AML/CFT Guidelines for Law Firms/Foreign Law Firms/Joint Law Venture/Foreign Lawyers

Issued under section 19H (1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002

Attorney General's Office

2019

Table of Contents

Table of acronyms

AML/CFT	Anti-money Laundering/Countering the Financing of Terrorism and proliferation
AGO	Attorney General's Office
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Money Laundering Group
FATF	Financial Action Task Force
FI	Financial Institution
FIAMLA	Financial Intelligence and Anti-Money Laundering Act 2002
FIAML Regulations	Financial Intelligence and Anti-Money Laundering Regulations 2018
FIU	Financial Intelligence Unit
LPP	Legal Professional Privilege
MER	Mutual Evaluation Report
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NRA	National Risk Assessment
PCPs	Policies, controls and procedures
PEP	Politically Exposed Person
POCA	Prevention of Corruption Act 2002
POTA	Prevention of Terrorism Act 2002
RBA	Risk Based Approach

Rec	Recommendation
Reg	Regulation
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
CSP	Company Service Providers
TF	Terrorist Financing
UN Sanctions Act	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
UNSCR	United Nations Security Council Resolutions

Terminology used in the guidelines

You – refers to a legal professional/practitioner or law practice or a reporting person.

Shall/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.

Disclaimer

These Guidelines[1] are intended to provide assistance to registered law firms, foreign law firms, joint law venture, foreign lawyers who are members of a relevant profession or occupation in meeting their obligations under the FIAMLA, POCA, POTA, UN Sanctions Act and the FIAML Regulations. This Guide has been prepared and published for informational and educational purposes only and should not be construed as legal advice. The laws and regulations discussed in this Guide are complex and subject to frequent change. If you are unsure about your obligations in a given case, you should consider taking independent legal advice.

The Guidelines must be read in conjunction with the Financial Intelligence and Anti-Money Laundering Act 2002, Prevention of Corruption Act 2002, Prevention of Terrorism Act 2002, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Convention of the Suppression of the Financing of Terrorism Act and the Financial Intelligence and Anti-Money Laundering Regulations 2018.

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

a) The FATF Recommendations 2012 and their Interpretive Notes, and the FATF Glossary.
b) Other relevant FATF Guidance documents such as:
    - The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
    - FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs)
    - FATF Guidance on Transparency and Beneficial Ownership (October 2014)
c) Other relevant FATF Reports such as:

[1] For the purposes of this exercise, the term 'guidelines' or 'guide' or 'guidance notes' mean one and the same thing and the term will be used interchangeably throughout this document.

- FATF Report on Money Laundering and Terrorist Financing: Vulnerabilities of Legal Professionals (June 2013)
- Risk Based Approach for Legal Professionals (June 2019)

d) The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

Chapter 1 Introduction

1.1 Who should read these Guidelines?

All legal professionals and other staff in a law practice who are involved in AML/CFT compliance.

As these guidelines apply across the entire legal sector, the term 'legal professional' has been used to include legal professionals working in law firms, foreign law firms, joint law venture and foreign lawyers as defined in the Law Practitioner's Act 1984.

1.2 Background

Mauritius is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a regional inter-governmental body established to combat money laundering and terrorism financing in the eastern and southern African region. ESAAMLG members adopted a Memorandum of Understanding which established the Group and provided the basis that would enable them to forge the process of cooperation for implementing the Recommendations of the Financial Action Task Force (FATF).

In February 2012, the FATF issued revised Recommendations which set out a number of new requirements compelling its members to implement in order to effectively combat money laundering and terrorism financing. Mauritius was assessed by ESAAMLG in relation to its anti-money laundering and counter-terrorist financing (AML/CFT) system, using the FATF Assessment Methodology 2013. The assessment comprised a comprehensive review of the effectiveness of Mauritius' AML/CFT system and its level of compliance with the FATF Recommendations.

The Mutual Evaluation Report (MER) was published in September 2018. The MER has identified the strengths and weaknesses of the systems and procedures in place in Mauritius for combating money laundering and terrorism financing and has made a number of recommendations to enable Mauritius improve its systems and procedures. On the basis of the results of the mutual evaluation, Mauritius was placed under ESAAMLG's enhanced follow

up procedures. Accordingly, Mauritius has to report bi-annually on the progress that it is making in implementing the recommended actions contained in the MER.

In this respect, Mauritius has amended the FIAMLA, POCA, POTA and enacted the FIAML Regulations and UN Sanctions Act in order to meet the FATF requirements and improve its AML/CFT framework. As it currently stands, all statutes pertaining to AML/CFT apply to all Financial Institutions (FIs) and the Designated Non-Financial Businesses and Professions (DNFBPs).[2]

1.3 Application to the legal practice

Legal professionals are key actors in the business and financial world, facilitating vital transactions that underpin the Mauritian economy. The FATF characterizes legal professionals as "Gatekeepers"[3] because they "protect the gates to the financial system," through which potential users must pass in order to succeed. The term includes professional experts who may, by the very nature of their work, provide financial expertise to launderers, including lawyers, accountants, tax advisers, and trust and service company providers (TCSP). The FATF has noted that gatekeepers are a common element in complex money laundering schemes. Gatekeepers' skills are important in creating legal structures that could be used to launder money and for their ability to manage and perform transactions efficiently to avoid detection.

Recommendation 22 of the FATF acknowledges the role that such gatekeepers can play by recommending that such individuals have AML/CFT responsibilities when engaged in certain activities. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. Legal professionals are therefore called to act with integrity and uphold the law. Money laundering and terrorist financing & proliferation are serious threats to society; endangering life, causing financial losses and fueling other criminal activities.

These guidelines aim to assist legal professionals to meet their obligations under the Mauritian AML/CFT regime.

[2] DNFBPs include legal professionals and the legal sector as a whole.

[3] FATF Methodology (2013) p 105.

1.4 What is Money Laundering and Terrorist Financing?

a) Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Under section 3 of the FIAMLA, the definition is broader as it puts an added layer of obligation on members of a relevant profession and occupation to prevent its services from being used to commit money laundering and the financing of terrorism. It also captures the elements of conspiracy under section 4 of the FIAMLA.
b) Terrorist financing is defined under section 2 of the UN Sanctions Acts which means the financing of terrorist, terrorist acts and terrorist organisations.

There are three acknowledged and distinct phases to money laundering, namely: placement, layering and integration.

1.4.1 Placement

It involves the introduction of criminally tainted money in the financial system. The money launderer intentionally breaks up large sums of money into conspicuously smaller sums of money. It is partly deposited in a bank and the rest is used to purchase a series of monetary instruments. The money is once again collected and deposited into various accounts at a different location. Because banks and financial institutions have developed AML procedures, criminals look for other ways of placing cash within the financial system. One such method may be through legal professionals as their activities commonly deal with criminals as clients[4] and also because the legal professionals usually engage/deal with high net worth clients.

[4] For all intents and purposes, the word 'client' has the same meaning as 'customer.' In this respect, both words will be used interchangeably throughout this guidance.

1.4.2 Layering

The second stage is 'layering' and it constitutes dissociating the laundered money from its origins. This is done through a series of complex and convoluted transactions in order to obscure the origins of the proceeds. These transactions may involve different entities such as companies and trusts. It can also take the form of financial assets such as shares, securities, properties or insurance products. The complicated process of creating layers of financial transactions is designed to mislead the audit trail. Additionally, the launderer may convert the money and\or move the funds around with the purpose of camouflaging the source. This can be done through buying and selling stocks, commodities, properties, or dealing in precious metal stones with cash and repaying a loan. The launderer might use various channels to wire funds in multiple bank accounts across the globe. Legal professionals may be targeted at this stage and detection can be difficult.

1.4.3 Integration

The final stage is called integration which involves the use of funds in the economy through different investments. The appearance of legitimacy illustrates that the two previous stages were successful. Here, the property becomes part and parcel of the wider economy. The criminal nature of the activity is absorbed and remains latent. The illusion of a legitimate source for criminally derived funds is maintained by common techniques like producing false invoices for goods sold in another country, using funds held in a foreign bank as security for a domestic loan, commingling of bank accounts from legitimate and illegitimate sources and buying property in order to show the appearance of legal proceeds upon disposal. Integration is the most difficult stage to detect money laundering.

1.5 Know your ML/TF risks

Undetected financial crime reduces the integrity of national and international financial systems, distorts the economy and diminishes opportunities for legitimate economic activities. The Government loses tax revenue, while people are rewarded for criminal

behaviour. Mauritius is at risk of being targeted by international criminal networks to inject the proceeds of crime into the international financial system. Money laundering and financing of terrorism are not solely international crimes. Domestic criminals use a variety of methods to conceal the proceeds of their criminal activities from authorities in Mauritius.

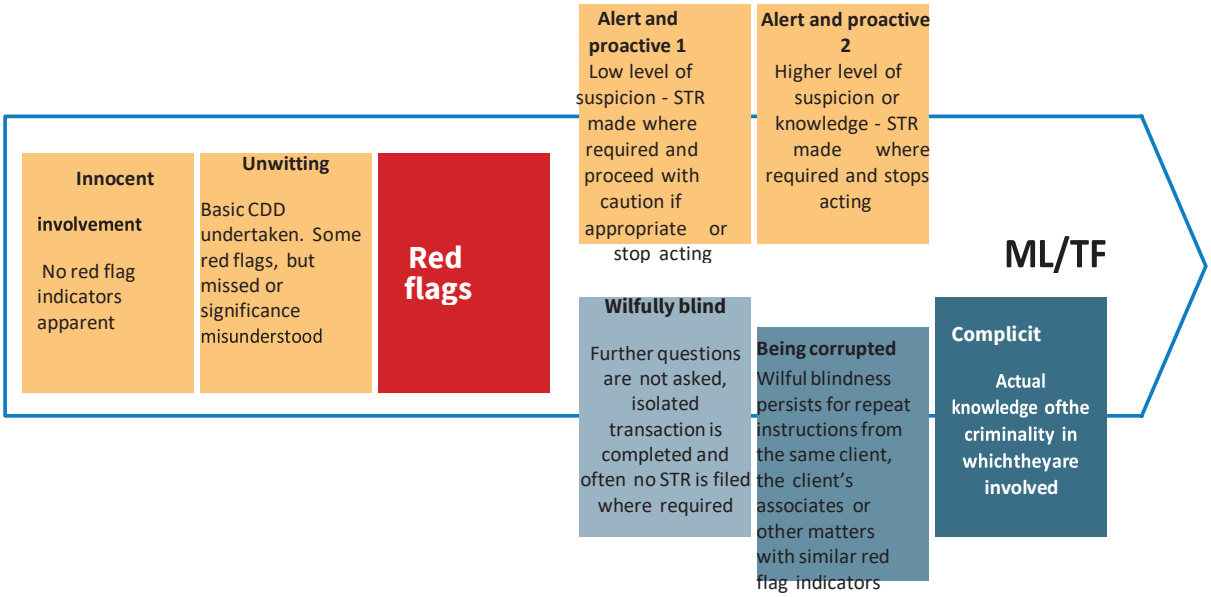
The Financial Action Task Force (FATF) is an inter- governmental body that sets standards for combating ML/TF and other related threats to the integrity of the international financial system.

Using legal professionals is attractive to some people because these professionals are required for the completion of certain kinds of transactions and because their specialist legal skills can be misused to assist the laundering of criminal proceeds or funding terrorism.

Given these risks, and the FATF recommendations, the Government has chosen to engage gatekeeper professions in the collective efforts to deter and detect these crimes. By expanding the AML/CFT system to include the gatekeeper professions, the Government intends that gatekeepers will be better able to protect themselves from customers who launder money and finance terrorism. The AML/CFT system has been designed to help businesses achieve the level of compliance required to assist authorities to identify criminal customers.

Compliance also has a value for business risk management. Professionals closely guard their reputations. It is in their interest to avoid relationships with customers who will cause them disrepute in the legal community or censure by their professional bodies or government authorities. Businesses that fail to comply and are misused by criminals risk negative media coverage both in Mauritius and internationally. This also diminishes the international reputation of Mauritius as a safe place to do business.

The FATF has provided the following diagram to describe the two potential trajectories of legal professionals' involvement in ML/TF:


Innocent involvement
No red flag indicators apparent
Unwitting
Basic CDD undertaken. Some red flags, but missed or significance misunderstood
Red flags
Alert and proactive 1
Low level of suspicion - STR made where required and proceed with caution if appropriate or stop acting
Alert and proactive 2
Higher level of suspicion or knowledge - STR made where required and stops acting
ML/TF
Wilfully blind
Further questions are not asked, isolated transaction is completed and often no STR is filed where required
Being corrupted
Wilful blindness persists for repeat instructions from the same client, the client's associates or other matters with similar red flag indicators
Complicit
Actual knowledge ofthe criminality in whichtheyare involved

Chapter 2 Nature and Scope of the powers of a Regulatory Body under the FIAMLA

2.1 Nature of the power

According to the First Schedule of the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA), the regulatory body for law firm, foreign law firm, joint law venture and foreign lawyer is the Attorney General's Office for anti-money laundering (AML) and counter financing terrorism (CFT) & proliferation purposes.

2.2 Functions of the Regulatory Body

Pursuant to section 19G of the FIAMLA, the functions of a Regulatory Body are to:

a. supervise, monitor and give guidance to a member falling under its purview;
b. cooperate with, and assist investigatory authorities;
c. exchange information with investigatory authorities and supervisory authorities;
d. assist and exchange information with overseas comparable regulatory bodies; and
e. undertake and assist in research projects in order to identify the methods and trends of money laundering activities and the financing of terrorism and proliferation activities in Mauritius and in the region.

A regulatory body may enter into an agreement or arrangement for the exchange of information with an overseas comparable regulatory body while protecting the confidentiality of any information exchanged.

A regulatory body may consult with, and seek such assistance from, any association or body representing a member or any other person as it may deem appropriate.

2.3 Scope of the powers of a Regulatory Body

According to section 19H of the FIAMLA, a regulatory body shall have such powers as are necessary to enable it to effectively discharge its functions and may, in particular –

a. issue guidelines for the purposes of combating money laundering activities and the financing of terrorism and proliferation activities;
b. give directions to a member falling under its purview to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts;
c. require a member falling under its purview to submit a report on corrective measures it is taking to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts, at such intervals as may be required by the regulatory body.
d. With respect to a member falling under its purview, the regulatory body may apply any or all of the following administrative sanctions –
    (i) issue a private warning;
    (ii) issue a public censure;
    (iii) impose such administrative penalty as may be prescribed by the regulatory body;
    (iv) ban, where the regulatory body has licensed or authorised the member to conduct his business or profession, from conducting his profession or business for a period not exceeding 5 years; and
    (v) revoke or cancel a licence, an approval or an authorisation, as the case may be.

Where a barrister, an attorney or a notary has failed or is failing to comply with, or has failed or is failing to take such measures as are required under this Act or the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, or any regulations made or guidelines issued under those Acts, FIU shall, pursuant to section 13 of the Law Practitioners Act, report the matter to the Attorney-General.

On receipt of a report, the Attorney-General shall take such measures as are required under section 13 of the Law Practitioners Act.

Any person who fails to comply with a direction issued shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

It is noteworthy to highlight that a regulatory body may publish any of its decision or determination, or the decision of the Review Panel, or any other information the regulatory body may deem appropriate.

2.4 Request for information

As per section 19J of the FIAMLA, a regulatory body may require a member falling under its purview to furnish any information and produce any record or document within such time as it may determine. Failing to comply with such requirement may constitute an offence punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 2 years.

2.5 Onsite Inspections

Section 19K of the FIAMLA states that a regulatory body may at any time-

i. audit and inspect the books and records of a member falling under its purview in order to verify that the member is compliant with the FIAMLA and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (UN Sanctions Act); and
ii. direct orally or in writing the member to produce documents or material that is relevant to inspection.

Any person who intentionally obstructs and fails without any reasonable excuse to comply with any direction of the regulatory body shall commit an offence and be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Additionally, any person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal of, any document, information stored on a computer or other device or other thing that the person knows or ought reasonably to have known is relevant to an onsite inspection or investigation, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

2.6 Directions by regulatory body

By virtue of section 19L of the FIAMLA, a regulatory body may give written directions to its member where he has reasonable cause to believe that a member who falls under its purview has failed or is failing to comply with the requirements under the FIAMLA and the UN Sanctions Act or is engaging in money laundering and the financing of terrorism and proliferation activities.

The regulatory body may take any of these actions-

i. remove or take steps to remove any specified employee from office;
ii. ask the member falling under its purview to refrain from doing a specified act;
iii. ensure that a specified employee does not take part in his management or conduct except as permitted by the regulatory body;
iv. appoint a specified person to a specified office for a period specified in the direction;
v. implement corrective measures and reports on the implementation of the corrective measures; and
vi. revoke a direction and notify accordingly its member.

Non-compliance with the direction of a regulatory body is punishable by 5000 rupees per day under section 19M of the FIAMLA. In addition, a person who knowingly hinders or prevents compliance with a direction may be liable to a fine not exceeding one million rupees and a term of imprisonment not exceeding 5 years.

2.7 Administrative sanctions

Where a regulatory body has reasonable cause to believe that a member falling under its purview has contravened the FIAMLA and/or the UN Sanctions Act, it is empowered to impose administrative sanctions under section 19N of the FIAMLA. Details of the Administrative Sanctions can be found at section 19H(1)(d) FIAMLA.

2.8 Compounding of offences

The regulatory body may with the consent of the Director of Public Prosecutions (DPP) compound any offence committed under the FIAMLA and the UN Sanctions Act as per section 19P of the FIAMLA.

Where the DPP does not give his consent to compound the offence or the person does not agree to the compounding of the offence, the regulatory body may, with the consent of the DPP, refer the matter to the police.

2.9 Review Panel

Section 19Q of the FIAMLA caters for the establishment of a Review Panel which will be responsible to review a decision of a regulatory body to impose an administrative sanction under section 19N of the same Act.

Under section 19S of the FIAMLA, a member who is aggrieved by the decision of the regulatory body, may within 21 days of the decision of the regulatory body, make an application to the Review Panel for a review of that decision.

Finally, the avenue for a judicial review of the determination of the Review Panel to the Supreme Court is made possible under section 19X of the FIAMLA.

Chapter 3 Risk-Based Approach to Supervision

Know if the FIAMLA applies to your business

Law firms, foreign law firms, joint law venture and foreign lawyers will have obligations under the First Schedule of the FIAMLA when they conduct certain activities (referred to throughout this guidance as "listed activities"). The following listed activities are:

i. buying and selling of real estate;

ii. managing of client money, securities or other assets;

iii. management of bank, savings or securities accounts;

iv. organisation of contributions for the creation, operation or management of legal persons such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed;

v. creating, operating or management of legal persons such as a company, a foundation, an association, a limited liability partnership or such other entity as may be prescribed, or legal arrangements, and buying and selling of business entities; or

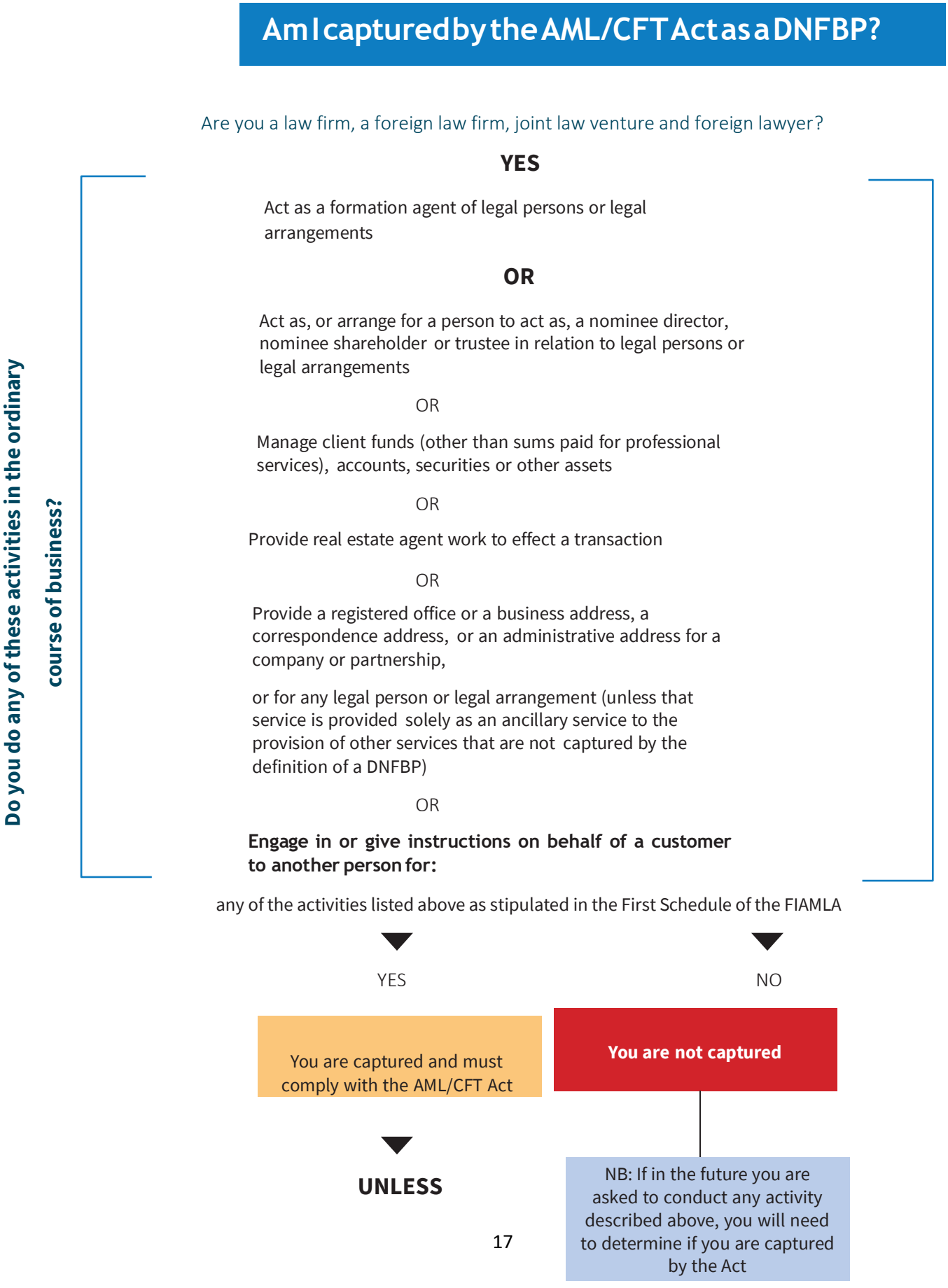
vi. acting as a formation agent of a legal person with a view to assisting another person to incorporate, register or set up, as the case may be, a company, a foundation, a limited liability partnership or such other entity as may be prescribed;

vii. acting, or causing another person to act, as a director, as a secretary, as a partner or in any other similar position, as the case may be, of a legal person such as a company, foundation, a limited liability partnership or such other entity as may be prescribed;

viii. providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; or

ix. acting, or causing for another person to act, as a nominee shareholder for another person.

How to know if you are captured by the FIAMLA



There is an exemption which excludes your business from compliance requirements

There will be circumstances where you give advice in relation to a listed activity (without necessarily then carrying out the activity). Generally, advice alone, in the absence of any actual listed activity, will not be caught.

It may be that in practice you expect to provide a mixture of advice and listed activities for a customer over a period of time. In those circumstances, you would need to conduct CDD to the required level *prior* to establishing a business relationship with the customer (and prior to providing any advice).

You also need to be aware of your obligations to report suspicious activities, which can include requests or enquiries about particular services you offer from potential new customers (regardless of whether you ultimately provide those services).

What obligations are related to the listed activities

The FIAMLA requires you to know who your customers are (as well as who any beneficial owners of your customer are, and any person acting on behalf of your customer) by conducting customer due diligence (CDD) to the level required before you conduct a listed activity or establish a business relationship.

3.1 Customer Due Diligence (CDD)

Section 2 of the FIAMLA defines a "reporting person" as a bank, financial institution, cash dealer or member of a relevant profession or occupation. A member of a relevant profession or occupation is further defined in the first schedule of the FIAMLA. This includes law firm, foreign law firm, joint law venture and foreign lawyer.

In this respect, by virtue of section 17 of the FIAMLA, every reporting person shall-

a. take appropriate steps to identify, assess and understand the ML and TF risks for customers, countries and products, services, transactions or delivery channels; and
b. consider all relevant risk factors before determining what is the level of overall risk and appropriate level and type of mitigation to be applied.

According to section 17(2) of the FIAMLA, the nature and extent of the assessment shall depend on the nature and size of the business which will include inter alia the following factors-

i. the nature, scale and complexity of the reporting person's activities;

ii. the products and services provided by the reporting person;

iii. the persons to whom and the manner in which the products and services are provided;

iv. the nature, scale, complexity and location of the customer's activities;

v. reliance on third parties for elements of the customer due diligence process;

vi. technological developments; and

vii. the outcome of any risk assessment carried out at a national level and any guidance issued.

Section 17(3) of the FIAMLA states that prior to the launch of a new product or business practice or the use of a new or developing technology, a reporting person or a supervisory authority shall identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices and take appropriate measures to mitigate these risks.

Pursuant to section 17(4) of the FIAMLA, every reporting person shall document the risk assessments in writing, keep it up to date and, on request, make it available to relevant competent authorities without delay.

3.1.1 CDD requirements

According to section 17C of the FIAMLA, a reporting person shall undertake CDD measures to-

- establish a business relationship with a customer;
- a transaction in an amount equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
- a domestic or cross-border wire transfer
- doubts exist the veracity or adequacy of previously obtained customer identification information;
- there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account;
- the risks are higher, a reporting person shall perform enhanced due diligence;
- the risks are lower; a reporting person may apply simplified due diligence measures. However, the low risk identified by the reporting person should be consistent with the findings of the National Risk Assessment (NRA) in order to comply with regulation 11(2) of the FIAML Regulations; and
- apply CDD measures as prescribed and specified by a supervisory authority.

The CDD requirements have to be in accordance with the findings of the National Risk Assessment pursuant to section 19D of the FIAMLA.

3.1.2 Methods of verification

Customer-natural person

Regulation 4 of the FIAML Regulations requires that the reporting person shall obtain from and verify a customer who is a natural person the following information-

a. the full legal and any other names, including, marital name, former legal name or alias;
b. the date and place of birth;
c. the nationality;

d. the current and permanent address; and
e. such other information as may be specified by a relevant supervisory authority or regulatory body.

Customer-legal person or legal arrangement

According to regulation 5 of the FIAML Regulations, where the customer is a legal person or legal entity, the reporting person shall-

(a) with respect to the customer, understand and document –

i. the nature of his business
ii. his ownership and control structure

(b) identify the customer and verify his identity by obtaining the following information –

i. name, legal form and proof of existence;
ii. powers that regulate and bind the customer;
iii. names of the relevant persons having a senior management position in the legal person or arrangement; and
iv. the address of the registered office and, if different, a principal place of business.

3.1.3 Independent source

You need a reliable source to verify your client's identity, which is independent of the client as per regulation 2 of the FIAML Regulations. This can include materials provided by the client, such as a passport. Consider the cumulative weight of information you have on the client and the risk levels associated with both the client and the retainer[5]. You are permitted to use a wider range of sources when verifying the identity of the beneficial owner and understanding the ownership and control structure of the client. Sometimes only the client or their representatives can provide such information. Apply the requirements in a risk-based manner to a level at which you are satisfied that you know who the beneficial owner is. In addition, it will be necessary to obtain further verification, for example confirmation from the

[5] A contract between lawyer and client specifying the nature of the services to be rendered and the cost of the services.

client that the information is up to date or other documentation confirming the beneficial ownership of the client.

3.1.4 Documents

Obvious forgeries should not be ignored. You may consider providing relevant employees with appropriate training and equipment to help identify forged documents.

3.1.5 Electronic verification

You should consider whether any electronic verification system you use properly establishes the customer's identity, rather than just establishing that the identity exists. You should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that your client is not the person they say they are. You may mitigate risk by corroborating electronic verification with some other CDD material. When using electronic verification, you are not required to obtain consent from your client, but they must be informed that this check will take place. While electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate.

3.1.6 Non-face to face clients

Risks that may arise from non-face-to-face relationships could favour anonymity. Due to the prevalence of electronic communication between legal professionals and clients in the delivery of legal services, non-face-to-face interaction between legal professionals and clients would not be considered a high-risk factor on its own. Because the legislation is silent on this issue, it would be only advisable to follow the best practices models.

Where a client is a natural person and they are not physically present for identification purposes, you must take this into account when assessing whether there is a high risk of money laundering or terrorist financing and the extent of any Enhanced Due Diligence measures that need to be taken. A client who is not a natural person will only be represented by an agent.

Therefore, you should consider your risk analysis, the risks associated with the retainer and the client, assess how well standard CDD measures are meeting those risks and decide whether further CDD measures are required. Instances where Enhanced Due Diligence measures may be required-

i. clients who appear to be acting on somebody else's instructions without disclosing the identity of such person;
ii. clients who appear to actively and inexplicably avoid face-to-face meetings without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected;
iii. clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the legal professionals to perform a proper risk assessment;
iv. clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g their age, income, occupation or wealth);
v. clients who have no address, or who have multiple addresses without legitimate reasons;
vi. clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last-minute changes are made to enable funds to be paid in from/out to a third party;
vii. clients who insist, without reasonable explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity;
viii. clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium;
ix. unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with similar profile;
x. where there are certain transactions, structure, geographical location, international activities or other factors that are not consistent with the legal professional's understanding of the client's business or economic situation;

xi. the legal professional's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent;
xii. clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions;
xiii. sudden activity from a previously dormant client without clear explanations;
xiv. client is from or in any country or jurisdiction in relation to which the FATF has called for countermeasures or enhanced due diligence measures; and
xv. client is from or in any country or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism.

3.2 Beneficial Ownership

Section 3 of the FIAMLA defines a 'beneficial owner' as a natural person-

i. who ultimately owns or controls a customer;
ii. on whose behalf a transaction is being conducted;
iii. includes those natural persons who exercise ultimate control over a legal person or arrangement; and
iv. such other persons as may be prescribed.

Regulation 6 of the FIAML Regulations states that where the customer is a legal person, the reporting person shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on-

i. the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;
ii. In case of doubt, the regulatory or supervisory authority may specify other means to know the identity of the natural person exercising control of the legal person; and
iii. In case no natural person is identified under (i) and (ii), the identity of the natural person who holds position of senior managing official must be sought.

3.2.1 Legal arrangements & Trusts

Regulation 7 of the FIAML Regulations sets out the information required to verify the identity of beneficial owners-

a) for trusts, the identity of the-
    i. settlor;
    ii. trustee;
    iii. beneficiaries or class of beneficiaries;
    iv. where applicable, the protector or the enforcer; and
    v. any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership.

3.2.2 Beneficiary of life insurance

According to regulation 8 of the FIAML Regulations, a reporting person has to perform CDD measures on the beneficiary of life insurance and other investment related insurance policies as soon as the beneficiary is identified or designated. The following information is required-

a. for a beneficiary that is identified as a natural or legal person or legal arrangement, the reporting person shall take the name of that person;
b. for a beneficiary that is designated by characteristics or class, or by other means, the reporting person shall obtain sufficient information concerning the beneficiaries to satisfy the life or investment related insurance business that would be able to establish the identity of the beneficiary at the time of the payout; and
c. in all the cases mentioned under paragraph 3.2, the reporting person shall verify the identity of the beneficiary at the time of the payout.

3.3 Ongoing CDD

Pursuant to regulation 9 of the FIAML Regulations, a reporting person shall verify the identity of the customer and beneficial owner-

i. before or during the course of establishing a business relationship or conducting transactions for occasional customers; and
ii. where doubts exist about the veracity or adequacy of previously obtained customer identification information, the reporting person shall identify and verify the identity of the customer and beneficial owner before the customer may conduct any further business.

By virtue of regulation 9(3) of the FIAML Regulations, a reporting person may be allowed by the relevant supervisory authority or regulatory body to complete the verification of the identity of the customer and beneficial owner after the establishment of the business relationship, provided that-

i. this is essential not to interrupt the normal conduct of business;
ii. the verification of identity occurs as soon as reasonably practicable;
iii. the money laundering and terrorism financing risks are effectively managed by the reporting person; and
iv. the reporting person shall adopt and implement risk management procedures concerning the conditions under which a customer may utilise prior to verification.

3.4 CDD on existing customers

According to section 17E of the FIAMLA, a reporting person shall apply CDD requirements to customers and beneficial owners-

- with which a business relationship has already commenced by having regard to the following factors-
    i. the basis of materiality and risk depending on the type and nature of the customer;
    ii. the business relationship;
    iii. products or transactions;
    iv. previous CDD measures; and
    v. adequacy of information obtained.

And as per Regulation 10 of the FIAML Regulations, a reporting person shall apply CDD measures to existing customers when-

i. there is indication that the identity of the customer or the beneficial owner has changed;
ii. any transactions which are not reasonably consistent with his knowledge of the customer;
iii. any change in the purpose or intended nature of his relationship with the customer; and
iv. any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

Therefore, you need not repeatedly identify and verify the identity of a customer 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 and/or any of the above-mentioned factors become pertinent to your customer.

3.5 Simplified Due Diligence

A reporting person may apply simplified CDD measures pursuant to Regulation 11 of the FIAML Regulations where-

i. lower risks have been identified;
ii. are in accordance with any guidelines issued by the AGO; and
iii. is consistent with the NRA findings and/or any risk assessment findings of the regulatory/supervisory body, whichever is most recently issued.

It is not appropriate to apply Simplified Due Diligence measures where a reporting person-

i. knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing; or
ii. that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

3.6 Enhanced Customer Due Diligence

According to Regulation 12 of the FIAML Regulations, a reporting person must, in addition to performing the basic CDD measures, perform enhanced CDD measures in the following situations-

i. where a higher risk of money laundering or terrorist financing has been identified;
ii. where through supervisory guidance, a high risk of money laundering or terrorist financing has been identified;
iii. where a customer or an applicant for business is from a high risk third country;
iv. in relation to correspondent banking relationships;
v. the customer is a PEP;
vi. where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer; and
vii. in the event of any unusual or suspicious activity.

Enhanced CDD measures include but not limited to-

i. obtaining additional information on the customer through:
    - occupation
    - volume of assets
    - information available through public databases
    - internet

ii. updating more regularly the identification data of the customer and the beneficial owner;
iii. obtaining additional information on the intended nature of the business relationship;
iv. obtaining information on the source of funds or source of wealth of the customer;
v. obtaining information on the reasons for intended or performed transactions;
vi. obtaining the approval of senior management to commence or continue the business relationship;
vii. conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
viii. requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards;
ix. where a reporting person determines that the beneficiary who is a legal person or legal arrangement presents a higher risk, the reporting person shall take enhanced due diligence measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout; and

x. where the beneficiary of a life insurance policy is identified as a relevant risk factor when determining whether enhanced CDD measures are required.

In any event, if the reporting person is unable to perform enhanced CDD where it is required under the law, he shall terminate the business relationship and shall file a suspicious transaction report under section 14 of the FIAMLA.

3.7 Inability to complete CDD measures

Where a reporting person is unable to comply with the relevant CDD measures under the FIAML Regulations, the following action shall be taken pursuant to Regulation 13 of the FIAML Regulations. Therefore, the reporting person-

i. must not open the account;
ii. must not commence the business relationship;
iii. must not perform a transaction;
iv. shall terminate the business relationship; and
v. shall file a suspicious transaction report.

3.8 Record keeping

Record keeping and quality assurance are important for supervisors to carry out risk-based approach to AML/CFT supervision on their members. Supervisors should be able to easily retrieve information while complying with the data protection rules. Having a proper and effective record keeping system assists significantly the supervisory process in decision making and sanctioning its supervised members.

To reflect the above, section 17F of the FIAMLA requires that a reporting person-

i. shall maintain all books and records with respect to his customers and transactions; and
ii. shall ensure that such records and books are kept for such time as specified.
The time limit to maintain such domestic and international records is 7 years after the business relationship has ended and/or after the completion of the transaction, as stipulated in section 17F (2)(b) of the FIAMLA.

The books and records shall include-

i. all records obtained through CDD measures-
    - account files;
    - business correspondence;
    - copies of all documents evidencing the identity of customers and beneficial owners;
    - records and the results of any analysis undertaken should be in accordance with the FIAMLA;
ii. records of both domestic and international transactions that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders; and
iii. copies of all suspicious transaction reports made to the FIU.

Moreover, Regulation 14 of the FIAML Regulations puts an added layer of requirement by stating that-

i. a reporting person shall keep and maintain all necessary records to transactions in such a form which enables the prompt reconstruction of each individual transaction;
ii. where a reporting person is responding to a request made under section 13(2) of the FIAMLA or to a request from a supervisory or relevant regulatory body, it shall provide for each transaction record the following information-
    - the full name of the party making a payment
    - the full name of the party receiving the payment; and
iii. a reporting person shall ensure that all CDD information and transaction records are kept in such a manner that they are swiftly made available to the FIU or any relevant regulatory body or supervisory authority upon request.

3.9 Obligation to report currency transactions

Section 17G of the FIAMLA puts a legal obligation on a reporting person to submit a report to the FIU of any currency transaction in an amount equal to or above the prescribed amount,[6] whether conducted as-

i. a single transaction; or

[6] a transaction in an amount equal to or above 500,000 rupees as per section 17C of the FIAMLA.

ii. several transactions that appear to be linked.

3.10 Third party reliance

In order to rely on another regulated/supervised/monitored person to perform CDD measures in accordance with section 17D of the FIAMLA you must also consider the implications of regulation 21 of the FIAML Regulations and-

i. obtain immediately the necessary information required;
ii. take steps to satisfy himself that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;
iii. satisfy himself that the party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing and has measures in place for compliance with CDD and record keeping requirements in line with the FIAMLA and FIAML Regulations; and
iv. not rely on a third party based in a high-risk country.

A reporting person may rely on a third party that is part of the same financial group where-

i. the group applies CDD and record keeping requirements and programs against ML and TF in accordance with the FIAMLA and FIAML Regulations;
ii. the implementation of those CDD, record keeping and programs against ML and TF is supervised at a group level by a competent authority; and
iii. any higher country risk is adequately mitigated by the group's policies to combat ML and TF.

You should note that you remain liable for any non-compliance with CDD requirements when you rely on a third party (section 17D (2) of the FIAMLA). For this reason, you should ask what CDD enquiries the third party has undertaken to ensure that there is compliance with the laws & Regulations and the risk-based approach. This is particularly important when relying on a person outside Mauritius. You should ensure that the CDD information provided to you is up to date.

3.11 High risk country

According to section 17H of the FIAMLA, where the FATF has identified significant or strategic deficiencies in the AML/CFT measures of a jurisdiction, the Minister may-

i. on the recommendation of the National Committee; and
ii. after giving due consideration to such factors as may be prescribed;

identify that jurisdiction as a high-risk country.

Mitigating measures

A reporting person with respect to business relationships or transactions involving a high-risk country shall-

i. apply enhanced CDD measures; and
ii. apply proportionate mitigating measures including-
    - the application of additional elements of enhanced due diligence;
    - the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and
    - the limitation of business relationships or transactions with natural persons or legal entities from the countries identified as high-risk countries.

Actions to be taken

Where the Minister identifies a high-risk country, he shall on the recommendation of the FATF or the National Committee, apply the following countermeasures-

i. refuse the establishment of subsidiaries or branches or representative officers of reporting persons from the country concerned;
ii. prohibit reporting persons from establishing branches or representative offices in the high-risk country;
iii. limit business relationships or financial transactions with the identified country or persons in that country;
iv. prohibit reporting persons from relying on parties located in the country concerned to conduct elements of CDD;

v. require reporting persons to review and amend, or if necessary terminate, correspondent banking and other similar relationships with institutions in the country concerned;
vi. require increased supervisory examination and external audit requirements for branches and subsidiaries of reporting persons based in the country concerned; and
vii. require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

Factors to consider when identifying a third risk country

Regulation 24 of the FIAML Regulations lists the factors to which due consideration shall be given in identifying a third risk country. These are-

i. Strategic deficiencies in the AML/CFT legal and institutional framework in particular in relation to-
    - criminalization of money laundering and terrorism financing
    - measures relating to CDD
    - requirements relating to record-keeping
    - requirements to report suspicious transactions
    - the availability and accurate and timely information of the beneficial ownership of legal persons and arrangements to competent authorities
ii. powers and procedures of the third country's competent authorities for the purposes of combating ML and TF with effective, proportionate and dissuasive sanctions;
iii. country's practice in cooperation and exchange of information with overseas competent authorities;
iv. effectiveness of the third country's system in addressing ML and TF risks;
v. to have regard to relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing ML and combating TF; and
vi. apply Enhanced Due Diligence proportionate to the risks, to business relationships and transactions with natural and legal persons to countries identified as high risk by the FATF.

Chapter 4 Policies, controls and procedures

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

A risk-based approach requires legal professionals to mitigate the risks they face with due regard to the resources available. Mitigating risks include but not limited to performing initial CDD, ongoing monitoring, having robust internal policies, training and systems to address the vulnerabilities faced by legal professionals in different situations. Policies and procedures supporting these systems enable staff to apply the systems consistently and demonstrate to supervisors that processes facilitating compliance are in place.

The law mandates that every reporting person, pursuant to section 17A of the FIAMLA, shall-

i. Establish policies, controls and procedures[7] to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the reporting person;
ii. Monitor the implementation, review and update the policies, controls and procedures;
iii. Maintain a record in writing of-
    - the policies, controls and procedures
    - any changes to the policies, controls and procedures
    - the steps taken to communicate those policies, controls and procedures internally; and
iv. establish policies, controls and procedures that are proportionate to the size and nature of the business of a reporting person which must be approved by the senior management.

[7] Abbreviated to PCPs.

Fictitious and anonymous accounts

Pursuant to section 17B of the FIAMLA, a reporting person shall not establish or maintain an anonymous account or an account in a fictitious name.

4.1 Programs for the prevention of money laundering and the financing of terrorism

Taking into account the risks that have been identified and the size of the business, legal professionals must develop programs for the prevention of money laundering and the financing of terrorism.

Rule 22 of the FIAML Regulations makes it a requirement for every reporting person to implement programs against money laundering and terrorism financing by having regard to the ML/TF risks identified and the size of the business. The internal policies, procedures and controls should include the-

i. designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with internal programs, controls and procedures;
ii. screening procedures to ensure high standard when hiring employees;
iii. ongoing training program for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to-
    - assist them in recognizing transactions and actions that may be linked to money laundering and terrorism financing
    - instruct them in the procedures to be followed where any links have been identified; and
iv. an independent audit function to review and verify compliance with and effectiveness of the measures;

Screening procedures

The screening of new employees (referred to in reg 22 of the FIAML Regulations) can be done by including relevant questions in the legal 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 and/or any other relevant factors.

Training

Training may cover the following areas-

i. money laundering and financing of terrorism vulnerabilities of a legal practice;
ii. the impact that money laundering and financing of terrorism may have on a legal practice, its business, clients and employees;
iii. effective ways of determining whether clients are politically-exposed individuals;
iv. client and business relationship risk factors;
v. the different CDD measures that have to be performed;
vi. how to deal with suspicious activities and transactions;
vii. suspicious transaction reporting; and
viii. 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-

i. attendance at conferences, seminars, or training courses organized by the Institute for Judicial and Legal Studies of Mauritius or other organizations;
ii. completion of online training sessions;
iii. law practice or practice group meetings for discussion on prevention of money laundering and financing of terrorism issues and risk factors; and
iv. (review of publications on current prevention of money laundering and financing of terrorism issues.

4.2 Group wide application

Law practices must consider the application of the FIAMLA and FIAML regulations to their wider group. According to regulation 23 of the FIAML regulations, every reporting person operating in a group structure shall implement group-wide program against money laundering

and terrorism financing which shall be applicable to all branches and subsidiaries of the group. The program shall include-

i. the internal policies, procedures and controls set out in regulation 22 of the FIAML regulations;
ii. policies and procedures for sharing information required for the purposes of customer due diligence and money laundering and terrorism financing risk management;
iii. procedures to ensure that group-level compliance, audit, Money Laundering and Reporting Officer shall have the power to request customer, account and transaction information from branches and subsidiaries as necessary to perform their functions in order to combat money laundering and terrorism financing;
iv. the provision to branches and subsidiaries information and analysis of transactions or activities which appear unusual when relevant and appropriate to risk management;
v. adequate safeguards on the confidentiality and use of information exchanged including safeguards against tipping off; and
vi. that a reporting person shall ensure that its foreign branches and subsidiaries-
    - apply measures to combat money laundering and terrorism financing consistent with the home country requirements to the extent that it is consistent with the laws and regulations of the host country; and
    - where the host country does not permit the proper implementation of anti-money laundering and combatting the financing of terrorism measures, the different branches and subsidiaries shall apply appropriate additional measures to manage the money laundering and terrorism financing risks and inform their home supervisors.

4.3 Appointment of Money Laundering Reporting Officer

Regulation 26 requires that a reporting person shall appoint-

i. a Money Laundering Reporting Officer to whom an internal report shall be made of any information or other matter that would give rise to knowledge or reasonable suspicion that a person is engaged in money laundering and financing of terrorism; and
ii. a Deputy MLRO in the absence of a MLRO.

The law provides for a derogation of the rule under Regulation 26(3) of the FIAML Regulations where a reporting person, due to the size of its business or activity, is unable to appoint a MLRO or a deputy MLRO, shall establish, maintain and operate reporting and disclosure procedures under the FIAMLA, FIAML Regulations and as may be specified by the AGO.

In addition, regulation 26(4) of the FIAML Regulations states that-

i. the MLRO and deputy MLRO shall be sufficiently senior in the organization of the reporting person or have sufficient experience and authority; and
ii. have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

4.4 Reporting procedures and disclosures

Reporting procedures are henceforth an obligation under regulation 27 of the FIAML Regulations. A reporting person shall establish document, maintain and operate reporting procedures that shall-

i. enable all its directors or, as the case may be, partners, of all other persons involved in its management;
ii. enable all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;
iii. ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the MLRO;
iv. require reports of internal disclosures to be made to the MLRO of any information or other matter when there is knowledge or suspicion of money laundering and terrorism financing activity;
v. require the MLRO to consider any report in the light of all other relevant information available for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;
vi. ensure that the MLRO has full access to any other information that may be of assistance and that is available to the reporting person; and
vii. enable the information or other matters contained in a report to be provided as soon as is practicable to the FIU where the MLRO knows or suspects that another person is engaged in money laundering or terrorism financing activities.

4.4.1 Enhanced CDD in relation to suspicious activity

Regulation 28 of the FIAML Regulations mentions that where a reporting person identifies any suspicious and/or unusual activity in the course of a business relationship or occasional transaction, the reporting person shall-

i. perform appropriate scrutiny of the activity;
ii. consider obtaining enhanced CDD; and
iii. make an internal disclosure.

4.4.2 Disclosures

By virtue of regulation 29 of the FIAML Regulations, the MLRO shall assess the information when an internal disclosure has been made and determine-

i. whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing; and
ii. file a report to the FIU if the MLRO knows or has reason to believe that an internal disclosure may be suspicious.

4.4.3 Registers

All internal and external disclosures have to be kept and maintained separately by a reporting person according to regulation 30 of the FIAML Regulations. The registers of internal and external disclosures may be contained in a single document if the details can be presented separately when requested by a competent authority (reg 30(2) FIAML Regulations).

The registers must contain the following details-

i. the date on which the report is made;
ii. the person who makes the report;
iii. for internal disclosures, whether it is made to the MLRO or deputy MLRO; and
iv. information sufficient to identify the relevant papers.

4.5 Monitoring Compliance with PCPs

Law practices must ensure that they regularly review their risk assessment and PCPs, even if they have determined that the size and nature of the practice is such that an independent audit function is not required. Monitoring compliance will assist you to assess whether the PCPs that you have implemented are effective in identifying and preventing money laundering and terrorist financing opportunities within your practice. Issues which may be covered in such a review may include-

i. procedures to be undertaken to monitor compliance, which may involve-
    - random file audits
    - file checklists to be completed before opening or closing a file
    - reports brought to the attention of MLRO and deputy MLRO, queries from staff and reports made;
ii. reports to be provided to senior management on compliance;
iii. how to rectify lack of compliance, when identified; and
iv. how lessons learnt will be communicated back to the staff and fed back into the risk profile of the practice.

The above-mentioned principle is reflected in regulation 31 of the FIAML Regulations where a reporting person shall establish and maintain appropriate procedures for monitoring and testing compliance with AML/CFT by having regard to-

i. the robust and documented arrangements for managing the risks identified by the business risk assessment;
ii. the operational performance of those arrangements is suitably monitored; and
iii. prompt action is taken to remedy any deficiencies in arrangements.

Chapter 5 Politically Exposed Persons

Politically Exposed Persons (PEPs) have been a focus of the FATF as there are concerns that PEPs have used their political position to corruptly enrich themselves. You should take a risk-based and proportionate approach to identifying PEPs and then apply EDD measures and treat business with PEPs on a case by case basis.

Peps have been classified as "domestic PEPs," "foreign peps" and "international organization PEPs" in the FIAML Regulations. A domestic PEP means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Foreign PEPs have the same definition as above insofar as they are entrusted with prominent public function by a foreign country.

An "international organization PEP" means a person who is or has been entrusted with a prominent function by an international organization and included members of senior management or individuals who have been entrusted with equivalent functions including directors, deputy directors and members of the board or equivalent functions and such other person or category of person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

5.1 Examples on who may be a PEP?

- heads of state
- heads of government
- ministers and deputy or assistant ministers
- members of parliament or similar legislative bodies
- members of governing bodies of political parties

- members of supreme courts, or any judicial body whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charges d' affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board of equivalent function of an international organization

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

In addition to the primary PEPs listed above, a PEP also includes (regulation 15(5) FIAML Regulations)-

i. close associates mean-
   - an individual who is closely connected to a PEP, either socially or professionally; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

ii. family members mean-
   - an individual who is related to a PEP either directly through consanguinity, or through marriage or similar forms of partnership; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

5.2 How to identify a PEP?

You are not required to conduct extensive investigations to establish whether a person is a PEP. You can use information that is in your possession or publicly known. Many practices use subscriber services that can run checks against the PEPs databases which they maintain. If your practice regularly encounters PEPs, you should consider a subscription as otherwise it is easy to 'miss' PEPs in your client database including at ultimate beneficial ownership level. To

assess your PEP risk profile, you must take into account your risk assessment, the level of risk of money laundering or terrorist financing inherent in your business and the extent to which that risk would be increased by a business relationship with a PEP. If the risk of you acquiring a PEP as a client is low, you may simply wish to ask clients whether they fall within any of the PEP categories. Where they say no, you may reasonably assume the individual is not a PEP unless anything else within the retainer, or that you otherwise become aware of, makes you suspect they may be a PEP. Where you have a higher risk of having PEPs as clients or you have reason to suspect that a person may actually be a PEP contrary to earlier information, you should consider conducting some form of electronic verification. You may find that a web-based search engine will be sufficient for these purposes, or you may decide that it is more appropriate to conduct electronic checks through a reputable international electronic verification provider. The range of PEPs is wide and constantly changing, so electronic verification will not give you 100 per cent certainty.

You should remain alert to situations suggesting the client is a PEP. Such situations include-

i. receiving funds in the retainer from a government account;
ii. correspondence on official letterhead from the client or a related person;
iii. general conversation with the client or person related to the retainer linking the person to a PEP; and
iv. news reports which come to your attention suggesting your client is actually a PEP or linked to one.

Where you suspect a client is a PEP but cannot establish that for certain, you should consider what steps you could take in order to resolve this uncertainty. If you are not able to resolve the issue to your satisfaction, you may consider on a risk-sensitive basis applying aspects of Enhanced Due Diligence procedures (as a lack of clarity as to whether a person is a PEP could, in and of itself, be indicative of a heightened risk of money laundering).

It is advisable for legal professionals to inform their senior management that they are dealing with a PEP. Senior management may be-

i. the head of a practice group;
ii. another partner who is not involved with the particular file;
iii. the partner supervising the particular file;
iv. the nominated officer or, if different, the officer responsible for compliance under the FIAML Regulations; and

v. the managing partner.

In any case, it is recommended that you advise those responsible for monitoring risk assessment that a business relationship with a PEP has begun, to help their overall monitoring of the practice's risk profile and compliance.

5.3 Enhanced Monitoring and supervision

According to regulation 15 of the FIAML Regulations, a reporting person shall in relation to a foreign PEP (both as a customer or beneficial owner) apply CDD measures and-

i. put in place and maintain appropriate risk management systems;
ii. obtain senior management approval before establishing or continuing for existing customers, such business relationships;
iii. take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
iv. conduct enhanced ongoing monitoring on that relationship.

In addition, a reporting person shall in relation to domestic PEPs or an international organization PEP-

i. verify if the customer or beneficial owner is a PEP; and
ii. apply enhanced monitoring and supervision measures as listed above.

Life Insurance Policies

At the time of payout in relation to life insurance policies, a reporting person should take reasonable measures to determine whether the beneficiaries or the beneficial owner of the beneficiary are PEPS. Where higher risks are identified, the reporting person shall-

i. inform senior management before the payout of the policy proceeds;
ii. conduct enhanced scrutiny on the whole business relationship with the policy holder; and
iii. consider making a suspicious transaction report.

Chapter 6 Filing of Suspicious Transaction Report

Recommendation 23 of the FATF requires legal professionals to report suspicious transactions set out in Recommendation 20 of the FATF, when on behalf of, or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 22 of the FATF. Subject to certain limitations, such reporting is not required if the relevant information is directly encompassed within a legitimate claim of professional secrecy or legal professional privilege. Legal professionals have an obligation not to facilitate illegal activity, so if there are suspicions, they could contact their FIU or Supervisory bodies for guidance, obtain independent legal advice if necessary, and do not provide services to that person/company and report the transaction or the attempted transaction. Legal professionals may be asked to advise a client on the client's own obligation to report suspicious activity. In doing so, the legal professional may become aware of the subject matter giving rise to the suspicion. In these circumstances, the legal professional will need to consider whether it should file a Suspicious Transaction Report (STR) where required.

6.1 Filing

To mirror this principle, section 14 of the FIAMLA imposes a legal obligation on a member of a relevant profession or occupation (which includes law firms and legal professionals who are also reporting persons under the law) to-

i. as soon as practicable; and
ii. but no later than 15 working days from the day the reporting person became aware of the suspicious transaction;

to make a report of such transaction to the FIU.

The FIU is also obligated by law to provide feedback to the reporting person and relevant supervisory authorities following an STR under section 14(1A) of the FIAMLA.

Lodging of reports of suspicious transaction

The procedure to lodge a report of suspicious transactions is laid down under section 15 of the FIAMLA. It stipulates that-

i. every report shall be lodged with the FIU;
ii. the report shall be in such a form as approved by the FIU;
iii. the report shall include-
    - the identification of the party or parties to the transaction
    - the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion
    - the business relationship of the suspect to the bank, financial institution, cash dealer or member of a relevant profession or occupation
    - where the suspect is an insider, whether the suspect is still affiliated with the bank, financial institution, cash dealer, or member of a relevant profession or occupation
    - any voluntary statement as to the origin, source or destination of the proceeds
    - the impact of the suspicious activity on the financial soundness of the reporting institution or person
    - the names of all the officers, employees or agents dealing with the transaction
iv. no report of a suspicious transaction shall be required to be disclosed or be admissible as evidence in any court proceedings.

No tipping off

According to section 16 of the FIAMLA, it is an offence to tip off the person who is suspected of money laundering. The law states that-

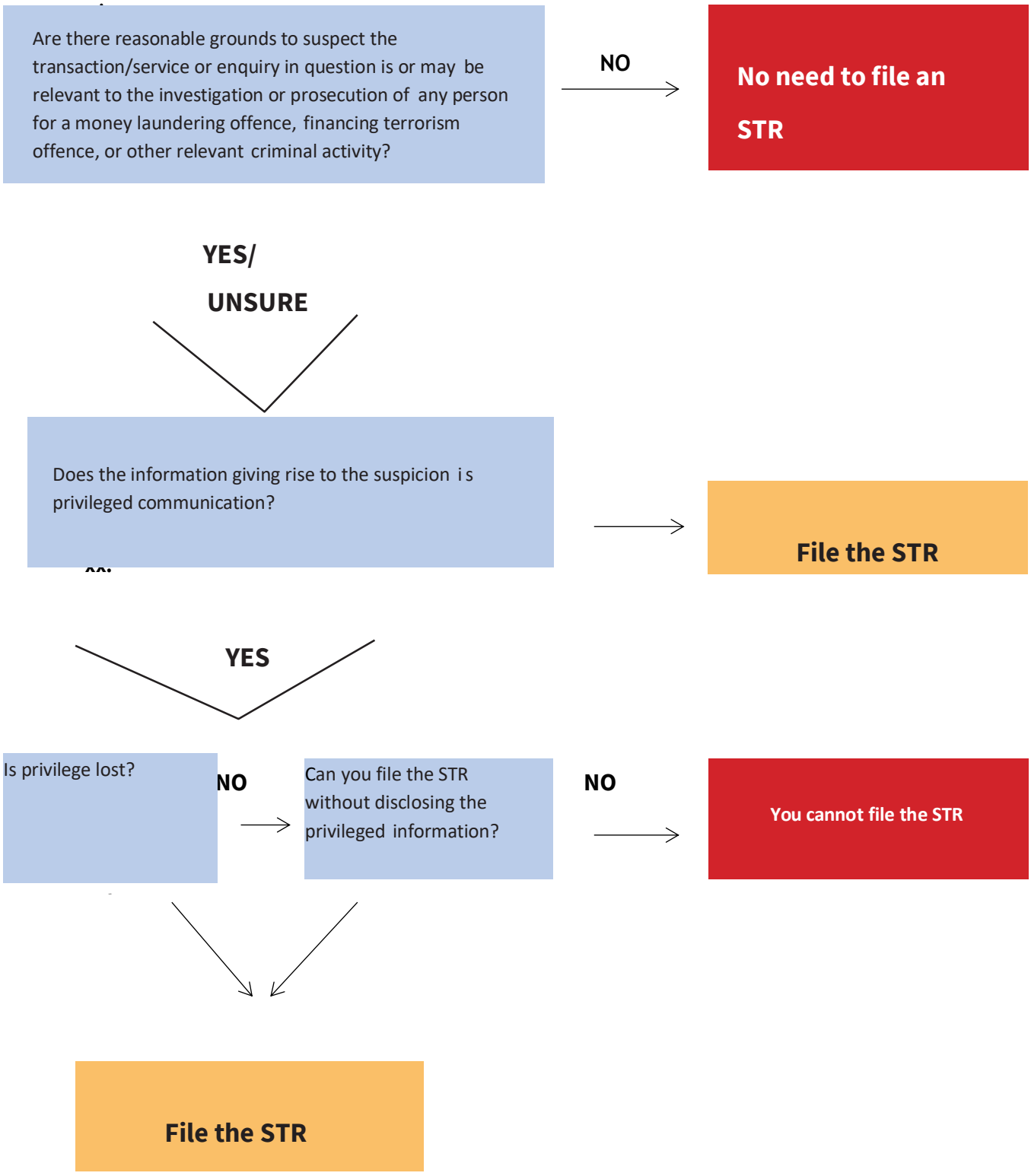
i. any reporting person and its officers shall not disclose to any person that suspicious transaction report is being or has been filed, or that related information is being or has been requested by, furnished or submitted to the FIU;
ii. any supervisory authority may for the sole purpose of discharging its compliance duty request the FIY a copy of the STR;

iii. no proceedings shall lie against any person who reported in good faith any suspicion of money laundering regardless of whether it was proved to be well founded following an investigation or prosecution or any other judicial action;

iv. no reporting person and its officers who shares a report will be in breach of confidentiality for any disclosure made in compliance with this Act or to assist its supervisory authority; and

v. any disclosure made for compliance, audit or AML/CFT functions at group level should have adequate standards on the confidentiality and use of information exchanged to prevent tipping off within the group.

Lawyers may find it thelpful to ask the following questions when consideringwhether to file an STR:



Chapter 7 Duty of Confidentiality and Legal Professional Privilege

Legal professionals are under a duty to keep the affairs of their clients confidential, and the circumstances in which they are able to disclose client communications are strictly limited. This chapter examines the tension between a legal professional's duties and the provisions in law pertaining to AML/CFT where disclosure may be compelled.

7.1 Duty of confidentiality

A legal professional is professionally and legally obliged to keep the affairs of clients confidential and to ensure that his staff abides by the same rules. The obligations extend to all matters revealed to a legal professional, from whatever source, by a client, or someone acting on the client's behalf. In exceptional circumstances this general obligation of confidence may be overridden. However, certain communications can never be disclosed unless a statute permits this either expressly or by necessary implication. These communications are ordinarily protected by legal professional privilege (LPP).

7.2 Legal Professional Privilege

LPP is a privilege against disclosure, ensuring clients know that certain documents and information provided to legal professionals cannot be disclosed at all. It recognises the client's fundamental human right to be candid with his/her legal adviser, without fear of later disclosure to his/her prejudice. It is an absolute right and cannot be overridden by any other interest, except when compelled by law. LPP does not extend to everything that legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

7.2.1 Advice Privilege

Communications between a legal professional, acting in his capacity as a legal professional, and a client, are privileged if they are both-

i. confidential; and
ii. for the purpose of seeking legal advice from a legal professional or providing it to a client.

Communications are not privileged merely because a client is speaking or writing to you. The protection applies only to those communications which directly seek or provide advice or which are given in a legal context, that involve the legal professional using his legal skills and which are directly related to the performance of the legal professional's professional duties [Passmore on Privilege 2nd edition 2006].

7.2.2 Litigation Privilege

This privilege, which is wider than advice privilege, protects confidential communications made after litigation has started, or is reasonably in prospect, between any of the following-

i. a legal professional and a client;
ii. a legal professional and an agent, whether or not that agent is a legal professional; or
iii. a legal professional and a third party.

These communications must be for the sole or dominant purpose of litigation, for any of the following-

i. for seeking or giving advice in relation to it;
ii. for obtaining evidence to be used in it; or
iii. for obtaining information leading to obtaining such evidence.

7.3 Legal position in Mauritius

Section 300 of the criminal code 1838 reads:

> *Any physician, surgeon, as well as any pharmacist, midwife, or any other person, who may, in consequence of his or her profession or avocation, become the depositary of any secret confided to him or her, and who, except when compelled by law, to become*

informer, reveals such secret, shall be punished by imprisonment for a term not exceeding 2 years and by a fine not exceeding rupees 100, 000 rupees.

The practitioner-client privilege is further expressed in section 10C (4)(a)-(b) of the Law Practitioners Act 1984 which states that-

i. a law firm shall have the same rights and be the subject to the same fiduciary, confidential and ethical obligations as a law practitioner has and is subject to; and
ii. the law practitioner-client privilege shall exist between a law firm and its clients and extends to every law practitioner who is a partner, director or employee of the law firm.

Fraud/crime exception

In section 13(2A) of the FIAMLA, a law practitioner is not required to disclose any information which he/she has acquired in privileged circumstances, unless it was communicated with a view to further a criminal or fraudulent purpose. The same legal principle of client-law practitioner privilege is expressed in section 14(2) of the FIAMLA with a caveat that a derogation of the principle is only permissible when it is to further a criminal or fraudulent purpose.

When to disclose?

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under FIAMLA. If the communication was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of FIAMLA. If neither of these situations applies, the communication will still be confidential. However, the material is disclosable and could only be disclosed under the FIAMLA if it falls outside the ambit of legal privilege and/or compelled by law.

Obligations under listed activities

The First Schedule of the FIAMLA states that legal professionals, law firm, a foreign law firm, a joint law venture, a foreign lawyer have to comply with the obligations under the FIAMLA

and any Regulations and/or guidelines made under this Act when engaging in the following activities-

x. buying and selling of real estate;

xi. managing of client money, securities or other assets;

xii. management of bank, savings or securities accounts;

xiii. organisation of contributions for the creation, operation or management of legal persons such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed;

xiv. creating, operating or management of legal persons such as a company, a foundation, an association, a limited liability partnership or such other entity as may be prescribed, or legal arrangements, and buying and selling of business entities; or

xv. acting as a formation agent of a legal person with a view to assisting another person to incorporate, register or set up, as the case may be, a company, a foundation, a limited liability partnership or such other entity as may be prescribed;

xvi. acting, or causing another person to act, as a director, as a secretary, as a partner or in any other similar position, as the case may be, of a legal person such as a company, foundation, a limited liability partnership or such other entity as may be prescribed;

xvii. providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; or

xviii. acting, or causing for another person to act, as a nominee shareholder for another person.

Chapter 8 Terrorist financing offences

8.1 Introduction

Terrorist organizations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The UN Sanctions Act criminalises the provision of monetary support for terrorist purposes by implementing the United Nations Security Council Resolutions on targeted sanctions including financial sanctions, arms embargo and travel ban.

8.2 Extension of obligations

According to section 19H & K of the FIAMLA, a member falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act as well. The prohibition to deal with funds or other assets of a designated party[8] or listed party[9] applies to all persons (including reporting persons which also encapsulate law firms & legal professionals) as per section 23 of the UN Sanctions Act.

In addition, section 24 of the UN Sanctions Act prohibits any person on making funds or other assets available to a designated party or listed party.

Reporting obligations

Where any person holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party, he/she shall immediately notify (section 23(4) UN Sanctions Act) the National Sanctions Secretariat of-

i. details of the funds or other assets against which action was taken against;
ii. the name and address of the designated party or listed party; and
iii. details of any attempted transaction involving the funds or other assets, including-
    - the name and address of the sender

[8] A designated party means any party designated by the National Sanctions Committee under section 9 of the UN Sanctions Act.

[9] A listed party means any party listed by or under the authority of the United Nations Security Council.

- the name and address of the intended recipient
- the purpose of the attempted transaction
- the origin of the funds or other assets
- where the funds or other assets were intended to be sent.

The reporting obligations continue under section 25 of the UN Sanctions Act which says that a reporting person shall immediately verify whether the details of the designated or listed party match with the particulars of any customer and if so, identify whether the customer owns any funds or other assets in Mauritius. A report has to be submitted to the National Sanctions Secretariat regardless of whether any funds or other assets were identified by the reporting person.

Reporting of suspicious information

Pursuant to section 39 of the UN Sanctions Act, any information related to a designated party or listed party which is known to the reporting person should be submitted to the FIU in accordance with section 14 of the FIAMLA.

Internal controls

Section 41 of the UN Sanctions Act states that a reporting person shall implement internal controls and other procedures to enable it to effectively comply with their obligations under this Act.

8.3 Concluding remarks

It is noteworthy to highlight that this chapter has to be read in conjunction with chapter 6-Filing of STRs and chapter 7-Duty of confidentiality and legal professional privilege. The obligations to file an STR when suspecting the financing of terrorism is also mandated under the FIAMLA and UN Sanctions Act. The same legal restriction on tipping off will apply here. Also, disclosures will be compelled by law when suspicion of terrorism financing is identified when conducting the activities listed in the First Schedule of the FIAMLA (see paragraph 7.3).

Chapter 9 Administrative sanctions

According to section 19H of the FIAMLA, a regulatory body shall have such powers as are necessary to enable it to effectively discharge its functions and may, in particular –

a. issue guidelines for the purposes of combating money laundering activities and the financing of terrorism and proliferation activities;
b. give directions to a member falling under its purview to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts;
c. require a member falling under its purview to submit a report on corrective measures it is taking to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts, at such intervals as may be required by the regulatory body.

d. With respect to a member falling under its purview, the regulatory body may apply any or all of the following administrative sanctions –
    i. issue a private warning;
    ii. issue a public censure;
    iii. impose such administrative penalty as may be prescribed by the regulatory body;
    iv. ban, where the regulatory body has licensed or authorised the member to conduct his business or profession, from conducting his profession or business for a period not exceeding 5 years; and
    v. revoke or cancel a licence, an approval or an authorisation, as the case may be.

There are no hard and fast rules on which sanction is more likely to be applied in a given scenario. The following factors will be considered when exercising the power to sanction members falling under the purview of the AGO-

i. nature of the offence;
ii. scale and gravity of the offence;
iii. frequency of re-offending;

iv. have failed to disclose information to a regulatory body when required to do so;

v. have significantly breached the requirements under FIAMLA, FIAML Regulations and UN Sanctions Act;

vi. have failed to comply with the reasonable requests of a regulatory body;

vii. have failed to furnish the regulatory body with any information and/or failed to produce any record or document as requested;

viii. have willfully or by inadvertence obstructed the regulatory body in discharging its duties under FIAMLA, FIAML Regulations and UN Sanctions Act;

ix. have failed to apply CDD and/or Enhanced Due Diligence measures where and when required, especially in relation to PEPs and beneficial owners;

x. have extensive and strategic deficiencies in their policies, internal controls and procedures;

xi. lack of AML/CFT training within an entity structure or at a group wide level;

xii. lack of or significant lack of monitoring in relation to compliance with the FIAMLA, FIAML Regulations and UN Sanctions Act;

xiii. failing to submit STRS when and where required;

xiv. proven record of tipping off and/or reasonable suspicion that tipping off has occurred within an entity or at group wide level;

xv. have failed to comply with the reporting obligations under the FIAMLA, FIAML Regulations and UN Sanctions Act;

xvi. the extent to which members have shown positive and tangible progress after receiving any sanctions; and

xvii. any other factors which the regulatory body may deem relevant whether aggravating or extenuating.

Chapter 10 Enforcement and Penalties

The Mauritius AML/CFT regime has been aligned with international standards in order to make it robust and effective. Breaches of obligations under the regime are backed by disciplinary and criminal penalties. Law enforcement agencies and AML supervisors are working co-operatively with regulated professions to assist with compliance of AML/CFT and increase understanding of how to effectively mitigate risks.

10.1 Supervision in practice

A regulatory body shall-

i. supervise, monitor and give guidance to a member falling under its purview;
ii. cooperate with, and assist investigatory authorities;
iii. exchange information with investigatory authorities and supervisory authorities;
iv. assist and exchange information with overseas comparable regulatory bodies; and
v. undertake and assist in research projects in order to identify the methods and trends of money laundering activities and the financing of terrorism and proliferation activities in Mauritius and in the region (section 19G FIAMLA).

Also, a regulatory body may consult with and seek assistance from any association or body representing a member or any other person as it may deem appropriate.

10.2 Enforcement in practice-Penalties

Financial Intelligence and Anti Money Laundering Act 2002

Section	Description	Penalty
s 8 applicable to PART II only	-Found that the offence of money laundering occurred -Property obtained from the proceeds of crime	On conviction-liable to a fine not exceeding 10 million rupees and penal servitude

	-Conspiracy to commit the offence of money laundering	for a term not exceeding 20 years
s 16	Legal consequences of reporting-tipping off	On conviction-liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years
s 17C (6)	Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements	On conviction-liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 5 years
s 19(1)	Failure to report and keep records and disclose information prejudicial to a request	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 19(2)	(a) Falsifies, conceals and destroys information (b) Divulging that a money laundering investigation is ongoing	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 19E (4)	Failure to provide information when requested by the Ministry for the purpose of conducting ML/TF risk assessment	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 19H (3)	Failure to comply with a direction of the regulatory	On conviction-liable to a fine not exceeding one million rupees and to imprisonment

	body issued under section 19H(1)(b)&(c)	for a term not exceeding 5 years
s 19J (4)	Failure to furnish information requested by your regulatory body	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 2 years
s 19K (5)	During onsite inspection-any person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal of any document, information stored on a computer or other device	On conviction-liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years
s 19M (1)	Non-compliance with directions given under this Act	-Commit a separate offence on each day -On conviction liable to a fine of 5,000 rupees per day in respect to each offence
s 19M (2)	A person knowingly hinders or prevents compliance with a direction given under this Act	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 19W	-Failure to attend without reasonable cause when summoned by the Review Panel -Knowingly gives false evidence -Willfully insults a member	On conviction-liable to a fine not exceeding 100,00 rupees and to imprisonment for a term not exceeding 3 years

	-Willfully interrupts or disturbs the proceedings	
s 32A	Contravention of the FIAMLA	Any person who contravenes this Act, where no specific penalty is provided, on conviction-be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years

Financial Intelligence and Anti Money Laundering Regulations 2018

Regulation	**Description**	**Penalty**
Regulation 33	Contravention of these regulations	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

Section	**Description**	**Penalty**
s 23(5)	Failure to follow a prohibition to deal with funds or other assets of a	On conviction-liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or

	designated party or listed party	other assets, whichever is the greater, and to imprisonment of not less than 3 years
s 24(2)	Failure to prohibit in making funds or other assets available to designated party or listed party available	On conviction-liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is the greater, and to imprisonment of not less than 3 years
s 25(3)	Failure to submit a report to the National Sanctions Secretariat and relevant supervisory authority	On conviction-liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years
s 28(6)	Failure to unfreeze the funds or other assets of a bona fide third party when the Designated Judge has made an order to that effect	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 29(6)	Failure to lift the prohibition when it is so granted by the National Sanctions Committee	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 34(3)	Failure to unfreeze or lift a prohibition of funds or other assets following a lapse of freezing order or prohibition	On conviction-liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years
s 45	Any person who contravenes this Act, where no specific penalty is provided	On conviction-liable to a fine not exceeding one million rupees and to imprisonment

		for a term not exceeding 10 years