the Legal Profession Act.

Legal practitioners and law practices must familiarise themselves with Part VA and the Rules and comply with them.

This Practice Direction sets out directions and guidance on Part VA and the Rules, and must be read together with Part VA and the Rules.

1.2 Summary of the obligations under Part VA and the Rules

In essence, Part VA and the Rules require a legal practitioner and law practice to undertake the following:

(a) Perform CDD measures (section 70C Part VA and Part 2 of the Rules)
A legal practitioner and law practice are required to conduct CDD not only on the client and any individual purporting to act on behalf of a client, but on all the beneficial owners of the client if it is an entity or legal arrangement and to pay particular attention if any persons involved are politically-exposed individuals.

(b) File a suspicious transaction report (section 70D Part VA, Parts 2 and 5 of the Rules)
If the legal practitioner and law practice have suspicions that their client is engaged in money laundering or the financing of terrorism. Failure to file a suspicious transaction report is an offence. The legal practitioner and law practice should note two aspects of this obligation to report in particular:

(i) The legal practitioner and law practice cannot tell anyone that they have reported, including their client, as doing so may amount to 'tipping-off'.

(ii) Failure to disclose any information or other matter which is an item subject to legal privilege is not an offence (CDSA).

Lawyers must also be aware of the rules regarding tipping off. If a lawyer suspects that a client may be engaged in money laundering or the financing of terrorism, and the lawyer has reasonable grounds to believe that the performance of any CDD measures will tip-off the client, by rule 16 of the Rules, the lawyer —

(a) need not perform those CDD measures; **but**

(b) must instead file a suspicious transaction report with either or both of the following (as the case may be):

(i) a Suspicious Transaction Reporting Officer, if the client may be engaged in money laundering; and/or

(ii) a police officer or Commercial Affairs Officer, if the client may be engaged in the financing of terrorism.

(c) Maintain all documents and records (section 70E Part VA and Part 3 of the Rules)
Relating to each relevant matter, and all documents and records obtained through CDD measures.

(d) For legal practitioners acting as trustees, the following CDD measures are necessary (section 84A of the Trustees Act).

(i) Obligation to perform CDD measures on relevant parties, effective controllers of relevant parties, as well as service suppliers: Within a specified time limitation, the legal practitioner must take reasonable steps to ensure that information about these parties is obtained and verified.

(ii) Obligation to disclose that trustee is acting for a relevant trust: If a trustee of a relevant trust, when acting for the relevant trust, forms a business relationship with any specified person after 30 April 2017, the trustee must, at or before the time the business relationship is formed, take reasonable steps to inform the specified person that the trustee is acting for the relevant trust.

(iii) Obligation to keep accounting records: A trustee of a relevant trust must take reasonable steps to ensure that there are kept in respect of the relevant trust, accounting records in the format explained below and in, Trustees Act, Trustees (Transparency and Effective Control) Regulations 2017, at 9(2) and 9(3).

1.3 Terminology used in this Practice Direction

Terms in the Legal Profession Act and the Rules have the same meaning in this Practice Direction, unless the context requires otherwise.

You – refers to a legal practitioner or law practice.

Must – refers to a specific requirement in legislation. You must comply unless there are statutory exemptions or defences.

Should – it is good practice in most situations, and these may not be the only means of complying with legislative requirements.
May – a non-exhaustive list of options to choose from to meet your obligations.

1.4 Money laundering and financing of terrorism

Part VA and the Rules set out the measures which a legal practitioner and law practice must take, when preparing for or carrying out any transaction concerning a relevant matter with a view to preventing the transaction from being used to facilitate either or both money laundering and the financing of terrorism.

1.4.1 Definition of money laundering and financing of terrorism

Money laundering is a process by which criminals attempt to conceal the true origin and ownership of money and other benefits derived from criminal conduct so that the money and other benefits appear to have a legitimate source.

Generally, money laundering involves three (3) stages, in the following order:

(a) Placement – This is the physical movement of the benefits (usually cash) from criminal conduct.

(b) Layering – This is the process of separating the benefits of criminal conduct from the illegitimate source through layers of financial transactions to disguise the audit trail.

(c) Integration – If the layering process is successful, the integration stage will place the laundered money and other benefits back into the economy so that they appear to be legitimate.

1.4.2 Legislation applicable to all persons

Legislation that applies to all persons in relation to money laundering is the CDSA; and legislation in relation to terrorism financing that applies to all persons is the TSOFA.

It is an offence under section 50 of the CDSA to assist another to retain benefits of drug dealing, and an offence under section 51 of the CDSA to assist another to retain benefits from criminal conduct. In May 2023 Parliament expanded the mens rea for these offences. Accordingly, the following mental states suffice:

- Knowing
- Having reasonable grounds to believe
- Rashly
- Negligently

There is also a new offence of money laundering in certain circumstances. Of particular interest to lawyers is enabling a client to money launder after failing to take reasonable steps to ascertain the purpose of the transaction from the client(s55A(1)(b)(ii) (B) CDSA) and failing to take reasonable steps to ascertain the source or destination of money (s55A(1)(b)(iv)(B) CDSA).

Legal practitioners should refer to the TSOFA to understand what constitutes a terrorist financing offence under the TSOFA, what the prohibitions are and what the duty to disclose entails in relation to terrorist financing. Unlike money laundering, the source of terrorist financing may be legitimate or illegitimate.

Under the TSOFA, a terrorist is defined as anyone who commits, or attempts to commit, any terrorist act or participates in or facilitates the commission of any terrorist act. It also includes any person set out in the First Schedule of the TSOFA. The First Schedule refers to specific individuals, all individuals and entities belonging to or associated with the Taliban in the Taliban List, and all individuals and entities belonging to or associated with the Al-Qaida organization in the Al-Qaida List as maintained by the

United Nations pursuant to the United Nations Security Council resolutions. (The latest updates to the Lists can be found at the relevant weblinks on the Law Society's website on Anti-Money Laundering) Sections 3 to 6 of the TSOFA expressly prohibit the following:

(a) provision and collection of property for terrorist acts;
(b) provision of property or services for terrorist purposes;
(c) use or possession of property for terrorist purposes; and
(d) dealing with property of terrorists or terrorist entity.

The United Nations Security Council have also announced targeted financial sanctions against certain other countries. These sanctions are given effect to in Singapore by regulations under the United Nations Act, and are predicate offences for the purposes of the CDSA. Of particular importance are the sanctions in respect of North Korea and Iran. The references to countering proliferation financing refers to countering attempts to breach or evade these specific sanctions. The other countries subject to targeted financial sanctions are Sudan, Central African Republic, Democratic Republic of Congo, Libya, Yemen, Mali, Somalia, and South Sudan. References to ML/AML will also include PF/CPF.

Since 2022, Singapore has also imposed its own sanctions on dealings in certain items with Russia. Practitioners should be alert for attempts to evade or breach such sanctions as such actions will be predicate offences under the CDSA.

Legal practitioners and law practices must familiarise themselves with the CDSA and the TSOFA and comply with the same.

1.5 Relevant matter

Part VA and the Rules apply to a legal practitioner and law practice preparing for or carrying out any transaction concerning a relevant matter.

The definition of "relevant matter" in the Legal Profession Act includes the "management of client's moneys, securities or other assets, or of bank, savings or securities accounts". This involves doing more than merely opening a client account[1]. What it refers to is the situation where the lawyer actually manages the client's assets and property, what is referred to in some jurisdictions as "man of affairs work"[2]. Situations where a legal professional may be undertaking these activities legitimately may involve a client who has limited capacity to manage his/her own affairs.

If a transaction does not concern a relevant matter, then the obligations under Part VA and the Rules do not need to be observed although, clearly, good due diligence on one's client is always good practice. Please note that the CDSA and TSOFA impose substantive legal obligations that are not necessarily connected directly with CDD. Their applicability is therefore **not** dependent on whether the matter is a relevant matter.

If you are uncertain whether Part VA and the Rules apply to your work generally or in a specific case, simply take the broadest of the possible approaches to comply with the statutory requirements. You can seek guidance from the Law Society.

Unless it is a matter that is unusual in the ordinary course of business, having regard to the complexity of the matter, the quantum involved, any apparent economic or lawful purpose of

[1] FATF Guidance for a Risk-Based Approach Legal Professionals para 44
[2] FATF Guidance For a Risk-Based Approach Legal Professionals para 52

the matter, and the business and risk profile of the client, the following are some examples of transactions and matters which Part VA and the Rules would not apply to:

(a) General Singapore law advice with no specific or substantial association with any transaction or matter.
(b) Transactions and matters pertaining to intellectual property rights.
(c) Acting for a client to apply for a grant of probate or letters of administration as a personal representative of an estate.
(d) Acting for a client in a family law matter to obtain a decree of nullity or divorce or custody/access of children.
(e) Appearing or pleading in any court of justice in Singapore, representing a client in any proceedings instituted in such a court or giving advice, the main purpose of which is to advise the client on the conduct of such proceedings.
(f) Appearing in any hearing before a quasi-judicial or regulatory body, authority or tribunal, including an arbitral tribunal.

Part 2 – Risk Assessment, Internal Policies, Procedures and Controls

2.1 Assessing your law practice's risk profile

A law practice must take appropriate steps to identify, assess and understand, its money laundering, proliferation financing and terrorism financing risks, taking into account the law practice's size, type of clients, countries or jurisdictions its clients are from and the practice areas it engages in.

The appropriate steps must include:

(a) documenting the law practice's risk assessments;
(b) considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;
(c) keeping these risk assessments up to date; and
(d) having appropriate mechanisms to provide risk assessment information to the Council.

There is a template available on the Law Society website that a practice can use to document its risk assessment.

The Law Society assesses the primary AML/CTF/CPF risks for the legal sector as a whole as:

- Property transactions in particular the acquisition and disposal of properties, both commercial and residential.
- Setting up of shell companies and other legal arrangements, and the provision of nominee directors and shareholders.
- Use of the client account to transmit money.

Singapore has a history as a trading nation and there is a record of illegal deals with Iran and North Korea. Those practices that are advising on international trade matters should be conscious of the need to be alert of attempts to breach or evade targeted financial sanctions.

The specific vulnerabilities of Singapore can be found in the Singapore National Risk Assessment Report 2013 and Terrorism Financing National Risk Assessment 2020. Each law practice should make its own assessment of its risk.

2.1.1 Programmes for the prevention of money laundering and the financing of terrorism

Rule 18(1) of the Rules requires a law practice to implement programmes for the prevention of money laundering and the financing of terrorism which have regard to:

(a) the risks of money laundering and the financing of terrorism; and

(b) the size of the law practice.

Taking into account the risks that have been identified and the size of a law practice, a law practice must develop programmes for the prevention of money laundering and the financing of terrorism. This should include an assessment of the level of exposure the practice has to overseas clients and the risk that these clients and/or their beneficial owners may be PEPs or subject to sanctions.

If there is a significant risk, law practices are strongly encouraged to subscribe to a reliable commercial database that will allow you to screen customers for ML/TF/PF/ risk.

2.1.2 Group–wide programmes for a Singapore law practice with any branch or subsidiary

If a Singapore law practice has any branch or subsidiary (whether in Singapore or elsewhere), the Singapore law practice must implement group-wide programmes for the prevention of money laundering and the financing of terrorism that apply to, and are appropriate for (rule 18(2) of the Rules) —

(a) every such branch; and
(b) every such subsidiary more than 50% of the shares or other equity interests of which are owned by the Singapore law practice.

If a Singapore law practice has any foreign branch or foreign subsidiary, the Singapore law practice must, as far as possible, ensure that every such foreign branch and foreign subsidiary apply measures for the prevention of money laundering and the financing of terrorism that are consistent with the measures that are applicable in Singapore (rule 18(4) of the Rules).

A 'Singapore law practice' does not include a Qualifying Foreign Law Practice, a licensed foreign law practice, the constituent foreign law practice of a Joint Law Venture, or a foreign law practice which is a member of a Formal Law Alliance.

In the case of a subsidiary that is not a law practice and which is required to apply measures for the prevention of money laundering and terrorism financing that are applicable in Singapore to the local subsidiary (such as those in the Accounting and Corporate Regulatory Authority (Filing Agents and Qualified Individuals) Regulations 2015 (S 198/2015)) it will suffice for the law practice to ensure that the subsidiary applies those measures.

2.1.3 Internal policies, procedures and controls

The programmes that a law practice must implement, and the group-wide programmes a Singapore law practice (with any branch or subsidiary) must implement must include the following (rule 18(3) of the Rules):

(a) the development and implementation of internal policies, procedures and controls for the prevention of money laundering and the financing of terrorism, including –
    (i) appropriate compliance management arrangements; and
    (ii) adequate screening procedures when hiring employees;
(b) the confirmation of the implementation, and the review, by an independent party of the internal policies, procedures and controls.

Policies refers to high level statements that are uniform across the entire organisation, and are approved by the management. Procedures identifies the acceptable and

workable practices that the organisation adopts that the policies are implemented at the operational level. Controls are the tools used to ensure that the program is operating as intended.

These programmes must include training and a law practice must ensure that its partners, directors and employees are regularly and appropriately trained on (rule 18(5) of the Rules) –

(a) the laws and regulations relating to the prevention of money laundering and the financing of terrorism; and
(b) the law practice's internal policies, procedures and controls for the prevention of money laundering and the financing of terrorism.

The issues which may be covered in the internal policies, procedures and controls include:

(a) the CDD measures to be met for low risk clients;
(b) the enhanced CDD measure to be met for higher risk clients;
(c) the CDD measures to determine if a client is a politically-exposed individual or a family member or close associate of such an individual;
(d) the ongoing CDD measures and enhanced ongoing monitoring (if any) that have to be met;
(e) the conditions to be met for reliance on CDD measures performed by third parties; and
(f) the circumstances in which deferral of the completion of CDD measures is permitted.
(g) whether you should subscribe to a suitable commercial screening service.
(h) the relevant procedure for making STR and Cross Border Cash Movement Reports.
(i) a prohibition against opening or maintaining accounts, or to hold or receive monies from an anonymous source or a client with an obviously fictitious name.

Compliance management arrangements

Compliance management arrangements (referred to in rule 18(3) of the Rules) means carrying out regular review, assessment and updates of the internal policies, procedures and controls to ensure that they are adequate and they manage the money laundering and financing of terrorism risks effectively.

Screening procedures

Employees: The screening of new employees (referred to in rule 18(3) of the Rules) can be done by including relevant questions in the law practice's employment application form, for example, whether the person has been convicted of any offence of dishonesty or fraud, whether the person has been sentenced to a term of imprisonment, and whether the person is an undischarged bankrupt. The employee should also make the requisite declarations when executing the statutory declarations as required by section 78(7) LPA. In Singapore it is not possible to check with the Criminal Records Office whether a person has a criminal record, so it is not necessary to do that.

Clients: As part of your risk assessment you should decide whether you should subscribe to a reliable commercial screening service. Such services will allow you to screen persons against consolidated sanctions lists as well as help you identify potential PEPs or individuals and entities who, for any reason, pose a risk. You should ensure that you choose a screening service that has access to the databases that are relevant to a Singapore practice, in particular, the lists of persons and entities of interest maintained by the MAS and Inter-Ministerial Committee – Terrorist Designation, the

schedules to TSOFA, and the lists maintained pursuant to the United Nations Security Council resolutions. It may also be useful to include the sanction lists maintained by the United States, European Union and the United Kingdom.

Clients, and in the case of legal persons, the beneficial owners and representatives of the clients, should be screened when you are being instructed in a Relevant Matter.

If you have assessed that your risk profile does not warrant such a subscription, then you should at least conduct an internet search. When conducting an internet search, appropriate known identifier information (such as the person's nationality or country of birth) ought to be included to help filter the results to a manageable number.

Whatever the screening method adopted might be, the outcome ought to be printed out or stored electronically for reference.

Such screening is not a substitute for you making necessary inquiries of the client to ensure that you truly know him or her and are able to assess whether they potentially pose a risk. Nor does it relieve you of your obligation to understand the nature of the transaction for which you are being retained.

Confirmation and review by an independent party

The requirement of the confirmation and review by an independent party (referred to in rule 18(3) of the Rules) may be satisfied through (but not limited to):

(a) the appointment of an external auditor to carry out the confirmation and review; or
(b) the appointment of a suitably experienced professional within the same law practice to carry out the confirmation and review.

2.1.4 Training

Training may cover the following areas:

(a) money laundering (including proliferation financing) and financing of terrorism vulnerabilities of a law practice;
(b) the impact that money laundering and financing of terrorism may have on a law practice, its business, clients and employees;
(c) effective ways of determining whether clients are politically-exposed individuals;
(d) client and business relationship risk factors;
(e) the different CDD measures that have to be performed;
(f) how to deal with suspicious activities and transactions;
(g) suspicious transaction reporting; and
(h) the internal policies, procedures and controls that have been put in place to reduce and manage money laundering and financing of terrorism risks.

The training frequency should be sufficient to maintain the knowledge and competence of partners, directors and employees to apply CDD measures appropriately.
Training can take many forms and may include:

(a) attendance at conferences, seminars, or training courses organised by the Law Society or other organisations;
(b) completion of online training sessions;
(c) law practice or practice group meetings for discussion on prevention of money laundering and financing of terrorism issues and risk factors; and
(d) review of publications on current prevention of money laundering and financing of terrorism issues.

The Law Society now offers an online e-learning training for AML.

2.2 Assessing individual risks

You must assess the risks posed by a specific client or retainer. Determining the risks posed by a specific client or retainer will then assist in applying the internal procedures and controls in a proportionate and effective manner.

Part 3 – Customer Due Diligence ('CDD') in Relation to a Client

3.1 CDD in general

CDD refers to due diligence measures performed by a legal practitioner or law practice in relation to a client. The term 'client' and 'customer' are synonymous and interchangeable.

In preparing for or carrying out any transaction concerning a relevant matter, you must perform the CDD measures prescribed in the Rules. CDD is required because you can better identify suspicious transactions if you know your clients and understand the reasoning behind the instructions given by your clients.

Certain CDD measures may be performed by a third party in circumstances set out in rule 17 of the Rules.

You can start working for a client before the CDD is completed. However, you must complete the CDD as soon as is reasonably practicable, and in any event before the transaction for which you are engaged is completed, e.g. before any funds are transferred. If you are unable to complete it, then you must not commence a new business relationship, must terminate any existing business relationship with the client and must not undertake any transaction for the client (see paragraph 3.15).

A business relationship refers to the client relationship.

3.2 Principal components of CDD

The principal components of CDD are:

(a) Identification and verification of the identity of the client.
(b) Identification and verification of the beneficial owners (if the client is an entity or legal arrangement).
(c) Understanding the nature of the client's business, and the ownership and control structure of the client (if the client is an entity or legal arrangement).
(d) Reasonable measures to determine whether the client and beneficial owner (if any) is a politically-exposed individual, or a family member or close associate of any such individual.
(e) Obtaining information on the purpose and intended nature of the business relationship and where applicable, source of funds.
(f) Ongoing CDD.
(g) Enhanced CDD, where required:
    (i) establish the source of wealth and the source of funds;
    (ii) obtain the approval of senior management; and
    (iii) enhanced ongoing monitoring.
(h) Require that the client's first payment be carried out through an account in the customer's name with a bank subject to similar CDD standards.

3.3 Risk-based approach

Singapore has adopted the risk based approach ("RBA") as recommended by FATF, in combatting money laundering and terrorist financing. RBA means that lawyers should

identify, assess and understand the ML/TF risks to which they are exposed, and take the required measures to mitigate and manage the risks. The key elements of RBA are:

- identifying the ML/TF risks facing the practice, given its clients, services, countries of operation, etc.
- identifying and applying measures to effectively and efficiently mitigate and manage the said risks.
- Putting in place policies, procedures and controls.
- Documenting its risk assessments, strategies, policies and procedures.

RBA means that you have the flexibility to calibrate the CDD measures you take in a specific case according to what you assess to be the risks. (rule 12(1) of the Rules). In other words, it is not a case of one size fits all.

In practical terms this means that you must —

(a) perform, in relation to each client, an adequate analysis of the risks of money laundering and the financing of terrorism;
(b) document the analysis and the conclusions reached; and
(c) keep the analysis up to date. (rule 12(2) of the Rules)

For an adequate analysis of the risks of money laundering and the financing of terrorism, you should take the following steps:

(a) Identify and assess the money laundering and the financing of terrorism risks based on the following factors:
    (i) The type of client —
        (A) whether the client is a new client or an existing client;
        (B) whether the client is an individual or entity or legal arrangement;
        (C) whether the client is a politically-exposed individual or close associate or family member of a politically-exposed individual; and
        (D) whether the client is from a country where there is a higher risk of money laundering or financing of terrorism.
    (ii) The business relationship with the client.
(b) Determine if the client is a higher risk client.
(c) Determine if the business relationship is a higher risk business relationship.
(d) Determine if there are reasonable grounds to suspect the client is engaged in money laundering or the financing of terrorism.

There are no universally accepted methodologies that prescribe the nature and extent of a risk based approach. Ultimately, you as a practitioner are in the best position to know the profile of your clients and the kinds of matters that they instruct you on. You are therefore in the best position to determine what steps you should be taking to address any possible risks of money laundering / terrorist financing which may be presented. It is absolutely critical that you document the basis of your risk assessment. This will come in useful if you are ever subject to an audit.

3.4 Lower risks

The risks of money laundering and the financing of terrorism are lowered if the client is any of the following (rule 12(3) of the Rules):

(a) a Ministry or department of the Government, an organ of State or a statutory board;
(b) a ministry or department of the government of a foreign country or territory;
(c) an entity listed on a securities exchange as defined in section 2(1) of the Securities and Futures Act (Cap 289), or a subsidiary of such an entity more than 50% of the shares or other equity interests of which are owned by the entity;
(d) an entity listed on a stock exchange outside Singapore that is subject to regulatory disclosure requirements;

(e) a relevant Singapore financial institution;
(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF;
(g) an investment vehicle every manager of which is a financial institution referred to in sub-paragraph (e) or (f);
(h) any of the following universities in Singapore:
    (i) Nanyang Technological University;
    (ii) National University of Singapore;
    (iii) Singapore Institute of Technology;
    (iv) Singapore Management University;
    (v) Singapore University of Technology and Design;
(i) a Government school as defined in section 2 of the Education Act (Cap 87);
(j) the Society;
(k) an entity that is made up of regulated professionals who are subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF.

There may be other cases where the risks might be considered lower. If so, you must ensure that this is properly documented.

3.5 High risk factors

Examples of high risk factors for ML/ FT may include but are not limited to the following:

(a) Type of client (Client risk factors)
    (i) Non-resident client and client who has no address or multiple addresses.
    (ii) Client or beneficial owner who is a politically-exposed individual or a family member or close associate of any such individual (see paragraph 3.14).
    (iii) Legal persons or arrangements that are personal asset holding vehicles.
    (iv) Companies with nominee shareholders or bearer shares.
    (v) Businesses that are cash-intensive.
    (vi) Client with criminal convictions involving fraud or dishonesty.
    (vii) Client shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory client identification.
    (viii) Client who asks for short-cuts and unexplained speed in completing the transaction.
    (ix) Client is overly secretive or evasive (for example, of who the beneficial owner is, or the source of funds).
    (x) Client is actively avoiding personal contact without good reason.
    (xi) Client is willing to pay fees without requirement for legal work to be undertaken (other than deposits as requested by you in advance of the work to be undertaken).

(b) Type of client (Country/territory risk factors)
    (i) Client is from or in any country or jurisdiction in relation to which the FATF has called for countermeasures or enhanced client due diligence measures (see paragraph 3.14).
    (ii) Client is from or in any country or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism (see paragraph 3.14).

(c) The business relationship with the client
    (i) Instructions to a legal practitioner or law practice at a distance from the client or transaction without legitimate or economic reason.

(ii) Instructions to a legal practitioner or law practice without experience in a particular specialty or without experience in providing services in complicated or especially large transactions.
(iii) Use of client account without underlying legal services provided.
(iv) Payments are made by the client in actual cash (in the form of notes and coins).
(v) The transaction relates to, any country or jurisdiction in relation to which the FATF has called for countermeasures or enhanced client due diligence measures (see paragraph 3.14).
(vi) Disproportionate amount of private funding for the purchase of real estate/property which is inconsistent with the socio-economic profile of the client.
(vii) Large cash payments made for purchase of interest in land whose value is far less, or the method of funding is unusual such as funding from a third party who is not a relative or known to the buyer, or there is an absence of any logical explanation from the parties why the property is owned by multiple owners or by nominee companies.
(viii) Unusually high levels of assets or unusually large transactions in relation to what might reasonably be expected of clients with a similar profile.
(ix) Transfer of real estate between parties in an unusually short time period.
(x) Requests by the client for payments to third parties without substantiating reason or corresponding transaction.
(xi) Instructions by the client for the creation of complicated ownership structures where there is no legitimate or economic reason.
(xii) Disputes which are settled too easily, with little involvement by the legal practitioner or law practice (may indicate sham litigation).
(xiii) Abandoned transactions with no concern for the fee level.
(xiv) Loss making transactions where the loss is avoidable.
(xv) An absence of documentation to support the client's story, previous transactions or company activities.
(xvi) Unexplained use of express trusts.
(xvii) Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices.
(xviii) In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
(xix) In the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and classes within an expression of wishes.

3.5A High Risk Factors for Proliferation Financing

Indicators of possible proliferation financing include:

(i) Transaction involves person or entity in foreign country of proliferation concern.
(ii) Transaction involves person or entity in foreign country of diversion concern.
(iii) The client or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" for the purposes of export control regimes.3
(iv) Client activity does not match business profile, or end-user information does not match end-user's business profile.
(v) A freight forwarding firm is listed as the product's final destination.

[3] Example of denied person list is the one maintained by the Bureau of Industry and Security, US Department of Commerce, available here.

(vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.

(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).

(viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).

(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.

(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.

(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.

(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

(xii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).

(xiv) Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.

(xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.

(xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.

(xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

(xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.

(xix) New customer requests letter of credit transaction awaiting approval of new account.

(xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

(xxi) Involvement of items controlled under WMD export control regimes or national control regimes.

(xxii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.

(xxiii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.

(xxiv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.

(xxv) Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.

(xxvi) Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.

(xxvii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).

(xxviii) Involvement of a university in a country of proliferation concern.

(xxix) Description of goods on trade or financial documentation is non-specific, innocuous or misleading.

(xxx) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.

(xxxi) Use of personal account to purchase industrial items.

The mere presence of risk factors is not necessarily a basis for suspecting money laundering or the financing of terrorism, as a client may be able to provide a legitimate explanation. Risk factors should assist you in applying a risk-based approach to your CDD requirements of knowing who your client and the beneficial owners are, understanding the nature and the purpose of the business relationship between you and the client, and understanding the source of wealth and the source of funds of the client.

If a client is unable to provide an adequate, satisfactory and credible explanation in response to an enquiry, that inability by itself does not necessarily constitute a sufficient basis to impute criminal activity on the part of the client. It simply means that further enquiry is required, and where responses are not credible, or your suspicions are not adequately allayed by the responses, you should not accept any further instructions from the client, and you must terminate the existing business relationship and consider whether to file a suspicious transaction report.

3.5B Specific situations

(a) You must not open or maintain any account for or hold and receive money from an anonymous source, or a client with an obviously fictitious name (Section 70B Part VA).

(b) If there are reasonable grounds to suspect that a client may be engaged in money laundering or the financing of terrorism, you must not establish any new business relationship with, or undertake any new matter for, the client; and must file a suspicious transaction report (rule 5 of the Rules).

(c) The creation, operation or management of a company includes:

a. Acting or arranging for another person to act as a director, secretary of a corporation or its equivalent in other legal entities;
b. Acting or arranging for another person to act as a partner in a partnership or its equivalent in other entities;
c. Providing a registered office, business or correspondence address, or other related services for a corporation, partnership or other legal entity; and/or
d. Acting or arranging for another person to act as a shareholder on behalf of any corporation other than a corporation whose securities are listed on a securities exchange or recognised securities exchange within the meaning of the Securities and Futures Act.

(d) You should be cautious when receiving unusual amounts of cash from your client. In particular, bear in mind the obligation under s60 of the CDSA which requires you to report receipt of cash exceeding the value of S$20,000.00 which originates from outside Singapore.

(e) Be careful of arrangements where you end up as no more than a financial conduit, receiving money from one source and routing it to another. An illustration of this can be found in the facts of Re Chan Chun Hwee Allan [2018] SGHC 21. The practitioner was introduced to an Australian who requested that the practitioner act for 2 companies. In particular, he was to receive monies on behalf of the companies and transmit them onwards as instructed. The practitioner was given vague descriptions of the nature of the payments, which he subsequently accepted without any critical examination. For this very simple work he was allowed to keep 5% of the monies received. The practitioner's bank queried why he was transmitting funds when his client could just as easily transfer the monies themselves. He was unable to provide an explanation. He was ultimately charged and convicted for failing to do CDD on his client.

Persons who are not able to open bank accounts or execute transactions (e.g. they are subject to targeted financial sanctions) may resort to instructing lawyers to assist them in receiving and transmitting funds, taking advantage of the anonymity afforded to them by using the account in the name of the law practice.

3.6 Basic CDD

You must perform the following CDD measures:

3.6.1 Identification and verification of the identity of the client

If the client is an individual

If your client is an individual, you must first ascertain the identity of the client. You must also verify your client's identity using objectively reliable and independent source documents, data or information (rules 6(1)(*a*) and 6(1)(*b*) of the Rules).

You are encouraged to use a wide range of sources when verifying the identity of the client including 'google searches', conversations with the client and reliable individuals, and, in appropriate cases checks with reliable commercial screening services. With internet searches, it is important to apply appropriate search parameters so as to generate results that are manageable to review.

To ascertain the identity of a client, you must at least obtain and record the following information:

(a) full name, including any alias;
(b) date of birth;
(c) nationality; and
(d) residential address.

If it is necessary you should also obtain information on the client's occupation and address of the employer; or if self-employed, the name and place of the client's business. Similarly, if required, you should understand the source of funds and source of wealth of the client.

You must verify the client's identity using objectively reliable and independent source documents, data or information to ensure that the information obtained and recorded is authentic. Examples of objectively reliable and independent source documents include the following original documents:

(a) identity cards;
(b) passports;
(c) driving licences;
(d) work permits; and

(e) other appropriate photo identification.

It is permissible to rely on the digital ID accessible via Singpass biometric verification provided the verification is witnessed by you.

Please note that law practices are permitted to collect personal data for the purposes of providing legal services (Personal Data Protection Act). If your client is unable to produce original documents, and there is a reasonable explanation for not doing so, you may consider accepting copies. In face to face engagements there should be very few cases when the client is unable to provide original identification documents. If appropriate, you may require that these documents be certified as true copies by other professionals (for example, lawyers or notaries), but this is not necessary if it is a straightforward matter and the risks of ML\FT and misidentification of the client are low.

If you are unable to meet the client face to face, you may rely on a copy of the identity document(s). If appropriate, you may require that these documents be certified as true copies by other professionals (for example, lawyers or notaries), but this is not necessary if it is a straightforward matter and the risks of ML\FT and misidentification of the client are low. You may consider alternative measures such as getting the client to allow you to inspect his original identity document over a video call. You should look out for obvious forgeries, but you are not required to be an expert in forged documents. In this respect you may wish to refer to the guidance and facility available on the ICA website for verifying that Singapore NRIC are genuine. Ministry of Manpower also has guidance and a facility to verify Singapore Work Passes. The Law Society has provided guidance on this in the e-blast of 23 June 2023.

You should understand the exact nature of the work that you are being engaged to perform and understand how such engagement could facilitate the movement or obscure the provenance of the proceeds of crime. Where you do not have the requisite expertise to understand the engagement, you should not undertake the work. You need to be reasonably satisfied that there is a commercial or personal rationale for the work to be done. Do not accept vague answers such as "for business purposes".

If the client is an entity or legal arrangement

If your client is an entity or legal arrangement, you must ascertain the identity the client, and verify the client's identity, respectively, through the following information (rule 6(2) of the Rules) –

(a) the name of the client;
(b) the legal form of the client;
(c) the documents that prove the existence of the client;
(d) the documents that regulate and bind the client;
(e) the individuals in the senior management of the client;
(f) the address of the registered office of the client; and
(g) the address of the principal place of business of the client, if the registered office of the client is not a principal place of business of the client.

You must obtain and record the following information –

(a) full name;
(b) incorporation number or registration number;
(c) address of place of business or registered office address and telephone number;
(d) the date of incorporation or registration; and
(e) the place of incorporation or registration.

(A) Singapore sole proprietorship, partnership, limited partnership, limited liability partnership, or a company

If your client is a Singapore sole proprietorship, partnership, limited partnership, limited liability partnership, or a company, a profile of the entity obtained from the Accounting and Corporate Regulatory Authority's ('ACRA') database is generally sufficient to establish the existence of the client and that it is incorporated/registered in Singapore, the name and legal form of the client, the identities of its directors/partners (including individuals in the senior management), the address of the registered office and the address of the principal place of business.

You should obtain from your client the documents that regulate and bind the client (such as the constitution, or the memorandum and articles of association, of a company, if the client is a company, or the trust deed of an express trust, if the client is an express trust).

(B) Foreign entity

For an overseas sole proprietorship, partnership, limited partnership, limited liability partnership, or a company, the same particulars as required for a Singapore entity must be obtained. If the necessary documents cannot be obtained from a body in a foreign country equivalent to ACRA, the entity's identity could be verified independently by a person/body responsible in that foreign country for the regulation of companies or by another professional or by other reasonable means.

(As a guide, a non-exhaustive list of foreign regulators of companies can be found at the following link – http://www.ecrforum.org/worldwide-registers/)

If you are satisfied that there is little or no risk of money laundering or terrorist financing or such risk is low and you have no suspicions of the same, you may obtain information on the identity of the client from (i) a structure chart (of the entity) provided by the client directly or (ii) information available on the client's website or (iii) information available from the client's annual reports or (iv) information from any publicly known source that is reliable.

(C) Trusts

Before acting for a trust, you must, ascertain the identity and particulars of each trustee, relevant party, effective controllers, and service suppliers (trustees must be identified in accordance with their categorisation, natural person or company etc) and the nature of the trust.

(For legal practitioners who act as trustees, please refer to paragraph 3.11.)

(D) Attorneys

If you are acting for an attorney, you must identify both the principal and the attorney.

You must cease or refuse to act for a client who gives a power of attorney in favour of any person without any apparent reason, and refuses to explain why a power of attorney is given and/or is reluctant to provide the identity documents of the attorney or principal.

(E) Singapore charities, clubs and societies

If you are acting for a charity or a society, you must check that the registration number for the charity or society or club is correct. For charities, you should check with the Commissioner for Charity and for societies, the Registrar of Societies.

You must obtain the names of all trustees and officers of the charity, club or society before accepting the retainer.

(F) Foreign charities, clubs and societies

For an overseas charity, club and society, the same particulars as required for a Singapore charity, club and society must be obtained. If the necessary information cannot be obtained from a body in a foreign country equivalent to the Commissioner for Charity or the Registrar of Societies, the entity's identity could be verified independently by a person/body responsible in that foreign country for the regulation of charities, clubs and societies or by another professional or by other reasonable means.

(G) Singapore co-operatives

If you are instructed to act for a co-operative society, you must check the registration particulars of the co-operative or check the same with the Registrar of Co-operative Societies. You must obtain the names of the members of the committee of management and officers of the co-operative before accepting the retainer.

(H) Management corporations

If you are acting for a management corporation ('MCST'), you must obtain the names of all officers of the Management Council of the MCST before accepting the retainer.

(I) Estates

If you are instructed to act for an estate, you must have sight of the death certificate and if applicable, the original will or a certified true copy of the will of the deceased. You must also obtain the relevant identity documents to establish the identities of the executors or administrators of the deceased estate and where applicable, the original or certified true copy of the letters of administration or probate.

3.6.2 Identification and verification of the beneficial owners (if the client is an entity or legal arrangement)

If the client is an entity or legal arrangement, you must (rule 8 of the Rules):

(a) ascertain whether the client has any beneficial owner;
(b) ascertain the identity of each beneficial owner (if any);
(c) take reasonable measures to verify the identity of each beneficial owner (if any) using objectively reliable and independent source documents, data or information;
(d) understand the nature of the client's business;
(e) understand the ownership and control structure of the client;

Beneficial owner

The client due diligence measures you must perform under paragraphs 3.6.2(b) and 3.6.2(c) above include identifying, and taking reasonable measures to verify the identity of, each beneficial owner of the client, through the following information:

(i) the identity of each individual (if any) who has a controlling ownership interest in the client;

(ii) if there is any doubt as to whether an individual who has a controlling ownership interest in the client is a beneficial owner of the client, or if there is no individual who has a controlling ownership interest in the client, the identity of each individual (if any) who has control of the client through other means;

(iii) if there is no individual who has a controlling ownership interest in the client or who has control of the client through other means, the identity of each individual in the senior management of the client.

What constitutes a controlling ownership interest is a question of fact in each case but in any case, you should treat direct or indirect control of more than 25% of the shares or voting rights of the client as a controlling interest.

If there is any doubt as to whether an individual who has a controlling ownership interest in the client is a beneficial owner of the client, or if there is no individual who has a controlling ownership interest in the client, you must ascertain and take reasonable measures to verify the identity of each individual (if any) who has control of the client through other means.

If there is no individual who has a controlling ownership interest in the client or who has control of the client through other means, you must ascertain and take reasonable measures to verify the identity of each individual in the senior management of the client, such as a chief executive officer, chief financial officer, managing or executive director, or president.

If the client is a legal arrangement, the client due diligence measures that you must perform under paragraphs 3.6.2(b) and 3.6.2(c) above include identifying, and taking reasonable measures to verify the identity of, each beneficial owner of the client, through the following information:

(a) if the client is an express trust, the identities of the settlor, each trustee, the protector (if any) and each beneficiary or class of beneficiaries of the trust, and any other individual exercising effective control over the client (including through a chain of control or ownership);

(b) if the client is any other legal arrangement, the identity of each person in an equivalent or a similar position to a settlor, trustee, protector or beneficiary of a trust, or any other individual exercising effective control over the client (including through a chain of control or ownership).

Reasonable measures to verify identity of beneficial owner

Ascertaining and verifying the beneficial owners of a legal person is often a very difficult exercise as this information is rarely publicly available in a reliable form. You are only obliged to take reasonable measures, which will depend on the risk assessment that you make. You may rely on information provided by the client (for example, a declaration by the client about its beneficial owner(s)), or information that is publicly known.

Other reasonable measures may include the following:

(a) using objectively reliable and independent source information or documents such as the business profile obtained from ACRA, or from a body in a foreign country equivalent to ACRA;

(b) using information, documents or data provided by the client, and arranging a face-to-face meeting with the beneficial owner (where necessary) to corroborate the information given by the client; or
(c) researching publicly available information on the beneficial owner.

Although Singapore companies are required to maintain registries of controllers and nominee directors and shareholders, they are not to be disclosed to members of the public but can be disclosed to a public agency enforcing any law. In all likelihood this means that they should not be disclosed to lawyers for the purposes of CDD.

(A) Company, foreign company, limited liability partnership

The beneficial owner of a company, foreign company and limited liability partnership, is any individual who:

(a) ultimately owns or controls (whether through direct or indirect ownership or control) more than 25% of the shares or voting rights of the client; or
(b) otherwise exercises effective control over the management of the client.

(B) Partnership

The beneficial owner of a partnership, is any individual who:

(a) is ultimately entitled to or controls (whether the entitlement or control is direct or indirect) more than 25% of the share of the capital or profits or more than 25% of the voting rights of the partnership; or
(b) otherwise exercises effective control over the management of the partnership.

(C) Trust

The beneficial owner:

(a) of a trust includes any individual who is entitled to a vested interest in at least 25% of the capital of the trust property. 'Vested interest' is defined as an interest that a person is currently entitled to, without any pre-conditions needing to be fulfilled;
(b) of a trust includes any individual who has control over the trust. 'Control' is defined as a power whether exercisable alone, jointly with another person or with the consent of another person under the trust instrument or by law: to dispose of, advance, lend, invest, pay or apply trust property; vary the trust; add or remove a person as a beneficiary to or from a class of beneficiaries; appoint or remove trustees; or direct, withhold consent to or veto the exercise of any of the above powers; or
(c) of a trust other than one which is set up or which operates entirely for the benefit of individuals entitled to a vested interest in at least 25% of the capital of the trust property, includes the class of persons in whose main interest the trust is set up or operates, and the class must be described.

(D) Other legal arrangements

The beneficial owners of other legal arrangements are:

(a) where the individuals who benefit from the legal arrangement have been determined, any individual who benefits from at least 25% of the property of the legal arrangement;

(b) where the individuals who benefit from the legal arrangement have yet to be determined, the class of persons in whose main interests the legal arrangement is set up or operates; or
(c) an individual who controls at least 25% of the property of the legal arrangement.

Understanding the nature of business, ownership and control
To understand the nature of the client's business, and to understand the ownership and control structure of the client, you may rely on the following:
(a) Information provided by the client.
(b) Information available on the client's website.
(c) Information available from the client's annual reports.
(d) Information from any publicly known source that is reliable.

To better understand the ownership and control structure, it would be prudent to monitor changes (if any) in instructions, or transactions which suggest that someone is trying to undertake or manipulate a retainer for criminal ends.

3.6.3 Reasonable measures to determine whether a client and beneficial owner is a politically exposed individual, or a family member or close associate of any such individual

You must take reasonable measures to determine if the client is a politically exposed individual, or a family member or close associate of any such individual (rule 6(1)(*c*) of the Rules).

If the client is an entity or legal arrangement, you must take reasonable measures to determine whether each beneficial owner (if any) is a politically-exposed individual, or a family member or close associate of any such individual (rule 8(1)(*d*) of the Rules).

A close associate in relation to a politically exposed individual is an individual who is known to you or is publicly known to be, closely connected to the politically-exposed individual, either socially or professionally. Based on the FATF Guidance dated June 2013 on "Politically Exposed Persons (Recommendations 12 and 22)", this includes partners outside the family unit (for example, girlfriends, boyfriends, mistresses); business partners or associates.

The reasonable measures referred to in rules 6(1)(*c*) and 8(1)(*d*) of the Rules include putting in place risk management systems to determine whether a client or beneficial owner is a politically-exposed individual or a family member or close associate of such an individual. Such reasonable measures may take into consideration the following:
(a) You are not required to conduct extensive investigations to establish whether a client is a politically exposed individual or a family member or close associate of any such individual. Just have regard to information that is in your possession or publicly known. With regard to information that is in your possession, this may be information provided to you by the client.
(b) If you have reason to suspect that a client is a politically exposed individual or a family member or close associate of any such individual, you should conduct some form of electronic verification. An Internet based search engine (including social media) may be sufficient for these purposes. If warranted, you can screen the individuals with a reliable commercial screening service.

A foreign politically exposed individual and a domestic politically-exposed individual are defined in the Rules to mean an individual who is or has been entrusted with a prominent public function. According to FATF, the handling of a client who is no longer

entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. Possible risk factors are:

(a) the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a politically exposed individual; or

(b) whether the individual's previous and current function are linked in any way (for example, formally by appointment of the politically-exposed individual's successor, or informally by the fact that the politically-exposed individual continues to deal with the same substantive matters).

If the client is:

(a) a foreign politically-exposed individual or a family member or close associate of any such individual; or

(b) a domestic politically-exposed individual/individual entrusted with a prominent function in an international organisation or a family member or close associate of any such individual (and where there is a higher risk business relationship);

you can still act on behalf of the client, but you should undertake enhanced due diligence and monitor the client (see paragraph 3.14).

3.6.4 Obtaining information on the purpose and intended nature of the business relationship

You must identify and if appropriate, obtain information on the purpose and intended nature of the business relationship with the client (rule 9 of the Rules).

For the purposes of rule 9 of the Rules, you must identity and if appropriate, obtain information concerning the retainer, and transaction and/or advice that you are proposing to act for the client on.

As part of the scrutiny of the business relationship, you must satisfy yourself as to the source of funds for the transaction. The source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship with the client. It is not enough to know that the money is transferred from a particular bank account. Possible sources of funds include a PEP's current income, wealth, savings, or funds obtained from his current and previous positions, business undertakings, and family assets. You should establish whether the answers as to the source of funds are consistent with the quantum involved.

3.7 Situations where specific CDD measures are not required

CDD measures in relation to client

You need not ascertain and verify the identity of the client through the information listed at rule 6(2) of the Rules if the client is a Ministry or department of the Singapore Government, an organ of the Singapore State or a statutory board in Singapore; or a ministry or department of the government of a foreign country or territory (rule 6(3) of the Rules) unless you suspect that the client may be engaged in, or the business relationship with the client or the matter undertaken for the client may involve engagement in, money laundering or the financing of terrorism.

CDD measures in relation to entity or legal arrangement

You need not perform the CDD measures referred to in paragraphs (1), (2) and (3) of Rule 8 of the Rules if the client is (rule 8(4) of the Rules) –

(a) a Ministry or department of the Government, an organ of State or a statutory board;

(b) a ministry or department of the government of a foreign country or territory;

(c) an entity listed on the Singapore Exchange (Mainboard or Catalist) or a subsidiary of such an entity;
(d) an entity listed on a stock exchange outside Singapore that is subject to regulatory disclosure requirements;
(e) a relevant Singapore financial institution;
(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF;
(g) an investment vehicle every manager of which is a financial institution referred to in sub-paragraph (e) or (f);
(h) any of the following universities in Singapore:
    (i) Nanyang Technological University;
    (ii) National University of Singapore;
    (iii) Singapore Institute of Technology;
    (iv) Singapore Management University;
    (v) Singapore University of Technology and Design;
(i) a Government school as defined in section 2 of the Education Act (Cap 87);
(j) the Society; or
(k) an entity that is made up of regulated professionals who are subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF,

unless you suspect that the client may be engaged in, or the business relationship with the client or matter undertaken for the client may involve engagement in. money laundering or the financing of terrorism.

For entities listed on foreign stock exchanges (sub para (d) above), you will have to determine whether the exchange in question imposes disclosure requirements ensuring adequate transparency comparable to Singapore. In determining this, your practice will have to make its own assessment considering *inter alia* country risk, and the overall compliance with FATF requirements from published materials.

3.8 Existing clients

You need not repeatedly identify and verify the identity of a client or beneficial owner. You may rely on the identification and verification measures that have already been performed unless you have doubts about the veracity of the information obtained.

If it is an existing client, you must perform the CDD measures based on your assessment of the materiality and risks of money laundering and the financing of terrorism, taking into account –

(a) any previous CDD measures performed in relation to the client;
(b) the time when any CDD measures were last performed in relation to the client; and
(c) the adequacy of the data, documents or information obtained from any previous CDD measures performed in relation to the client (rule 14(1) of the Rules).

Generally, you may waive the full client identity checks if the client is an existing client who has been in contact with the law practice within the last five years.

You may consider waiving the full client identity checks for the following categories of existing clients who have been in contact with the law practice within the last five years and who provided some formal identification on first contact.

For category (a) clients, you may waive ascertaining the identity and verifying identity of the client provided that there are no suspicions of money laundering and financing of terrorism, and you are satisfied that the original identification documents were adequate. A note confirming this must be signed by the proprietor or partner or director of the law practice and attached to the file.

For category (b) clients, you may waive ascertaining the identity and verifying identity of the client provided that there are no suspicions of money laundering and financing of terrorism, and you are satisfied that you know the client. A note confirming this must be signed by the proprietor or partner or director of the law practice and attached to the file. The note should include details of the length of time you have known the client and the nature of the referral to the law practice (for example, through a friend, business acquaintance or client).

3.9 Instructions from individual purporting to act on behalf of a client

If you receive instructions from an individual purporting to act on behalf of a client, you must perform the following CDD measures in relation to that individual (rule 7 of the Rules):

(a) verify whether the individual is authorised to act on behalf of the client; and
(b) ascertain and verify the identity of the individual.

To verify whether the individual is authorised, you may:

(a) confirm this with the client; and
(b) rely on any documents or information provided by that individual or the client.

To ascertain and verify the identity of the individual, you should consider the extent and nature of the documents (if any) or information required to ascertain and verify the identity of the individual. You may:

(a) obtain his/her business card;
(b) refer to his/her email address or email signature; and
(c) refer to the website of the client (if the client is an entity) for a profile of the individual.

If your client is an entity and you receive instructions from an individual, you need not perform the CDD measures in rule 7 of the Rules if you know the individual to be a member of the senior management or in-house counsel of the entity.

3.10 Performance of CDD measures by third parties

You may rely on a third party such as another law practice or bank (that is appropriately qualified – see below) to perform the CDD measures (apart from ongoing CDD on the business relationship with the client during the course of the business relationship) (rule 17 of the Rules). However, you remain ultimately responsible for the performance of those measures.

If you rely on a third party to perform any CDD measures, you must obtain from the third party all information required as part of those CDD measures.

Before you rely on a third party to perform any CDD measures, you must be satisfied that —

(a) where necessary, you will be able to obtain from the third party, upon request and without delay, all source documents, data or information required to verify the information required as part of the CDD measures; and
(b) the third party —
    (i) is subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with the standards set by the FATF; and
    (ii) has measures in place for compliance with those requirements.

With regard to paragraph 3.10(b) above, you may refer to any publicly available reports or material on the quality of the prevention of money laundering and the financing of terrorism supervision in the jurisdiction where the third party operates and any publicly available reports or material on the quality of that third party's compliance with those requirements.

3.11 CDD measures for legal practitioners who act as trustees

If a legal practitioner acts as a trustee of an express trust:

(i) Governed by Singapore law;

(ii) That is administered in Singapore, namely where the control and management of the trust is exercised in Singapore; or

(iii) In respect of which any of its trustees is resident in Singapore, namely, a trustee who is an individual ordinarily resident in Singapore or a trustee which is incorporated, formed or established in Singapore.

You are subject to these CDD obligations in the Trustees Act and Trustees Act Regulations.

3.11.1 Identification and verification of the relevant parties

If the relevant party is an individual:
You must take reasonable steps to ensure that the following information is obtained from the relevant parties.

(a) Full name, including any aliases;

(b) Identity card number, birth certificate number, passport number, or other similar unique identification number issued by a government authority;

(c) Residential address;

(d) Date of birth; and

(e) Nationality.

You must also take reasonable steps to verify the relevant party's identity using objectively reliable and independent source documents, data or information to ensure that the information obtained and recorded is authentic. Examples of objectively reliable and independent source documents include the following original documents:

(a) identity cards;

(b) passports;

(c) birth certificates;

(d) driving licences; and

(e) work permits.

If the relevant party is unable to produce original documents for a good reason, you may consider accepting documents that are certified to be true copies by other professionals (for example lawyers or notaries). If you are unable to meet the relevant party face to face, you may rely on a certified true copy of the identity document(s). You should take appropriate precautions to ensure that the relevant party's identity document(s) are adequately and independently certified. You should look out for obvious forgeries, but you are not required to be an expert in forged documents.

If the relevant party is an entity or legal arrangement:
If the relevant party is an entity or legal arrangement, you must take reasonable steps to ensure that the following information is obtained from the relevant parties: -

(a) Full name;

(b) Incorporation number or business registration number;

(c) Registered or business address;

(d) Its principal place of business (if different from the registered address);

(e) The date of constitution, incorporation or registration;

(f) The place of incorporation or registration; and
(g) The following information about every connected individual of the entity:
    (i) His or her full name, including any aliases;
    (ii) His or her identity card number, birth certificate number, passport number, or other similar unique identification number issued by a government authority.

You must also take reasonable steps to verify the relevant party's identity using objectively reliable and independent source documents, data or information to ensure that the information obtained and recorded is authentic. Examples of objectively reliable and independent source documents include the following original documents:
(a) The documents that prove the existence of the relevant party;
(b) The documents that regulate and bind the relevant party;
(c) The individuals in the senior management of the relevant party;
(d) The address of the registered office of the relevant party; and
(e) The address of the principal place of business of the relevant party, if the registered office of the client is not a principal place of business of the relevant party.

3.11.2 Identification and verification of effective controllers of relevant parties

If the effective controller is an individual:
You must take reasonable steps to ensure that the following information is obtained from the effective controllers of relevant parties: -
(a) Full name, including any aliases;
(b) Identity card number, birth certificate number, passport number, or other similar unique identification number issued by a government authority;
(c) Residential address;
(d) Date of birth; and
(e) Nationality

You must also take reasonable steps to verify the effective controller's identity using objectively reliable and independent source documents, data or information to ensure that the information obtained and recorded is authentic. Examples of objectively reliable and independent source documents include the following original documents:
(a) identity cards;
(b) passports;
(c) birth certificates;
(d) driving licences; and
(e) work permits.

If the effective controller is unable to produce original documents for good reason, you may consider accepting documents that are certified to be true copies by other professionals (for example lawyers or notaries). If you are unable to meet the effective controller face to face, you may rely on a certified true copy of the identity document(s). You should take appropriate precautions to ensure that the effective controller's identity document(s) are adequately and independently certified. You should look out for obvious forgeries, but you are not required to be experts in forged documents.

3.11.3 Identity of service suppliers

You must take reasonable steps to ensure that the following information is obtained from each person who is appointed or engaged as a service supplier to the relevant trust: -

(a) The name of the service supplier;
(b) The registered or business address of the service supplier;
(c) The contact details of the service supplier; and
(d) Where the service supplier is an entity, the name of the individual who is authorised to act for the service supplier.

3.11.4 Obligation to disclose to specified persons that trustees are acting for relevant trusts

When entering into a business relationship with a specified person, or enters a prescribed transaction with a specified person after 30 April 2017, you must take reasonable steps to inform the specified person at or before the business relationship is formed that you are acting for the relevant trust. This includes dealings with both local and foreign lawyers.

3.11.5 Obligation to keep accounting records

You must take reasonable steps to ensure that there are kept in respect of the relevant trust, accounting records including the following:

(a) Details of all sums of money received and expended by the relevant trust, and the matters in respect of which the receipt and expenditure takes place;
(b) Details of all sales, purchases and other transactions by the relevant trust;
(c) Details of the assets and liabilities of the relevant trust;
(d) Underlying documents (including but not limited to invoices and contracts); and
(e) Such notes as may be necessary to give a reasonable understanding of the details.

These details and documents must meet the following requirements:

(a) In the case of a trust that is a relevant trust on 30 April 2017 —
    (i) correctly explain all the transactions entered into by the relevant trust after 30 April 2017;
    (ii) enable the financial position of the relevant trust after 30 April 2017 to be determined with reasonable accuracy; and
    (iii) enable financial statements of the relevant trust in respect of any period after 30 April 2017 to be prepared;

In the case of a relevant trust created after 30 April 2017 —

(a) correctly explain all the transactions entered into by the relevant trust on or after it is created;
(b) enable the financial position of the relevant trust on or after it is created to be determined with reasonable accuracy; and
(c) enable financial statements of the relevant trust in respect of any period on or after it is created to be prepared; and

In the case of a trust that is not a relevant trust on 30 April 2017 but which becomes a relevant trust after 30 April 2017 —

(a) correctly explain all the transactions entered into by the relevant trust more than 30 days after it becomes a relevant trust;

(b) enable the financial position of the relevant trust more than 30 days after it becomes a relevant trust to be determined with reasonable accuracy; and
(c) enable financial statements of the relevant trust in respect of any period more than 30 days after it becomes a relevant trust to be prepared.

3.11.6 Timing of CDD measures for obtaining and verifying basic information about relevant trust parties, effective controllers and service suppliers

For the purposes of obtaining and verifying basic information about relevant trust parties, effective controllers and service suppliers, the reasonable steps must be taken within the time specified:

In the case of a trust that is a relevant trust on 30 April 2017 -
(a) On or before 30 May 2017; or
(b) In respect of any of the following relevant parties, effective controllers or service suppliers that are not known to the trustee on or before 30 May 2017 - as soon as reasonably practicable after the relevant parties, effective controllers and service suppliers are known to the trustee:
    (i) A beneficiary;
    (ii) A protector; and/or
    (iii) A person who has any power over the disposition of any property that is subject to the relevant trust;

In the case of a relevant trust created after 30 April 2017 -
(a) In respect of any of the following relevant parties, effective controllers or service suppliers - before the trustee exercises or performs any function, duty or power in respect of the relevant trust:
    (i) A settlor; and/or
    (ii) Another trustee; or
(b) In respect of any of the following relevant parties, effective controllers or service suppliers - as soon as reasonably practicable after the relevant parties, effective controllers or service suppliers is known to the trustee:
    (i) A beneficiary;
    (ii) A protector; and/or
    (iii) A person who has any power over the disposition of any property that is subject to the relevant trust; and

In the case of a trust that is not a relevant trust on 30 April 2017 but which becomes a relevant trust after 30 April 2017 -
(a) Within 60 days after the date on which the trust becomes a relevant trust; or
(b) In respect of any of the following relevant parties, effective controllers or service suppliers that is not known to the trustee within the time specified in sub-paragraph (a) - as soon as reasonably practicable after the relevant parties, effective controllers or service suppliers are known to the trustee:
    (i) A beneficiary;
    (ii) A protector; and/or
    (iii) A person who has any power over the disposition of any property that is subject to the relevant trust.

3.11.7 Obligation to maintain and update obtained information

As an additional safeguard, you are expected to: -
(a) Obtain and maintain adequate, accurate and current information on the identities of the settlor, each trustee, the protector (if any) and each beneficiary or class of beneficiaries of the trust, relevant parties and effective controllers;

(b) Obtain and maintain basic information on every other service supplier;
(c) Maintain the above information for at least 5 years after the legal practitioner's involvement with the trust ceases; and
(d) Ensure that the information is kept accurate and as up-to-date as possible, and is updated on a timely basis.

3.12 Timing of CDD

The following CDD measures must be performed before the start, or during the course of establishing a business relationship with the client:

(a) ascertaining the identity of the client (rule 6(1)(*a*) of the Rules);
(b) where the client is an entity or legal arrangement, ascertaining the client's identity through specific information (rule 6(2) of the Rules); and
(c) ascertaining whether the client has any beneficial owner (rule 8(1)(*a*) of the Rules).

The following CDD measures need not be completed before the start, or during the course, of establishing a business relationship with the client provided that a deferral of the completion of the measures is necessary in order not to interrupt the normal conduct of business operations and the risks of money laundering and the financing of terrorism can be effectively managed (rule 11(2) of the Rules):

(a) Verifying the client's identity using objectively reliable and independent source documents, data or information (rule 6(1)(*b*) of the Rules).
(b) Where the client is an entity or legal arrangement, verifying the client's identity through specific information (rule 6(2) of the Rules).
(c) Taking reasonable measures to determine whether the client is a politically – exposed individual, or a family member or close associate of any such individual (rule 6(1)(*c*) of the Rules).
(d) Verifying whether an individual purporting to act on behalf of a client is authorised, and ascertaining and verifying the identity of the individual (rule 7 of the Rules).
(e) Ascertaining the identity of each beneficial owner (if any) (rule 8(1)(*b*) of the Rules).
(f) Taking reasonable measures to verify the identity of each beneficial owner (if any) using objectively reliable and independent source documents, data or information (rule 8(1)(*c*) of the Rules).
(g) Taking reasonable measures to determine whether each beneficial owner (if any) is a politically-exposed individual, or a family member or close associate of any such individual (rule 8(1)(*d*) of the Rules).
(h) Understanding the nature of the client's business (rule 8(1)(*e*) of the Rules).
(i) Understanding the ownership and control structure of the client (rule 8(1)(*f*) of the Rules).
(j) Identifying and taking reasonable measures to verify the identity of, each beneficial owner of the client, where the client is an entity (rule 8(2) of the Rules).
(k) Identifying and taking reasonable measures to verify the identity of, each beneficial owner of the client, where the client is a legal arrangement (rule 8(3) of the Rules).
(l) Identifying and if appropriate, obtaining information on the purpose and intended nature of the business relationship with the client (rule 9(2) of the Rules).
(m) A legal practitioner who is a trustee of an express trust governed by Singapore law, obtaining and maintaining adequate, accurate and current information on the identities of the settlor, each trustee, the protector (if any) and each beneficiary or class of beneficiaries of the trust, and of any other individual exercising effective control over the trust (rule 10(2) of the Rules).
(n) A legal practitioner who is a trustee of any trust governed by Singapore law, obtaining and maintaining basic information on every other regulated agent of, or service provider to, the trust, including any investment adviser or manager, accountant or tax adviser (rule 10(3) of the Rules).

If the completion of the measures is deferred, the law practice must adopt internal risk management policies and procedures under which a business relationship may be established before the completion of the relevant CDD measures; and you must complete the relevant client due diligence measures as soon as is reasonably practicable (rules 11(3) and 11(4) of the Rules).

3.13 Ongoing CDD on business relationship

Your CDD obligations do not end after the onboarding of the client. You are obliged to continue to monitor both the client and the transaction for the duration of your retainer (rule 9(3) of the Rules). In the context of the legal profession, ongoing monitoring does not mean regular and repeated screening of clients. This is because most of our engagements will be for a short duration. The most important aspect of ongoing monitoring is for you to scrutinise transactions undertaken throughout the course of the engagement, to ensure that those transactions are consistent with your knowledge of the client, the client's business, the client's risk profile and, where appropriate, the source of funds for those transactions. FATF records show that half of all STRs lodged by lawyers were after the initial onboarding of the client.

Of course, for longer engagements (such as retainer arrangements) you need to ensure that the CDD data, documents and information obtained in respect of the client, each individual appointed to act on behalf of the client, and each beneficial owner of the client, are relevant and kept up-to-date. Accordingly, appropriate cases you must conduct regular reviews of existing client due diligence data, documents and information. You should determine your own schedule appropriate to your circumstances for this refreshing of you CDD data. An example will be:

- In case of Enhanced CDD – every 3 months
- In cases where the risk of money laundering is elevated – every year; and
- In other cases - every 2 years.

The degree and nature of the ongoing monitoring should be appropriate to the level of the ML/TF risks.

You should be alert to changes in instructions that substantially alter the nature of your engagement. For example, where you are instructed in the acquisition of a business, but when the acquisition is abandoned, you are instructed to transfer the purchase monies that you were holding to a different source.

Ongoing CDD does not require you to do the following:

(a) suspend or terminate a business relationship until you have updated CDD data, documents and information so long as you are satisfied that you know who your client is;
(b) perform the whole CDD process again every few years; and
(c) conduct random checks of files.

If you have reasonable grounds, based on the ongoing CDD, or otherwise, for suspecting that the business relationship with the client involves engagement in money laundering or the financing of terrorism, you should as appropriate:

(a) file a Suspicious Transaction Reporting Officer, if the client may be engaged in money laundering; and/or
(b) lodge a report with a police officer or Commercial Affairs Officer, if the client may be engaged in financing of terrorism.

In such a circumstance, you should also consider whether you should carry on with the engagement or retain the client (rule 9.3(c) of the Rules). One factor you should consider is

that you or your practice may be at risk of a civil claim by the victims of any crime as a constructive trustee. You should also consider your obligations under rule 26 PCR.

If you decide to retain the client, you must substantiate the reasons for doing so and document those reasons; and the business relationship must be subjected to commensurate risk mitigation measures, including enhanced ongoing monitoring. Possible reasonable reasons for continuing to act include situations where:

(a) ceasing to act may risk tipping off the suspect;
(b) the suspicion of money laundering is not on the part of your client but by some other party, and by ceasing to act you may jeopardise your innocent client's rights
(c) your engagement is not transactional and your continuing to act will not affect the ML/TF.

An illustration of the failure of ongoing monitoring is the case of PP v Kang Bee Leng [DAC 940645/2017]. The practitioner was instructed to act for a Chinese national in the acquisition of a property. The practitioner received funds from the client, *inter alia*, for the purposes of paying stamp duty. Subsequent to the engagement, the practitioner discovered that the client had been arrested for financial crimes in China. The practitioner suspected the monies passed to her represented the proceeds of those crimes, but did not make an STR. The practitioner was prosecuted and convicted for failing to make an STR.

3.14 Enhanced CDD measures

Enhanced CDD is an increased level of CDD for those clients that are considered to present a higher risk, but who do not arouse the level of suspicion to warrant filing an STR. This may be because of client's identity, status as a PEP, business activity, or association with a high risk territory.

Enhanced CDD is mandatory in the following situations (rule 13(1) of the Rules):

Country Risk

(i) If the client is from or in, or the transaction relates to, any country or jurisdiction in relation to which the FATF has called for countermeasures or enhanced client due diligence measures (the FATF black list). At present the black list consists of Iran, North Korea and Myanmar and can be viewed here.[4]
(ii) If the client is from or in any country or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism, as determined by the legal practitioner or law practice.

For the purposes of (ii), there is no universally agreed list of high risk countries or established criteria or determining the same. This country risk may arise in a variety of circumstances, including from the domicile of the client, the location of the transaction, or source of wealth/ funds.

However, it may be useful to consider these lists:

- FATF's website link of high-risk and non-cooperative countries http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

[4] The FATF black list should not be confused with the grey list. Countries on the grey list are actively working with FATF to address deficiencies in their AML/ CFT/ CPF regimes. FATF publishes the information relating to the specific deficiencies and encourages entities to consider them when assessing the risk posed by clients/ transaction associated with these countries. The grey list is reviewed regularly and updated 3 times a year as necessary. The latest list is available on the FATF website.

- BASEL AML Index: https://www.baselgovernance.org/basel-aml-index

- Corruption Perception Index by Transparency International: https://www.transparency.org/en/cpi#

Lists relevant to terrorist financing include:

- The List established and maintained by the Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL (Da'esh) Al-Qaida and associated individuals groups undertakings and entities: https://www.un.org/securitycouncil/sanctions/1267

- The List established and maintained by the Committee established pursuant to resolution 1988 (2011) with respect to individuals, entities, groups, or undertakings https://undocs.org/S/RES/1988(2011)

- MAS' website on targeted financial sanctions: https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities

All practices should subscribe to the MAS website to receive updates on the designations for terrorism.

More information on FT risks may be obtained from the Inter-Ministry Committee on Terrorist Designation's ('IMC-TD') website. IMC-TD was formed in 2012 to act as Singapore's authority relating to the designation of terrorists.

For risk countries in the context of tax crimes, you can refer to:

Global Forum on Transparency and Exchange of Information for Tax Purposes

Financial Secrecy Index by Tax Justice Network

In referencing a list, you should also bear in mind the circumstances. For example, if you are concerned about tax evasion, reference to a terrorism list is unlikely to be helpful.

The URLs above may change from time to time.

Law Society's AML portal provides links to all the above https://www.lawsociety.org.sg/for-lawyers/aml/

Politically Exposed Persons ("PEP")

(a) Where the client, or the beneficial owner of the client (being an entity or legal arrangement), is a foreign PEP or a family member or close associate of a PEP (rule 13(1)(b) of the Rules)
(b) Where the client or the beneficial owner of the client (being an entity or a legal arrangement) is a domestic PEP, or an individual entrusted with a prominent function in an international organisation, or a family member or close associate of any such individual AND you have assessed the business relationship with the client to be a higher risk business relationship, and (rule 13(1)(c) of the Rules)

The business relationship, based on information (on the purpose and intended nature of the business relationship) you have obtained, should be commensurate with what one could reasonably expect from the client, given his/her particular circumstances. Where the level or

type of activity in the business relationship diverges from what can be reasonably explained, the business relationship may be a higher risk business relationship (see paragraph 3.5).

When the risk assessment establishes that the business relationship with a domestic PEP /individual entrusted with a prominent function in an international organisation (or a family member or close associate) does not present a higher risk, the individual in question can be treated like any other normal client.

You should familiarise yourself with the definition of PEP in the Definitions part of this Practice Direction. Those who want to understand more about PEPs in the context of AML can refer to the FATF Guidance on Politically Exposed Persons, the link for which is available at the Law Society's AML Portal.

Enhanced CDD measures

When you conduct Enhanced CDD (or ECDD), you should do the following (rule 13(2) of the Rules):

(i) obtain the approval of your senior management before —
  (A) in the case of a new client, establishing a business relationship with the client; or
  (B) in the case of an existing client, continuing a business relationship with the client;
(ii) take reasonable measures to establish the source of wealth, and the source of funds, of the client and, if the client is an entity or a legal arrangement, of the beneficial owner of the client;
(iii) conduct enhanced ongoing monitoring of the business relationship with the client (see section 3.13 above).

Senior management

What constitutes senior management will depend on the size, structure, and nature of the law practice and it is for the law practice to determine their senior management. Senior management may be:

(i) the head of a practice group;
(ii) the partner or director supervising the file;
(iii) another partner or director who is not involved with the particular file; or
(iv) the managing partner or director.

If enhanced CDD measures have to be performed by the foreign branch or foreign subsidiary of a Singapore law practice (see paragraph 2.1.2), and senior management approval is required, the Singapore law practice may determine whether the approval should be given by the senior management of that foreign branch or subsidiary.

Source of wealth and source of funds

The source of wealth refers to the origin of the client's entire body of wealth (that is, total assets). The source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship with the client. Possible sources of wealth or funds include a PEP's current income, wealth or funds obtained from his current and previous positions, business undertakings, and family assets. It may be possible to gather general information on the source of wealth or funds from publicly disclosed assets, any other publicly available sources, from commercial databases or other open sources. An internet search (including of social media) may also reveal useful information about the client's wealth and lifestyle and about their official income. You may also rely on self-declarations of the client. If you rely on the client's declaration of the source of wealth or funds, any inability to verify the information should be taken into account in establishing its reliability. Discrepancies between client declarations and reliable information from other sources may be suspicious if such discrepancies cannot be satisfactorily explained.

Enhanced ongoing monitoring

What constitutes enhanced ongoing monitoring of the business relationship, will depend on the circumstances. Possibilities include:

- increasing the number and timing of controls applied,
- selecting transactions that need further examination.
- senior management taking on responsibility for monitoring the matter rather than delegating it to a junior.

3.15 Inability to complete CDD measures

If you are unable to complete any CDD measures, you (rule 15 of the Rules) –

(a) must not commence any new business relationship, and must terminate any existing business relationship, with the client;

(b) must not undertake any transaction for the client; and

(c) must consider whether to file a suspicious transaction report in relation to the client.

You are unable to complete the CDD measures if you:

(a) are unable to obtain or to verify any information required as part of those CDD measures; or

(b) do not receive a satisfactory response to any inquiry in relation to any information required as part of those CDD measures.

If you have started work for a client in relation to a transaction but completion of CDD was deferred in accordance with rule 11 of the Rules, you must not commence any new business relationship and must terminate any existing business relationship, if you are unable to complete the CDD measures. If you are unable to complete any ongoing CDD or enhanced CDD, you must terminate any existing business relationship with the client.

3.16 Where there are grounds to suspect money laundering or financing of terrorism

If you have reasonable grounds to suspect that a client may be engaged in money laundering or the financing of terrorism, you (rule 5 of the Rules):

(a) must not establish any new business relationship with, or undertake any new matter for the client; and

(b) must file a suspicious transaction report with either or both of the following –

(i) a Suspicious Transaction Reporting Officer, if the client may be engaged in money laundering;

(ii) a police officer or Commercial Affairs Officer, if the client may be engaged in the financing of terrorism.

If you suspect that a client may be engaged in money laundering or the financing of terrorism and have reasonable grounds to believe that the performance of any CDD will tip-off the client, you need not perform those CDD measures but must instead file a suspicious transaction report with either or both of the following (rule 16 of the Rules) –

(a) a Suspicious Transaction Reporting Officer, if the client may be engaged in money laundering;

(b) a police officer or Commercial Affairs Officer, if the client may be engaged in the financing of terrorism.

Part 4 – Suspicious Transaction Report

4.1 Duty to disclose under the CDSA

In accordance with section 70D in Part VA, where a legal practitioner or law practice knows or has reasonable grounds to suspect any matter referred to in section 39(1) of the CDSA, the legal practitioner or law practice must disclose the matter to a Suspicious Transaction Reporting Office ("STRO") under the CDSA by way of a suspicious transaction report ("STR").

The CDSA requires a suspicious transaction report to be made as soon as is reasonably practicable. The failure to make a suspicious transaction report is an offence punishable with up to $250,000 or imprisonment of up to 3 years or both.

If a suspicious transaction report is made in good faith, the disclosure will not be a breach of any restriction upon the disclosure imposed by law, contract or the rules of professional conduct (sections 39(6) and (8) CDSA).
In proceedings under the CDSA against a person for an offence (under section 43 or section 44 of the CDSA), he will be deemed not to have knowledge of the matters referred to in the STR (section 40 CDSA).

STRs must be lodged with the STRO via their online reporting system SONAR at https://www.police.gov.sg/SONAR. This requires registering for an account. All practices should so register so that when necessary, they can make their STR without delay.

4.2 Duty to disclose under the TSOFA

There is a duty under section 8(1) of the TSOFA for every person in Singapore and every citizen of Singapore outside Singapore who has (*inter alia*) information about any transaction or proposed transaction in respect of any property belonging to any terrorist or terrorist entity, to file a suspicious transaction report. Failure to do so is an offence. The report can be made through SONAR.

4.3 Not to prejudice investigation

If you know or have reasonable grounds to suspect that a suspicious transaction report has been made; it would be an offence (section 48 of the CDSA and section 10B of the TSOFA) to disclose to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following the disclosure.

4.4 Legal professional privilege

<u>Advocates and solicitors</u>
Singapore lawyers have a specific defence under s39(4) CDSA from making disclosure of information that is protected by legal professional privilege as defined in s2A CDSA. This definition of legal professional privilege closely follows the common law and in broad terms covers:

- communications between lawyer and client in connection with the giving of legal advice;
- communications between lawyer and client in connection with and for the purposes of any legal proceedings.

However, any communication, item or document that is made, prepared or held with the intention of furthering a criminal purpose is not covered by privilege. Although there are no reported Singapore decisions on the threshold for this illegality, this issue was recently

considered by the English High Court in the case *Addlesee v Dentons Europe LLP*[5]. The judge ruled that the evidential threshold was a "strong prima facie case" - being lower than "a balance of probabilities" or the threshold for summary judgment, "that the defendant had no real prospect of success".

Since money laundering itself is illegal, in practice it is very likely that there will be very few instances where the practitioner will be able to rely on the privilege. In practice it is likely only to be in the following circumstances:

- when being consulted by a client on whether the client should lodge an STR; and
- when being instructed by a client after the transaction has been completed, e.g. when the client is being investigated or prosecuted in relation to the subject transaction.

Practitioners should also bear in mind that the following information is not protected by privilege:

- identity and address of client (JSC BTA Bank v Syram, Clyde & Co [2011] EWHC 2163)
- Work product e.g., company formation documents (Time Super v ICAC [2002] HKCFI 707) conveyancing documents (ex P Baines & Baines [1988] QB 579), contracts and declarations of trust (DPP v Holman & Fenwick unreported 13 Dec 1993)

Foreign practitioners

Owing to the restrictive drafting of s39(4) and s2A CDSA, foreign practitioners in Singapore are not able to rely on these provisions as a defence. However, Singapore law generally recognises that foreign lawyers can rely on legal professional privilege under the common law to the same extent that Singapore lawyers can. Accordingly, the comments above on the scope and nature of legal professional privilege will apply equally to them. To the extent that they need to rely on a statutory foundation, the foreign practitioner will have to rely on the defence under s39(5) CDSA; that they had a reasonable excuse for not disclosing the information in question. If they are relying on a privilege that is coextensive with s2A, it is very likely that a court will find that it is a "reasonable excuse".

However foreign practitioners who wish to claim a wider privilege that they enjoy in their home jurisdiction may find that this will not be accepted as a reasonable excuse by a Singapore court. This is not an issue that has ever been addressed by the courts in Singapore and will almost certainly depend on the specifics of the situation.

Part 5 - Keeping of Records

5.1 General comments

In accordance with section 70E in Part VA, a legal practitioner and law practice are required to maintain all documents and records relating to each relevant matter, and all documents and records obtained through CDD measures.

Rule 19 of the Rules requires keeping of records in respect of the relevant matter, that is, the business relationship itself, not the materials obtained through CDD measures. Rule 20 of the Rules, on the other hand, refers to keeping of records of the CDD materials and supporting evidence.

A law practice has the discretion to keep the records:

(a) by way of original documents;
(b) by way of photocopies of original documents; or

[5] 2020 EWHC 238

(c) in computerised or electronic form including a scanned form.

5.2 Documents and records in relation to a relevant matter

You must maintain a document or record relating to a relevant matter for at least five years after the completion of the relevant matter (rule 19 of the Rules). It would suffice for one set of documents or records to be maintained between the legal practitioner and the law practice.
The obligations to continue maintaining the documents and records may change in the circumstances as described in rule 19 of the Rules.

5.3 Document and records in relation to CDD measures

You must maintain a document or record obtained through CDD measures for at least five years after termination of the business relationship with the client, or after the date of a transaction (which is in relation to an occasional transaction). An occasional transaction refers to a transaction carried out in a single transaction or several operations which appear to be linked.
It would suffice for one set of documents or records to be maintained between the legal practitioner and the law practice.

Examples of records to be kept, include the following:

(a) A copy each of the information and evidence of the client's, beneficiary owner's (if any) identity, and identity of individual purporting to act on behalf of a client. These include:
  (i) copies of all documents used in establishing and verifying the client's, beneficial owner's and the individual's (purporting to act on behalf of a client) identity; and
  (ii) the individual's authority to act on behalf of a client.

(b) Information on the purpose and intended nature of the business relationship.

(c) Written records that CDD measures are performed by a third party and the basis for relying on a third party to perform CDD.

(d) Written records of the analysis of the risks of money laundering and the financing of terrorism.

(e) Written records of the basis for determining that a client falls into the categories for which an inquiry into the existence of beneficial owner is not required.

(f) Written records of the reasons for retaining a client where there are reasonable grounds for suspecting that the business relationship with the client involves engagement in money laundering or the financing of terrorism.

(g) Written records of ongoing CDD measures.

(h) The legal practitioner or law practice's assessment where it performs enhanced CDD measures and the nature of the enhanced CDD measures.

(i) Written records of a determination whether to file a suspicious transaction report.

5.4 Application

By referencing the completion of the relevant matter and the termination of the business relationship respectively, rules 19 and 20 of the Rules make clear the records obtained through CDD may need to be kept longer than the records obtained on the relevant transaction itself. In other words, records of a particular transaction, either as an occasional transaction or within the business relationship, must be kept for five years after the date the transaction is completed. All other documents obtained through CDD must be kept for five years after the termination of the business relationship with the client.

The requirement on a legal practitioner to maintain records and documents is on the legal practitioner who acted on the matter. It is possible that more than one legal practitioner was involved in the matter. However, not all the legal practitioners may have acted in preparing for or carrying out any transaction concerning a relevant matter. The obligations to perform CDD

measures and to keep records would apply only to the legal practitioner(s) who acted in preparing for or carrying out any transaction concerning a relevant matter.
In the situation of a law practice dissolving or the license being revoked, and the legal practitioner ceasing to practise (rules 19(3)(*b*) and 20(3)(*b*) of the Rules), the proprietor or partner or director responsible for the file (subject to any agreement or understanding with the other legal practitioners (if any)), should continue to maintain the document or record.

5.5 Sufficiency of document and records

You must take reasonable steps to ensure that the documents and records kept in relation to a relevant matter are sufficient to substantially permit a reconstruction of the relevant matter and if required, to provide evidence for the prosecution of an offence relating to the relevant matter (rule 21 of the Rules).

Rule 21 of the Rules does not impose any additional obligations on legal practitioners or law practices over and above those set out in rules 19 and 20 of the Rules.

5.6 Documents and records to be made available to Council of the Law Society

Council may pursuant to section 70F of Part VA and rule 26 inspect practices in order to ascertain whether Part VA and the Rules are being complied with. Pursuant to this, the Law Society regularly inspects practices.

You must cooperate with these inspections and ensure that any documents and records required by the Council for purposes of an inspection are produced to the Council or to any person appointed by the Council (rule 22 of the Rules).

Part 6 – New Technologies, Services and Business Practices

6.1 General comments

You must identify and assess the risks of money laundering and the financing of terrorism that may arise in relation to (rule 23 of the Rules) —

(a) the development of any new service or new business practice (including any new delivery mechanism for any new or existing service); and
(b) the use of any new or developing technology for any new or existing service.

Before offering any new service or starting any new business practice, or using any new or developing technology, you must:

(a) undertake an assessment of the risks of money laundering and the financing of terrorism that may arise in relation to the offering of that service, the starting of that business practice or the use of that technology; and
(b) take appropriate measures to manage and mitigate those risks.

6.2 Virtual assets

One emerging area is in relation to virtual assets. If you act for clients in the virtual assets industry, you must assess the attendant risks of ML and TF.

In particular, FATF has noted that the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralised platforms and exchanges, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows. There are many documented cases of criminal and terrorist groups using virtual assets and you must be alert to the risk.

There has also been the emergence of other virtual asset business models or activities such as initial coin offerings, that present fraud and market manipulation risks. There have been many fraudulent ICOs. There are also new illicit financing typologies that continue to emerge, including the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap and secure manner.

Legal practitioners and law practices may act for virtual asset clients in different capacities, including but not limited to assisting by providing escrow or trust services, legal opinions on the legitimacy of offerings and services, regulatory applications and advice, transactional support, corporate setup, and legal consulting services. They may also be advising exchanges and wallet providers in relation to their money laundering and terrorism financing policies and procedures, suspicious transaction reporting, and regulatory reporting requirements.

When acting for clients in the virtual assets industry, you should apply a risk-based approach when considering whether to establish or continue relationships with clients, evaluate the money laundering and financing of terrorism risks of the business relationship, and assess whether these risks can be appropriately mitigated and managed. You should also satisfy yourself that you have a sufficient understanding of the transactions that you are advising on so that you have a basis to make your assessment.

Depending on the scope and nature of work carried out for the client, you may also need to consider whether your firm needs to employ enhanced due diligence tools specific for the virtual assets industry to screen the client and his source of funds during the client onboarding process.

However, it is important that the risk-based approach should be applied properly, and clients are not excluded within the sector without a proper risk assessment.

The following indicators may raise red flags warranting ECDD:

- the initial coin offering issuer requests for funds to be distributed immediately after token distribution but before the completion of the said project, or requests that the law practice distributes funds in a manner that deviates from the outlined structure in the white paper;

- the client requests for tax advice or corporate setup advice in other jurisdictions to assist with the evasion of taxes, transfers of funds or to evade regulations;

- the founders or advisers of the initial coin offering have been linked to failed offerings or scams in the market, or there are falsehoods involved in their profiles or white paper claims;

- the client requests for payment to be made from a third-party payer which does not seem to be clearly linked to the project or client; and/or

- the source of funds or virtual assets cannot be clearly established.

- Real world identity of the source of the virtual asset cannot be established.

- You appear to be interposed into a virtual asset transaction without any good commercial reason but rather to lend an appearance of legitimacy to a transaction.

You should ensure that you have sufficient technical expertise to evaluate your client's marketing claims so that you are able to properly assess the money laundering and terrorist financing risks of your client's business model and projects.

If you accept virtual assets as payment for legal services, sufficient information should be requested to verify the source of funds for payment. You should also consider whether enhanced due diligence tools would be required to help screen the source wallet address. You should assess the risks of using any virtual currency payment processors to convert virtual assets to fiat currencies.

FATF have produced a Guidance For a Risk-Based Approach To Virtual Currencies which is available from the Law Society's AML Portal.

Part 7 – Creation, Operation or Management of a Company

7.1 General

This includes:

a. Acting or arranging for another person to act as a director, secretary of a corporation or its equivalent in other legal entities;
b. Acting or arranging for another person to act as a partner in a partnership or its equivalent in other entities;
c. Providing a registered office, business or correspondence address, or other related services for a corporation, partnership or other legal entity; and/or
d. Acting or arranging for another person to act as a shareholder on behalf of any corporation.

If you are performing these functions in respect of a Singapore company, your practice will be a registered filing agent or RFA licensed by ACRA and will have to comply with the AML/TF requirements in Part 2 of the First Schedule of the ACRA Regulations.

These include, but are not limited to the following:

- Conducting due diligence on customers (including ascertaining beneficial ownership);
- Developing internal policies, procedures and controls to prevent activities related to money laundering and financing of terrorism; and
- Assessing risks and applying a risk-based approach.

For more information, please refer to the ACRA Regulations and the ACRA AML Guidelines on the CDD measures applicable for RFAs. A copy of the ACRA AML Guidelines can be accessed here: https://www.acra.gov.sg/docs/default-source/default-document-library/corporate-service-providers/rfaguidelines_v2-3(12nov).pdf

7.2 Formation of corporations and other legal entities on behalf of customers

In assessing the risks of forming a corporation or other legal entity on behalf of a customer, you should take into account factors such as: (i) the type of customer (taking into account the risk factors that are described in this Practice Direction); (ii) the type of transaction that the customer expects you to perform; (iii) the purpose the company is being formed; (iv) the geographical area of the operation of the customer's business; and (v) the business relationships and transactions with persons from high risk jurisdictions.

You must be particularly careful when you are being required to provide nominee services (e.g., as a director or shareholder) or act as bank signatory.

7.3 Acting as an Intermediary

Rather than undertaking the actual incorporation, you may be instructed as an intermediary to procure an offshore corporation or other entity for the client- for example, acquiring a shelf company from a service provider. This is particularly prevalent in the context of acquiring offshore companies from jurisdictions such as the British Virgin Islands. Such an engagement will also constitute a relevant matter requiring you to conduct CDD on the client, and the directors and shareholders of the offshore entity.

Other Information

If you wish to read further guidance in connection with the Rules, please refer to the Law Society's website (https://www.lawsociety.org.sg/for-lawyers/aml/).

There are other materials available which may be useful. This is primarily as a result of the Rules closely following the FATF Recommendations which set out a comprehensive framework of international standards. As a FATF member, Singapore is obliged to implement the FATF Recommendations, which have been adopted by many countries around the world. In understanding and implementing your obligations under Part VA, the Rules and this Practice Direction, we would draw your attention to the following additional materials issued by FATF (which may be updated from time to time):

1. The FATF Risk-Based Approach Guidance for Legal Professionals, June 2019
2. FATF - Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, June 2013
3. FATF Guidance – Politically Exposed Persons (Recommendations 12 and 22), June 2013
4. FATF Guidance On The Risk Based Approach to Combating Money Laundering and Terrorist Financing-high level principles and procedures
5. FATF Guidance Transparency and Beneficial Ownership
6. FATF Guidance on Proliferation Financing Risk Assessment and Mitigation
7. FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers