

Guidance Notes
on
Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation
for
Legal Practitioners

Issued by the
BVI Financial Investigation Agency
Revised: February 2023

Table of Contents

Table of Acronyms **5**
SECTION 1 Purpose and Scope of these Guidance Notes **10**
SECTION 2 Money Laundering, Terrorist Financing, Proliferation Financing & Legal Practitioners **12**
2.1. Introduction 12
2.2. What is a legal practitioner? 12
2.3. What is Money Laundering? 12
2.4. What is Terrorist Financing? 13
2.5. What is Proliferation Financing? 14
2.6. What does the AML/CFT/CPF regime have to do with legal practitioners? 14
SECTION 3 The BVI Legal Framework to fight Money Laundering, Terrorist Financing and Proliferation Financing 17
3.1. Key BVI AML/CFT/CPF Legislation 17
3.2. Summaries of BVI AML/CFT/CPF legislation 17
3.2.2. Anti-Money Laundering and Terrorist Financing Code of Practice, 2008, as amended 17
3.2.3. Anti-Money Laundering Regulations, 2008, as amended 18
3.2.4. Drug Trafficking Offences Act, 1992, as amended 18
3.2.5. Proliferation Financing (Prohibition) Act, 2021 18
3.2.6. The Terrorism (United Nations Measures) (Overseas Territories Order), 2001 and the Anti- Terrorism (Financial and Other Measures) (Overseas Territories) Order, 2002 18
3.2.7. The Counter-Terrorism Act, 2021 18
3.2.8. The Financial Investigation Agency Act, 2003, as amended 18
3.3. What applies to legal practitioners? 19
3.4. Agencies that supervise and monitor AML/CFT/CPF Activity 19
3.5. Who is the Financial Investigation Agency? Why is it important for you to know? 19
SECTION 4 AML/CFT/CPF Obligations and Requirements for legal practitioners **21**
4.1. Summary of key obligations for legal practitioners 21
4.2. Why do legal practitioners have to fulfill these obligations and follow these requirements? 22
SECTION 5 Appointing a Money Laundering Reporting Officer ("MLRO") **23**
5.1. What is an MLRO and what are their duties and obligations? 23
5.2. What to do when appointing an MLRO? 24
5.3. What happens if you lose your MLRO? 24
SECTION 6 Assessing risk as a legal practitioner to money laundering, terrorist financing and proliferation financing 25
6.1. Institutional risks 26
6.2. Customer/applicant for business risks 26
6.3. Business activities and services risks 27
6.4. Country or jurisdiction risks 28
6.5. Mitigating risk 29
SECTION 7 Customer Due Diligence Measures: Identifying, Verifying and Keeping Records **30**
7.1. What is customer due diligence? 30
7.2. Undertaking risk assessments 31
7.3. Whose information do I have to collect? 32

7.4. What information must I collect and keep? 32
7.5. Verifying identity 34
7.6. What is enhanced customer due diligence ("ECDD")? 34
7.7. When should ECDD measures be applied? 35
7.8. Simplified due diligence – low risk 36
7.9. What if I already know my client because they are well known in the community and/or personally known to me? Do I still have to collect CDD on them? 36
7.10. When do I have to collect the due diligence? 37
7.11. Is there ever an instance where I shouldn't collect due diligence? 37
7.12. Face to Face Versus Non-Face to Face Customer and Applicants for business 38
7.13. Certification of documents for due diligence 38
7.14. What if I cannot get due diligence on the customer/applicant for business? 39
7.15. Monitoring and updating ongoing customer due diligence 40
7.16. Retrospective due diligence - collecting due diligence on business relationships established prior to the enactment of the AML legislation 41
SECTION 8 Record Keeping 42
8.1. What records must a legal practitioner keep? 42
8.1.4. Legal Practitioner's Organisational Records 42
8.1.6. Transaction records 42
8.2. How should the records be kept? 43
8.3. How long must records be kept? 43
SECTION 9 Training 44
9.1. Why is training important? 44
9.2. Who within my firm must be trained? 45
9.3. What should the training be on? 45
9.4. How often should the training take place? 46
9.5. What records of the training must be kept? 46
9.6. Where Can I Get Training? 47
SECTION 10 Reporting Suspicious Activity and Suspicious Transactions 48
10.1. What is suspicious activity? 48
10.2. What is a suspicious transaction? 48
10.3. Unusual vs. Suspicious 48
10.4. Reporting suspicious activity or suspicious transactions 49
10.5. Reporting suspicious activity or suspicious transactions to your MLRO 49
10.6. Reporting suspicious activity or suspicious transactions to the Agency if you are an MLRO 50
10.7. When must I submit an STR? 51
10.8. Must I report attempted business dealings or transactions that are suspicious? 51
10.9. What information should be submitted when I make an STR? 52
10.10. Keeping a register of STRs 52
10.11. What is tipping off? 53
10.12. Consequences of not reporting a suspicion of money laundering, terrorist financing or proliferation financing 53
SECTION 11 Compliance Manual: Creating, Implementing and Following Written Procedures and Controls 55
11.1. Creating, implementing, and following written policies, processes and procedures 55
11.2. What information should be in your compliance manual? 55

SECTION 12 Consequences of non-compliance with the AML/CFT/CPF obligations.....57
12.1. Administrative Penalties under the AML Code 57
12.2. Criminal Penalties under the AML Code..... 59
12.3. Criminal Penalties under the Proceeds of Criminal Conduct Act 60
12.4. Tipping Off Offences for TF under the Counter-Terrorism Act, 2021 61
12.5. Penalties under the Proliferation Financing (Prohibition) Act, 2021..... 61
SECTION 13 Where Can I Get Help? 64
13.2. The Agency 64
13.3. Volunteers and other local resources..... 64
13.4. Private sector businesses and consulting firms..... 64

Table of Acronyms

Agency	Financial Investigation Agency
AML	Anti-money laundering
AML Code	Anti-Money Laundering and Terrorist Financing Code of Practice 2008, as amended
AML Regulations	Ant-Money Laundering Regulations 2008, as amended
BVI	British Virgin Islands
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
CFT	Countering the financing of terrorism
Compliance manual	A written system of internal controls which includes policies, processes and procedures for forestalling and preventing money laundering, terrorist financing and proliferation financing.
CPF	Countering proliferation financing
DNFBP	Designated non-financial businesses and professions. These are businesses defined as undertaking relevant business in the AML Regulations and those defined within the DNFBP Notice.
DNFBP Notice	Non-Financial Business (Designation) Notice, 2008
DTOA	Drug Trafficking Offences Act 1992, as amended
ECDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FATF Recommendations	The Revised FATF Recommendations 2012: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
FIA Act	Financial Investigation Agency Act 2003, as amended
FIU	The Agency's Financial Intelligence Unit
FSC	The BVI Financial Services Commission
KYC/KYD	Know you client/ know your donor
MLRO	Money laundering reporting officer
PEP	Politically exposed person
POCCA	Proceeds of Criminal Conduct Act 1997, as amended
SEU	The Agency's Supervision and Enforcement Unit
SOF	Source of funds
STR	Suspicious transaction report – A suspicious transaction report, which is also referred to as a suspicious activity report, is a form used to file both suspicious activities and suspicious transactions.
Territory	The British Virgin Islands

Glossary of Key Terms

Beneficial Owner - the natural person who ultimately owns or controls a company or legal entity. This can include people who own 10% or more of the shares in a company or entity or those persons who even though not on paper control or will ultimately get the benefit of the company or legal entity.

Customer Due Diligence/CDD - The steps that a legal practitioner is required to take to identify and verify transactions as well as the identities of their customers/applicants for business and any other applicants for business, irrespective of the nature or form of the business.

Caribbean Financial Action Task Force/CFATF - The CFATF is an organisation of states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering, terrorist financing and the proliferation of weapons. The main objective of the CFATF is to achieve effective implementation of, and compliance with, the FATF recommendations.

Enhanced Customer Due Diligence/ECDD - The extra checks and steps a legal practitioner takes to vet and review transactions or customers/applicants for business and any other applicants for business that are considered to have a higher risk to money laundering, terrorist financing and proliferation financing, including transactions or business relationships involving politically exposed persons, jurisdictions that have a higher risk of money laundering or terrorist activity and businesses that have a higher risk of being involved in money laundering, terrorist financing or proliferation financing.

Financial Action Task Force/FATF - An intergovernmental organisation founded in 1989 on the initiative of various countries to develop policies to combat money laundering. In 2001, after the September 11 terrorist attacks in New York City, their purpose expanded to acting on and preventing terrorism financing and proliferation financing. It is made up of representatives from different jurisdictions for the purposes of setting standards and promoting effective implementation of legal and regulatory measures for the forestalling and preventing money laundering and countering the financing of terrorism and proliferation.

The FATF Recommendations - FATF issued their first set of recommendations in 1990 and have amended them several times. These recommendations set, and are recognised as, the international standard on combating money laundering and the financing of terrorism and proliferation, which countries are expected to implement and follow. More specifically to legal practitioners, these recommendations set out what steps countries should take in their supervision and monitoring.

Financial Investigation Agency - The BVI Agency responsible for monitoring and supervising the activities of DNFBPs, NPOs to ensure that they are following and putting into practice BVI anti-money laundering, terrorist financing and proliferation financing laws. The Agency is also the BVI Agency to which suspicions of money laundering, terrorist financing and proliferation financing should be reported.

Financial Services Commission - The BVI statutory body that is responsible for regulating and ensuring that entities in the BVI such as banks, trust companies, insurance companies, and companies buying, selling, or managing securities follow BVI law.

Foreign Regulated Person means a person or company that:

(a) is incorporated, registered, licensed or formed, or has its principal place of business outside the BVI;

(b) carries on business outside the BVI that is similar to business listed as regulated business in the BVI under the BVI AML Regulations and BVI AML Code; and

(i) is subject to legal requirements in its jurisdiction for the detection and prevention of money laundering that are consistent with the requirements of the CFATF Recommendations or FATF Recommendations in relation to that business; and

(ii) is properly and adequately supervised for compliance with those legal requirements by a foreign regulatory authority;

Money Laundering - The process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities and attempt to integrate those illegal proceeds into the normal financial system so that they appear legal and legitimate.

Politically Exposed Person/PEP means a person who is or has been entrusted with prominent public functions or is a member of senior management of an international organisation, including members of his or her immediate family, or persons who are known to be close associates of such a person. PEPs hold positions of power, such as Heads of State/government, cabinet ministers/secretaries of state, judges, military leaders and heads of police and national security services, senior public officials and heads of public utilities/corporations, members of ruling royal families, senior representatives of religious organisations where their functions are connected with political, judicial, security or administrative responsibilities. There are three (3) main types of PEPs, namely:

(a) **foreign politically exposed person**, which means a person who is or has been entrusted with prominent public functions in a jurisdiction outside of the Territory, and includes the family members and close associates of that person;

(b) **domestic politically exposed person**, which means a person who is or has been entrusted with prominent public functions in the Territory, and includes the family members and close associates of that person; and

(c) **international organisation politically exposed person**, which means a person that is a member of senior management of an international organisation and includes the family members and close associates of that person.

i. *Family members* generally cover persons in consanguine and affinity relations with PEPs; these would include, amongst others:

- a spouse;

- a partner considered by national law as equivalent to a spouse;
- a child;
- a spouse or partner of a child;
- a brother or sister (including a half-brother or half-sister);
- a parent;
- a parent-in-law;
- a grandparent; or
- a grandchild.

ii. *Close associates* would include:

- personal advisers/consultants to PEPs;
- close business colleagues and friends likely to benefit from association with, PEPs;
- individuals who have joint beneficial ownership of a legal person or legal arrangement with a PEP; and
- PEP-supported NPOs.

Proliferation Financing – takes place when a person:

(a) makes available an asset,

(b) provides a financial service, or

(c) conducts a financial transaction, and

the person knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended, in whole or in part, to facilitate the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of weapons of mass destruction including nuclear weapons, chemical weapons and biological weapons.

Regulated Person - A person who is licensed or registered by a regulator to carry on: a) banking business; b) insurance business; c) company management business; d) mutual fund business; e) trust or company service provider providing registered office or company formation or directors services; f) money transmission business.

Supervised Entity – Within the BVI, these are entities which are supervised by the Agency for the purposes of forestalling and preventing money laundering and countering the financing of terrorism and proliferation. These are the entities which fall within the NPO and DNFBP categories.

Terrorist Financing means:

(a) using or making funds available for the purposes of terrorism; or

(b) acquiring, possessing, hiding, possession, concealment, converting or transferring funds that are

intended to be used or made available for the purposes of terrorism.

Tipping off - The criminal offence of discussing a suspicion of money laundering, terrorist financing and proliferation financing or a known investigation into money laundering, terrorist financing and proliferation financing with any person who might block, stop, disrupt, or prejudice the investigation or potential investigation.

United Nations Security Council Resolution ("UNSCR") 1373 - UNSCR 1373 was the Resolution passed by the international community in response to the September 11, 2001 terrorist attacks in New York City. Resolution 1373 among other things called on UN member states to ensure that their domestic laws established terrorist acts as serious criminal offences.

United Nations Security Council Resolution 1566: UNSCR Resolution 1566 also dealt with terrorism and, although non-binding on members, the said Resolution defines terrorism as: "*criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act*.

Both UN Resolution 1373 and 1566 apply to the BVI due to its status as a UK overseas territory and provided the framework of what legislation should be within the jurisdiction to deal with the issues of terrorism.

SECTION 1 Purpose and Scope of these Guidance Notes

1.1. These Guidance Notes apply specifically to legal practitioners operating within the Territory who engage in the provision of services to clients which involve transactions concerning any of the following activities:

1.1.1. buying and selling of real estate;
1.1.2. managing of client money, securities, or other assets;
1.1.3. management of bank, savings or securities accounts;
1.1.4. organisation of contributions for the creation, operation or management of companies; and
1.1.5. creation, operation or management of legal persons or arrangements, or buying and selling of business entities.

1.2. Some legal practitioners may draw the conclusion that due to the services their office renders, they do not have any specific AML/CFT/CPF obligations considering they do not engage in any of the functions set out at paragraph 1.1. However, although specific AML/CFT/CPF obligations may not apply to a legal practitioner in such instances, implementing safeguards within the firm to ensure that the legal practitioner's services are not being misused, including by criminals, is consistent with the overall ethics and best practices of the legal profession. Consequently, even legal practitioners that do not engage in the activities specified at paragraph 1.1 should consider what they need to do to guard against that, to not be unwittingly involved in money laundering, terrorist financing or proliferation financing.

1.3. These Guidance Notes exist to assist legal practitioners to better understand the following:

1.3.1. what money laundering, terrorist financing and proliferation financing are and how they relate to legal practitioners;

1.3.2. what BVI government agencies, BVI laws and key terms are relevant to anti-money laundering and counter terrorist financing and proliferation financing in the BVI; and

1.3.3. what a legal practitioner's obligations are in the fight against money laundering, terrorist financing and proliferation financing.

1.4. These Guidance Notes are not law, but they can and should be used side by side with current BVI laws and as a reference for what the Agency considers best practice for the interpretation and implementation of existing BVI AML/CFT/CPF legislative requirements which apply to legal practitioners.

1.5. These Guidance Notes are, therefore, meant to provide industry guidance, practical assistance and a basis to better make legal practitioners able to meet their AML/CFT/CPF obligations.

1.6. For ease of reference, at the end of each Section you will also find the relevant AML Code and legislative references.

1.7. These Guidance Notes should also be considered in the context of applicable legal professional privilege. Legal professional privilege is a protection to the client and a duty to the legal practitioner to protect client information or advice from being divulged. In instances where legal practitioners are claiming legal professional privilege, they must be satisfied that the information is protected by legal professional privilege and the relevant rules.

SECTION 2 Money Laundering, Terrorist Financing, Proliferation Financing & Legal Practitioners

2.1. Introduction

2.1.1. Governments and international bodies like the FATF have seen criminals and terrorists taking advantage of businesses and organisations to further their criminal activities. It is estimated that anywhere between eight hundred billion (US$800,000,000,000) and two trillion dollars (US$2,000,000,000,000) of illegal or criminal money gets into the world economy from criminal activities every year. As a result, international organisations have made several specific recommendations (the main ones generally referred to are the FATF Recommendations) that governments should adopt appropriate AML/CFT/CPF measures, which prevent and stop such criminal activity.

2.1.2. Many governments, including the BVI Government, have implemented these recommendations into law in the form of what we call anti-money laundering and countering the financing of terrorism and proliferation laws. The AML/CFT/CPF laws also specifically apply to legal practitioners, as generally they are known to be targeted by money launderers and other criminals to further their illegal activity. In addition to adopting AML/CFT/CPF laws, the BVI Government has also appointed several Agencies to oversee and monitor organisations to ensure they comply with their AML/CFT/CPF obligations.

2.2. What is a legal practitioner?

2.2.1. In the BVI, a legal practitioner means a person whose name is entered on the Roll in accordance with the Legal Profession Act, 2015.

2.2.2. For the purposes of being subject to specific AML/CFT/CPF obligations, a legal practitioner must be engaging in the activities specified at paragraph 1.1 of these Guidance Notes.

2.2.3. If the activities performed by the legal practitioner fits this definition, he/she will be required to follow and implement certain rules and obligations which are outlined in later sections below.

- **Legal practitioner definition, as provided within the Legal Profession Act, 2015**

2.3. What is Money Laundering?

2.3.1. Money Laundering is the process of integrating illegal proceeds of crime into the legitimate financial system by hiding or concealing its true origin. There are three (3) accepted methods in

the money laundering process, namely, 1) placement, 2) layering and 3) integration. Under the Law, money laundering means the act of concealing, retaining, converting, transferring or in any other way moving funds acquired, directly or indirectly, from an unlawful activity or otherwise from an unlawful source. This includes any activity or offence prescribed as money laundering under the POCCA as well as other legislation. It also includes drug money laundering as defined in the DTOA. Further information on the POCCA and DTOA legislation is given below.

2.3.2. Criminals will hide the fact that their money came from illegal activity in order to get their illegal money into the financial system. If they are known or suspected criminals, they may try to hide the fact that the money is theirs.

2.3.3. The most common ways for criminals to successfully get their illegal money into society is by using the dirty money to start legitimate businesses, passing money through front companies or by purchasing expensive items like land, houses, boats, cars and jewellery.

2.3.4. You should also know that persons can also be considered money launderers if they deliberately assist, facilitate whether by hiding illegal money or activity for a money launderer/criminal, possess or transfer the illegal money or remove it from the Territory. The commission of such acts can result in a fine ranging from $250,000 to $ $500,000 or two (2) to fourteen (14) years imprisonment, or both.

- **Money laundering definition, as provided in the FIA Act**
- **Sections 28, 29, 30 and 30A POCCA**
- **Section 2(1) DTOA**

2.4. What is Terrorist Financing?

2.4.1. Terrorist financing is the use of funds or the making available of funds for terrorist activity. Funds may come from legitimate transactions, profits from business and even charitable organisations. Funds may also be derived from criminal sources, such as the drug trade, fraud, extortion and the smuggling of weapons and other goods.

2.4.2. Terrorist financing includes the acquisition, possession, concealment, conversion or transfer of funds that are directly or indirectly intended to be provided for or used for the purposes of terrorism.

2.4.3. Terrorist financing can also include any type of assistance to help further, sponsor, promote or facilitate terrorism or terrorist activity from providing funds to buying weapons or training or assisting to shelter or buy clothes or transportation for terrorists or even facilitating so that terrorists can broadcast or hand out leaflets to promote their terrorist ideologies.

2.4.4. Therefore, the money used in financing or funding terrorism can be from legal or illegal sources. In fact, often terrorists and those who fund terrorists get their funding from perfectly legal sources. Due to the nature of terrorists' activities, terrorists are more concerned with hiding where their money might be going and what their money will be used for. Terrorist financing is a crime, so is helping to facilitate it.

- **Terrorist financing definition, as provided in the FIA Act**

2.5. What is Proliferation Financing?

2.5.1. Proliferation financing is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, in contravention of national laws or international obligations.

2.5.2. Proliferation of weapons of mass destruction can take many forms but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

2.5.3. To combat this crime, targeted financial sanctions relating to the prevention, suppression and disruption of proliferation financing should be implemented, according to the FATF recommendations. Targeted financial sanctions mean asset freezing and prohibitions, without delay, to prevent funds or other assets from being made available, directly or indirectly, for the benefit of the designated persons and entities.

2.5.4. The AML/CFT/CPF regime is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation.

- **Proliferation financing definition, as provided in the Proliferation Financing (Prohibition) Act, 2021**

2.6. What does the AML/CFT/CPF regime have to do with legal practitioners?

2.6.1. The FATF in assessing risks and vulnerabilities determined that legal practitioners are susceptible to being used not only in the layering and integration stages of the money laundering process, but also as a means to disguise or conceal the origin of funds before placing said funds into the financial system. Legal practitioners are often the first professionals consulted for general business advice

and on a wide range of regulatory and compliance matters.

2.6.2. The FATF characterises legal practitioners as "gatekeepers" because they "protect the gates of the financial system" through which potential users must pass in order to succeed. Gatekeepers have the ability to allow illicit funds into the financial system, whether knowingly or not. The term comprises professional experts who provide financial expertise to launderers, such as legal practitioners, accountants and trust and service company providers. The FATF has noted that gatekeepers are a common factor 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 and to avoid detection. FATF's recommendation 22 acknowledges the role that such gatekeepers can play by recommending that such professions have AML/CFT/CPF responsibilities when engaged in specific activities.

2.6.3. Consequently, legal practitioners must see AML/CFT/CPF policies and procedures as part of their operational practice. This is important because the consequences of participating in money laundering activity or the financing of terrorism or proliferation or failing to prevent one's practice from being used in furtherance of such activity, are rather severe.

2.6.4. The AML Code and the AML Regulations apply to Designated Non-Financial Businesses and Professions ("DNFBPs") in the same manner as they apply to financial institutions. Consequently, the duties contained in the legislation for financial institutions, also form part of the responsibilities of legal practitioners and other DNFBPs. This therefore requires legal practitioners to keep customer records and perform due diligence procedures in seeking to properly know their customers/applicants for business. Legal practitioners are also duty bound to submit suspicious transaction reports to the Agency, when the need arises. In order to make a proper judgment in this regard, legal practitioners will need to avail themselves of training opportunities so that they would be properly equipped to protect themselves and their practices.

2.6.5. The issue of attorney-client privilege looms greatly over the responsibility of legal practitioners to report their clients' suspicious activity to the authorities. This Guidance Note does not intend to compromise this important principle of the legal profession. However, the law is blind when it comes to determining the profession of a person engaged in a money laundering enterprise or a terrorist financing act, or a professional who fails to report such activity.

2.6.6. It is imperative to state here that the AML/CFT/CPF regime understands that as part of the right to an effective legal defence, a client must be free to disclose the circumstances of his or her case fully to his or her legal representative, without fear of counsel divulging such information, shared in confidence, to any authority. However, one does not anticipate that this will include counselling in money laundering, terrorist financing, proliferation financing or the furtherance of any other criminal purpose.

2.6.7. It is worth emphasizing and reiterating that the anti-money laundering responsibilities of a legal practitioner arise only in the circumstances specified at paragraph 1.1 of these Guidance Notes and not to the general practice of all aspects of legal practice.

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

SECTION 3 The BVI Legal Framework to fight Money Laundering, Terrorist Financing and Proliferation Financing

3.0.1. As noted above, the BVI has in place a legislative framework to fight money laundering, terrorist financing and proliferation financing that has incorporated and adopted international standards and recommendations. The framework includes legislation and guidelines for supervised entities, including legal practitioners. It also includes the establishment of supervisory bodies to monitor and ensure that the laws and standards are being adhered to.

3.1. Key BVI AML/CFT/CPF Legislation

3.1.1. For a legal practitioner operating within the Territory, the key BVI AML/CFT/CPF legislation are as follows:

- Proceeds of Criminal Conduct Act, 1997, as amended;
- Anti-Money Laundering/Terrorist Financing Code of Practice, 2008, as amended;
- Anti-Money Laundering Regulations, 2008, as amended;
- Drug Trafficking Offences Act, 1992, as amended;
- Proliferation Financing (Prohibition) Act, 2021;
- The Terrorism (United Nations Measures) (Overseas Territories) Order, 2001;
- Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order, 2002;
- Counter-Terrorism Act, 2021; and
- Financial Investigation Agency Act, 2003, as amended

3.2. Summaries of BVI AML/CFT/CPF legislation

3.2.1. Proceeds of Criminal Conduct Act, 1997, as amended

POCCA is the primary anti-money laundering legislation from which many of the other specific AML legislation derives. The POCCA defines money laundering within BVI legislation and criminalises tipping off, which is where a person knows or suspects that an investigation is or is about to be conducted into money laundering and discloses information to any other person which is likely to prejudice the investigation. The POCCA also makes it a crime not to report a suspicion of money laundering.

3.2.2. Anti-Money Laundering and Terrorist Financing Code of Practice, 2008, as amended

The AML Code is the BVI anti-money laundering, counter terrorist financing and proliferation financing legislation that spells out in detail what a legal practitioner performing the activities at paragraph 1.1, its management and staff are required to do to combat money laundering, terrorist financing and proliferation financing.

3.2.3. **Anti-Money Laundering Regulations, 2008, as amended**

The AML Regulations set out the majority of institutions and organisations that are required to adopt AML measures and adhere to the BVI AML legislation. The AML Regulations also outlines the basic obligations an institution or organisation must meet to fulfill their AML obligations including establishing and maintaining identification and verification procedures, maintaining records and transactions, appointing an MLRO, ensuring staff are trained and establishing procedures in relation to suspicious transactions.

3.2.4. **Drug Trafficking Offences Act, 1992, as amended**

The DTOA, as the name suggests deals with crimes that come about as a result of drug trafficking. The DTOA also gives the authorities the right to confiscate or take away any property or proceeds that are proved to have come from drug trafficking or related offences.

3.2.5. **Proliferation Financing (Prohibition) Act, 2021**

The Proliferation Financing (Prohibition) Act, 2021 is a piece of legislation that makes provision for the prevention of the proliferation of weapons of mass destruction and ensures the implementation of financial measures relating to counter-proliferation Resolutions of the United Nations. The Proliferation Financing (Prohibition) Act, 2021 confers functions on the Agency such as monitoring and assessing the level of risk of proliferation financing in the Territory and taking appropriate measures to address such risk.

3.2.6. **The Terrorism (United Nations Measures) (Overseas Territories Order), 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order, 2002**

The Terrorism Orders refer generally to terrorist type offences and imposes penalties for such offences. Therefore, if a legal practitioner takes funds from a terrorist or provides goods or services that are later used to engage in terrorist activity, the legal practitioner may be committing an offence.

3.2.7. **The Counter-Terrorism Act, 2021**

The Counter-Terrorism Act, 2021 is domestic legislation that criminalises terrorism and the financing of terrorism, and makes provision for the detection, prevention, prosecution, conviction of terrorist activities within the Virgin Islands, and to give effect to several international Conventions and Resolutions for the countering of terrorism and terrorist financing.

3.2.8. **The Financial Investigation Agency Act, 2003, as amended**

The FIA Act is the BVI legislation that established the Agency as an autonomous Agency and outlines its powers and authority. It also outlines the Agency's supervisory responsibility for legal practitioners.

3.3. **What applies to legal practitioners?**

3.3.1. The laws which apply directly to legal practitioners and provide guidance with respect to their AML/CFT/CPF obligations are as follows:

3.3.2. The **AML Code** and **AML Regulations** spell out in detail what a legal practitioner is required to do to combat money laundering, terrorist financing and proliferation financing. The AML Code and AML Regulations apply specifically to legal practitioners that are engaged in the activities specified at paragraph 1.1 of these Guidance Notes.

3.3.3. Therefore, any legal practitioner that performs any of the activities specified at paragraph 1.1 of these Guidance Notices will be required to establish internal control systems, as set out in the AML Code and AML Regulations. The internal control systems (also sometimes referred to as a compliance manual) should comprise employee training, record keeping measures and customer due diligence measures, *amongst other things*.

3.3.4. **The POCCA** is the primary legislation to both the AML Code and AML Regulations, thus making both laws subsidiary legislation. The POCCA specifies the entities and professionals that form vital links in the AML/CFT/CPF regime, which include legal practitioners. The POCCA makes provision for legal practitioners to comply with their AML/CFT/CPF obligations and makes it mandatory for DNFBPs such as legal practitioners to file STRs that involve suspicion of money laundering.

3.3.5. **The FIA Act** is also relevant to legal practitioners because part of the mandate of the Agency is to register, supervise and monitor DNFBPs for AML/CFT/CPF purposes.

3.4. **Agencies that supervise and monitor AML/CFT/CPF Activity**

3.4.1. There are two (2) Government establishments that are primarily involved in the supervision and monitoring of entities for the purposes of AML/CFT/CPF, namely the FSC and the Agency.

3.4.2. The FSC is responsible for the supervision and monitoring of financial institutions including but not limited to banks, trust and corporate service providers and money service businesses. Whereas the Agency is responsible for the supervision and monitoring of DNFBPs and NPOs.

3.4.3. Considering these guidance notes focus on the supervision and monitoring of legal practitioners, the Agency, as the supervisory body for such professionals will be discussed in more detail.

3.5. **Who is the Financial Investigation Agency? Why is it important for you to know?**

3.5.1. The Agency is responsible for supervising and monitoring DNFBPs, which includes legal practitioners, to ensure that they are meeting their obligations to fight money laundering, terrorist financing and proliferation financing.

3.5.2. The Agency is effectively responsible for ensuring compliance by legal practitioners with the requirements of the AML Code, the AML Regulations, and other applicable legislation. The Agency supervises and monitors legal practitioners by reviewing and approving compliance manuals to ensure they meet the requirements in the law; by undertaking outreach with legal practitioners with the objective of protecting them from being used for money laundering, terrorist financing and proliferation financing; and from time to time by performing examinations (inspections) to make sure that legal practitioners are following the policies, processes and procedures required by the AML Code. Ultimately, the Agency in carrying out its supervisory role uses a risk-based approach to determine the level of supervision required for DNFBPs pursuant to the AML Code and the FIA Act.

3.5.3. The Agency is also the body to whom any suspicions of money laundering, terrorist financing or proliferation financing, should be reported, if reporting is deemed necessary. Once the Agency receives an STR, the Agency investigates and analyses the information and takes the necessary action to prevent or attempt to stop money laundering, terrorist financing or proliferation financing from occurring.

3.5.4. The Agency has two departments which deal with each of the above. The Supervision and Enforcement Unit/the SEU is responsible for supervising legal practitioners. It will also undertake outreach and examinations. If a legal practitioner liaises with the Agency with respect to AML/CFT/CPF compliance, chances are it will be with a member of the Supervision and Enforcement Unit.

3.5.5. The Agency also has a Financial Intelligence Unit, also referred to as the FIU. The FIU receives, analyses and investigates STRs submitted to the Agency.

3.5.6. If you have any questions on your AML/CFT/CPF obligations as a legal practitioner, you should contact the Agency's Supervision and Enforcement Unit in the first instance, who will be able to provide further guidance.

3.5.7. If you have any questions on STR filing, you should contact the Agency's FIU.

SECTION 4 AML/CFT/CPF Obligations and Requirements for legal practitioners

4.0.1. International recommendations, the BVI Government and the BVI legislation on AML/CFT/CPF all outline ways that are proven to help deter and detect instances of money laundering, terrorist financing and proliferation financing. These all form the basis of your AML/CFT/CPF obligations and the requirements which must be followed and implemented by a legal practitioner.

4.0.2. These Guidance Notes will now take you through the specifics of your current obligations as a legal practitioner.

4.0.3. To provide additional clarity, we have summarised the key AML/CFT/CPF obligations for legal practitioners. This section will then cover each of these in further detail.

4.1. Summary of key obligations for legal practitioners

4.1.1. As noted previously, if you as a legal practitioner perform the activities specified at paragraph 1.1 above, then based on legislation, you are required to implement certain policies, processes and procedures to prevent you or your firm from being used by money launderers and financiers of terrorism or proliferation to further their illegal agendas.

4.1.2. These requirements are there because they have been proven to make it more difficult for and potentially stop money launderers and terrorists. Even in instances where money launderers and terrorists are not stopped, these steps often allow the authorities to become aware of illegal activity, investigate the criminals and eventually identify them. Following these steps will also help to protect you as a legal practitioner, as it will show that you have taken the required steps to ensure that you are not involved in money laundering, terrorist financing or proliferation financing.

4.1.3. As a legal practitioner operating within the Territory, the following are **critical** for you to do to meet your obligations:

4.1.3.1. Put in place and maintain a written and effective system of internal controls which provides appropriate policies, processes and procedures for forestalling and preventing money laundering and countering the financing of terrorism and proliferation (a compliance manual). From time to time the Agency's SEU may ask to review the said manual;

4.1.3.2. Conduct periodic reviews of your compliance manual;

4.1.3.3. Appoint a Money Laundering Reporting Officer, in accordance with the requirements of the AML Regulations;

4.1.3.4. Assess the risk you as a legal practitioner may face from funds linked to money launderers/terrorists and/or be used to fund or support terrorist activity as well as funds

linked to the financiers of proliferation of weapons of mass destruction;

4.1.3.5. Undertake due diligence on your customers and applicants for business;

4.1.3.6. Maintain records including records of transactions, financial transactions and suspicious transactions;

4.1.3.7. Provide training and awareness on money laundering, terrorist financing and proliferation financing obligations as well as your policies, processes and procedures in relation to these and maintain an on-going training programme for themselves and all persons working in your firm;

4.1.3.8. Report suspicions of money laundering, terrorist financing and proliferation financing to the Agency; and

4.1.3.9. When you have a suspicion of money laundering, terrorist financing or proliferation financing activity, do not "tip-off". In other words, do not say anything about that suspicion to the person who is the subject of the suspicion or to anyone who might reveal to them that they are the subject of an investigation or that an STR has been filed on them.

4.2. Why do legal practitioners have to fulfill these obligations and follow these requirements?

4.2.1. It is imperative that you fulfill these obligations because if you fail to do so you can be fined or in some cases imprisoned for failing to comply. Such failure can also cause reputational damage, not only to you but to the BVI as a whole.

4.2.2. Additionally, if you can meet your obligations and can demonstrate that you follow all the requirements as provided by law, then in the event, you as a legal practitioner, for some reason, becomes involved in a situation involving money laundering, terrorist financing or proliferation financing, you may have a defense against prosecution.

SECTION 5 Appointing a Money Laundering Reporting Officer ("MLRO")

5.1. What is an MLRO and what are their duties and obligations?

5.1.1. A legal practitioner is required to appoint from within its staff an MLRO. The MLRO is responsible for ensuring AML/CFT/CPF compliance by staff and is the one who implements the AML/CFT/CPF requirements including those mentioned above.

5.1.2. The MLRO is responsible for:

5.1.2.1. ensuring AML/CFT/CPF compliance by staff of the legal practitioner and implements procedures, policies and internal controls to deter and detect money laundering, terrorist financing and proliferation financing;

5.1.2.2. carrying out risk assessments on the customers and applicants for business;

5.1.2.3. ensuring that staff are properly trained on and aware of issues, legislation and internal policies and procedures relating to AML/CFT/CPF;

5.1.2.4. being the first point of contact regarding AML/CFT/CPF issues and communicating and liaising with the Agency on behalf of the legal practitioner;

5.1.2.5. reporting suspicious transactions and suspicious activity to the Agency;

5.1.2.6. maintaining a register of money laundering and suspicious transaction reports and inquiries from the Agency.

5.1.3. Additionally, the MLRO is the person to whom any suspicions of money laundering, terrorist financing or proliferation financing activity should be reported. The MLRO is also responsible for investigating and asking appropriate questions to determine whether internally reported unusual or suspicious activity rises to a suspicion of money laundering, terrorist financing or proliferation financing that should be reported to the Agency.

5.1.4. It is not obligatory that the MLRO pass on to the Agency all STRs the MLRO receives. Prior to filing an STR with the Agency, the MLRO should analyse every STR they receive internally and apply judgment based on the facts, the statutory obligations, current policies and internal controls regarding the AML/CFT/CPF obligations of the legal practitioner, to determine if an internal reported suspicion should result in an STR filing to the Agency. There may be instances, where after investigation, an MLRO finds that there were reasonable explanations for what at first appeared to be suspicious activity, and therefore decides that an STR to the Agency is not required. In these instances, the MLRO should document the analysis and investigation they did and make a note as to why they believe they are justified in not making a report to the Agency.

5.1.5. However, it is important to know that if the MLRO in analysing the internal STR is uncertain that

the report amounts to suspicious activity, the STR filing should be made to the Agency.

5.1.6. Moreover, the MLRO liaises with and corresponds with the Agency and responds to any requests for information the Agency may make regarding the activities of the legal practitioner.

5.2. What to do when appointing an MLRO?

5.2.1. When appointing an MLRO, you must ensure that the MLRO understands your activities and your customers. The person should have an understanding of the BVI's AML/CFT/CPF legislation and the requirements in the said legislation.

5.2.2. Due to the serious nature of money laundering, terrorist financing and proliferation financing and the consequences of not following the legislation or accidentally becoming involved in money laundering, terrorist financing or proliferation financing, the person appointed as MLRO, must have the following:

5.2.2.1. sufficient seniority, meaning that the person appointed must be at a senior management level and is fit and proper for the position and capable of fulfilling the role;

5.2.2.2. appropriate qualifications in accordance with the AML Regulations requirements;

5.2.2.3. a good knowledge and understanding of AML/CFT/CPF matters and BVI AML/CFT/CPF laws; and

5.2.2.4. independence in the performance of his or her duties and not subject to any undue internal or external influence or pressure.

5.2.3. The MLRO should also be able to communicate with, and report to, the Board of Directors/the firm's management and the Agency and must have enough time and resources to fulfill his or her obligations.

5.3. What happens if you lose your MLRO?

5.3.1. If your MLRO permanently leaves your firm or for some reason stops holding the position of MLRO, you must write to the Agency within fourteen (14) days of the date when your MLRO stops holding the position and replace your MLRO as soon as possible.

- **Regulation 13 of the AML Regulations**
- **Sections 11, 13, 14 and 16 of the AML Code**

SECTION 6 Assessing risk as a legal practitioner to money laundering, terrorist financing and proliferation financing

6.0.1. A key element of being able to forestall and prevent money laundering and counter the financing of terrorism and proliferation is assessing your risk exposure to same.

6.0.2. This means looking at your firm, its activities, objectives, services provided, customers, applicants for business and transactions and considering what level of risk they may pose to money laundering, terrorist financing or proliferation financing. This will often be determined as High, Medium or Low risk.

6.0.3. The risk level will in turn help you to determine the level of internal controls you need to put in place to manage the risks posed.

6.0.4. Where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. However, where the money laundering/terrorist financing/proliferation financing risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT/CPF controls should apply.

6.0.5. Assessing risks requires you as a legal practitioner to have a sound understanding of the money laundering/terrorist financing/proliferation financing risks in general and those applicable to your profession. You should also be able to exercise good professional judgment. Above all, legal practitioners should recognise the importance of a culture of compliance across their firms and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of their law firms. This requires the allocation of necessary resources to gather and interpret information on money laundering/terrorist financing/proliferation financing risks, both at the country and institutional levels, and to develop procedures and systems.

6.0.6. In addition to assessing the overall risks your firm may be exposed to when it comes to money laundering, terrorist financing and proliferation financing, you must also undertake a risk assessment of every customer and applicant for business, where they meet the due diligence thresholds. Further details on this are provided in the Due Diligence section. This section focuses solely on the overall risks you may face as a legal practitioner.

- **Section 11, 12 and 14 of the AML Code**

6.1. **Institutional risks**

6.1.1. An institutional risk assessment is essentially a risk assessment of your business, to evaluate the business' inherent risk exposure to money laundering, terrorist financing and proliferation financing. The AML Code requires legal practitioners to undertake institutional risk assessments in order to determine whether any ML, TF or PF risks exist [to your firm] and to determine what is the best way to manage and mitigate those risks. Additionally, your firm is also required to put in place appropriate AML/CFT/CPF systems and controls based on the risks identified from the institutional risk assessments.

6.1.2. When undertaking an institutional/firm risk assessment, you must ensure that you take into consideration all products and services provided by your firm; how you provide those products and/or services; your customers and applicants for business; the countries with which you may deal with or your customers are affiliated with as well as any other relevant risks, which may apply.

6.1.3. You must also ensure that, prior to the launch or use of a new product, service, business practice, delivery mechanism or technological development, you must identify any money laundering, terrorist financing or proliferation financing risks from the same; and take relevant and adequate mitigation measures and steps.

6.1.4. All risk assessments **must** also be documented – the Agency can request these at any time, including at the time of an examination.

6.2. Customer/applicant for business risks

6.2.1. There are a number of issues that may point to a high-risk customer/applicant for business, such as:

6.2.1.1. Reluctance to provide relevant information or you having reasonable grounds to suspect that the information provided is incorrect or insufficient;

6.2.1.2. Where a considerable part of their business or affiliations are in countries that may pose higher geographic risk;

6.2.1.3. The structure or nature of the company or relationship makes it difficult to identify the true beneficial owner or controlling interests or customers attempting to obscure understanding of their business, ownership or the nature of their transactions;

6.2.1.4. PEPs and/or their family members and close associates;

6.2.1.5. Customers/applicants for business who have funds that are clearly and inexplicably disproportionate to their circumstances (e.g., their income, wealth or occupation); and

6.2.1.6. Titling a residential property or business venture in the name of a third party (e.g., a

friend, relative, business associate or another legal practitioner).

6.2.2. Some questions that you should consider to determine customer/applicant for business risks are as follows:

6.2.2.1. Who are your customers? Are they high risk?

6.2.2.2. Are your customers, individuals or companies? If they are companies, do you know who owns the companies or makes the decisions?

6.2.2.3. If your customers are companies, are they regulated and required to follow the same or similar AML/CFT/CPF laws?

6.2.2.4. Do your customers live locally or overseas?

6.2.2.5. How well do you know them? Do you know them personally or are they complete strangers?

6.2.2.6. Do you transact your business with them face-to-face or non-face to face (by correspondence, over the phone or by internet)?

6.2.2.7. Can you easily verify the information they have given you either because of personal knowledge or reliable documentation or information?

6.2.2.8. Are any of your customers or have any of your customers been previously suspected of illegal/criminal activity?

6.3. Business activities and services risks

6.3.1. The context of the services being offered and delivered is fundamental to assessing risk exposure as some services/business activities will carry a higher risk of money laundering/terrorist financing/proliferation financing. When determining the risks associated with the provision of services related to specific activities, consideration and appropriate weight should be given to the following:

6.3.1.1. Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment;

6.3.1.2. Services where the customer/applicant for business may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client) (e.g. through the firms' general account and/or a personal or business account held by the legal professional himself/herself);

6.3.1.3. Transfer of real estate or other high valued goods or assets between parties in a time

period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason;

6.3.1.4. Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes; and

6.3.1.5. Any other activities which demonstrate suspicious behaviour and do not make professional or commercial sense based on the industry norms and the normal course of business.

6.3.2. Some questions that you should consider to determine business activities and services risks are as follows:

6.3.2.1. What business activities and services does your firm offer?

6.3.2.2. Do these business activities and services carry a higher risk of abuse for the purposes of money laundering, terrorist financing and proliferation financing?

6.3.2.3. Do you often deal with customers or applicants for business who deal in large amounts of cash/monies? Please note cash would include wire transfers, and other types of monetary instruments.

6.3.2.4. Are there any complex or unusual transactions occurring?

6.3.2.5. Does payment for your services come from regulated financial institutions such as banks who themselves are legally required to conduct money laundering, terrorist financing and proliferation financing checks?

6.3.2.6. Do the services you offer allow you to know the customer or applicant for business or are there layers of anonymity where you may not be sure with whom you are doing business or from where the money you are receiving is coming?

6.4. Country or jurisdiction risks

6.4.1. Country or jurisdiction risks of money laundering/terrorist financing/proliferation financing may arise in a variety of circumstances, including from the domicile of the customer or applicant for business, the location of the transaction or the source of funds or wealth.

6.4.2. Countries with AML/CFT/CPF regimes that fall below acceptable standards may be regarded as high risk. Countries which support terrorist activities or are known for significant political corruption are also high risk.

6.4.3. As a legal practitioner, you should be careful when doing business with persons from countries

where, for instance, it is believed that there is a high level of drug trafficking or corruption, and greater care may be needed in establishing and maintaining the relationship or accepting business from such countries. You may also need to put in place additional controls to manage the extra risk the relationship or transaction carries. As a legal practitioner, you should observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, from listed countries and to observe the list of countries published, which lists countries that are non-compliant or do not sufficiently comply with FATF recommendations.

6.4.4. Legal practitioners should therefore have regard to where a transaction or request for their services originated.

6.4.5. Some questions that you should consider to determine country or jurisdiction risks are as follows:

6.4.5.1. Do you do business with customers or applicants for business who reside in or whose money comes from sanctioned countries?

6.4.5.2. Do the countries where you do business follow and implement international rules and standards adopted to fight money laundering, terrorist financing and proliferation financing?

6.4.5.3. Are there high levels of corruption and criminal activity in those countries?

6.5. Mitigating risk

6.5.1. As a legal practitioner, you should implement appropriate measures and controls to mitigate the potential money laundering/terrorist financing/proliferation financing risks for those customers or applicants for business who, as a result of the risk assessment, are determined to be higher risk. These measures should be tailored to the specific risks faced, to ensure the risk is adequately addressed. Paramount to these measures is the requirement for you and appropriate staff to be adequately trained to identify and detect relevant changes in customer activity by reference to risk-based criteria.

6.5.2. The presence of a single risk factor, or even multiple factors, does not necessarily mean that the customer/applicant for business is engaging in money laundering, terrorist financing or proliferation financing activities. As a legal practitioner, you should be familiar with these risk factors, and exercise sound judgment based on your knowledge of the relevant industry, and when a combination of these factors truly raises a red flag, you should know the proper action to take.

6.5.3. In light of this, it is important that you, as a legal practitioner, develop a sound risk management policy that you will follow in all relevant transactions. This policy should document what customer information is required to facilitate a transaction. It should also set out in what circumstances business should be refused.

SECTION 7 Customer Due Diligence Measures: Identifying, Verifying and Keeping Records

7.0.1. The BVI AML/CFT/CPF legislation requires that DNFBPs, which include legal practitioners, conduct Customer Due Diligence/CDD when undertaking what is described as relevant business. For you as a legal practitioner, this means undertaking the services described in paragraph 1.1 above.

7.0.2. CDD measures should allow you, as a legal practitioner, to establish with reasonable certainty the true identity of each of your customers and/or applicants for business.

7.0.3. CDD is a crucial element in the role you can play in helping to identify and combat money laundering, terrorist financing and proliferation financing. Knowing your customer/applicant for business does not mean knowing their name and address. This can only be satisfied by understanding their business and his or her desired relationship with your professional service.

7.0.4. You, as a legal practitioner, are required to apply each of the following CDD measures:

7.0.4.1. Identification and verification of the customer's/applicant for business' identity;

7.0.4.2. Identification of the beneficial owner and taking reasonable measures to verify the identity of that beneficial owner;

7.0.4.3. Understanding the purpose and nature of the business relationship; and

7.0.4.4. On-going due diligence on the relationship.

7.1. What is customer due diligence?

7.1.1. CDD simply means **identifying** the persons with whom you undertake business/transactions with and **verifying** their identity.

7.1.2. **Identifying** your customer or applicants for business (essentially who it is that your firm is doing business with/for) entails having some information about them that lets you know and have an understanding of who they are.

7.1.3. **Verifying** their identity means gathering information and evidence that proves that the information they have provided is true and correct.

7.1.4. You may have previously heard people use the term KYC or Know Your Customer. This is basically used to describe the due diligence process of identifying and verifying. It refers to the process itself knowing who you, as a legal practitioner, are dealing with.

7.1.5. Remember, the purpose of the BVI AML/CFT/CPF legislation is to ensure that neither you nor your

firm inadvertently engage in or assist with money laundering, terrorist financing or proliferation financing. Identifying who you, as a legal practitioner, are dealing with, verifying their identity by getting documents or evidence to confirm who they are, where they live and where their funds come from are measures that protect you and reduces your risk of being involved in money laundering, terrorist financing and proliferation financing. This is an incredibly important step in the fight against money laundering, terrorist financing and proliferation financing as persons may try to hide their true identity – therefore, as a legal practitioner, you must take the necessary steps to establish who your customer actually is.

7.1.6. While you, as a legal practitioner, may be able to obtain the CDD directly by asking the customers/applicants for business to supply the required information, the law also assists you, and allows you to use reliable evidence as well as independent sources of information to identify and verify this information. Therefore, you have several options and means to be able to collect the due diligence you need and meet the legal obligations.

7.2. Undertaking risk assessments

7.2.1. Before you can undertake any type of due diligence on a customer or applicant for business you must first undertake a risk assessment.

7.2.2. The purpose of the risk assessment is to determine the existence of any risks – with the customer/applicant for business or even with that relationship. This will help you identify what type of due diligence you need to undertake; the extent of the information you need to seek and determine how best to manage any specific risks that may arise.

7.2.3. The key requirement being to ensure that there is, at all times, compliance with the AML/CFT/CPF requirements.

7.2.4. Risks come from a variety of factors and from different variables. In considering a customer/applicant for business, you, as a legal practitioner, should consider the potential AML/CFT/CPF risk they pose. You need to consider what they do; their business profile; whether they are based in a jurisdiction which carries a high risk of money laundering, terrorist financing or proliferation financing; whether they are considered a PEP; etc.

7.2.5. There is no exhaustive list of factors to consider, you should look at your firm's risk profile and what kinds of risks you are likely to face – you should then use these to form the basis of your risk assessment, which will guide you in what due diligence to undertake.

7.2.6. Further details on risk assessments and the types of factors you should consider when undertaking a risk assessment are outlined in the AML Code (*explanatory notes to Section 19 of the AML Code*).

- **Section 12 of the AML Code**

7.3. **Whose information do I have to collect?**

7.3.1. You must collect (and keep) due diligence on all your customers and applicants for business that requires you to engage in the activities specified at paragraph 1.1 of these Guidance Notes.

7.3.2. You must also have some information on the source from which the funds for the services rendered were derived. This will often be referred to as identifying the "source of funds". Essentially it means establishing where the funds come from.

7.4. **What information must I collect and keep?**

7.4.1. Individuals

7.4.1.1. You, as a legal practitioner, should obtain relevant information on the identity of your individual customers/applicants for business and seek to verify the relevant information on a risk basis, through the use of reliable, independent source documents, data or information to prove to your satisfaction that the individual is who that individual claims to be; and that they are your actual customer. The relevant information should include:

7.4.1.1.1. Full legal name (including any former name, other current name or aliases used);
7.4.1.1.2. Date of birth;
7.4.1.1.3. Place of birth;
7.4.1.1.4. Nationality;
7.4.1.1.5. Residential address;
7.4.1.1.6. Contact details (telephone number, email address);
7.4.1.1.7. Occupation;
7.4.1.1.8. Place of business or employment; and
7.4.1.1.9. Purpose of business.

7.4.2. Corporate Customers (Companies)

7.4.2.1. Where the customer/applicant for business is **a corporate customer/company,** the relevant information should include:

7.4.2.1.1. Full name of the company;
7.4.2.1.2. Company address (principal place of business);
7.4.2.1.3. Type of business the company engages in;
7.4.2.1.4. Company registration/identification number;

7.4.2.1.5. Date and place of incorporation, registration or formation;
7.4.2.1.6. The address of the registered office in the country of incorporation;
7.4.2.1.7. If applicable, the address of the registered agent of the company to whom any correspondence may be sent;
7.4.2.1.8. Details of the identity of each director of the company, and any persons who own 10% or more of the company; and
7.4.2.1.9. Recent financial information or audited statements, depending on the nature of the transaction.

7.4.2.2. Additionally, you may obtain any other information deemed appropriate. For instance, you may also request the financial statements of parent or affiliate companies or seek evidence that the company is not in the process of being dissolved or wound-up. You should request this information, particularly for non-resident companies, where the corporate client has no known track record, or it relies on established affiliates for funding.

7.4.3. Trusts/Foundation

7.4.3.1. Trust business is typically regarded as inherently risky because of the confidentiality associated with these entities. Where the customer/applicant for business is **a trust or a foundation,** the following relevant information should be obtained:

7.4.3.1.1. Name of the trust/foundation;
7.4.3.1.2. The date and country of establishment;
7.4.3.1.3. The nature and purpose of the trust/foundation;
7.4.3.1.4. Country of establishment;
7.4.3.1.5. Information on any persons appointed as Trustees, settlors or protectors or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;
7.4.3.1.6. Information of person(s) with powers to add beneficiaries, where applicable;
7.4.3.1.7. Information on the person providing the funds, if not the ultimate settlor; and
7.4.3.1.8. If there is an acting agent, their name and address.

7.4.3.2. Ongoing due diligence should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets.

7.4.4. Please note that the above lists are not exhaustive, and you should request any other information considered appropriate and reasonable as further proof of identity based on the circumstances. The requirements placed within the AML Code set a minimum standard for acting in these cases. If you, as a legal practitioner, are of the view, based on the circumstances of your customer, transaction or matter, that additional information must be sought in order to manage any risks, you should seek and record that information.

- **Sections 23 through 28 of the AML Code**

7.5. **Verifying identity**

7.5.1. Verifying identity effectively means confirming that the customers/applicants for business are who they claim to be and that the information they have provided to you is correct. It means having in place documentary evidence which supports and corroborates the due diligence information that the persons have given you.

7.5.2. The documentary evidence of identity can take a number of forms and can come from a number of sources. For example, to verify a person's identity, you may ask for a copy of their passport, which will include their details. Similarly, to verify a company's details, you may ask to see company documentation, which would show this.

7.5.3. The type of documentary evidence that is acceptable will be dependent on the persons you are dealing with as well as the level of risk you determine they pose. The type of documentary evidence to be collected will differ depending on whether the person is an individual, a company, a Trust or a Foundation.

7.5.4. The key thing to always remember is that it is not sufficient for a legal practitioner to rely on a customer's or applicant for business' claim that they are who they say they are. Verification of that information **must** take place.

- **Sections 23 through 28 of the AML Code**

7.6. **What is enhanced customer due diligence ("ECDD")?**

7.6.1. ECDD is the extra due diligence steps a legal practitioner takes when dealing with a customer/applicant for business that presents a higher risk of money laundering, terrorist financing or proliferation financing, irrespective of the nature or form of the transaction.

7.6.2. These extra measures or ECDD are designed to assist legal practitioners in identifying, considering and ensuring that they can, and are happy to, manage the increased risk associated with a higher risk transaction. They allow legal practitioners to take extra steps and precautions to reduce the likelihood that they may inadvertently aid in money laundering, terrorist financing or proliferation financing.

7.6.3. ECDD measures include:

7.6.3.1. Having an increased level of awareness and knowledge about the persons with whom you are transacting. Often, this means doing additional public searches and having available more relevant news and publicly available information, (positive, negative or neutral), which helps the legal practitioner decide whether or not they want to do business or take money from the customer.

7.6.3.2. Escalating internal approval to ensure that senior managers are aware of the higher risk a transaction poses and approve doing business or taking funds from them.

7.6.3.3. Increasing your controls and ongoing monitoring of the higher risk relationships.

7.7. When should ECDD measures be applied?

7.7.1. ECDD should be applied in instances where a customer or applicant for business presents a higher risk or is deemed to carry a higher risk of money laundering, terrorist financing or proliferation financing, irrespective of the nature or form of the relationship or transaction. Each legal practitioner will have its own criteria for determining risk ratings and what criteria would carry a higher risk.

7.7.2. However, by law, the following are deemed as presenting a higher risk and automatically require ECDD measures to be performed:

7.7.2.1. Foreign PEPs;

7.7.2.2. Domestic or International Organisation PEPs that present a higher risk;

7.7.2.3. Persons, business relationships or transactions located in or from high-risk countries (including countries identified as having higher risk by the FATF) or they have international sanctions, embargoes or other restrictions levied against them; and

7.7.2.4. Any other situation that may present a higher risk of money laundering, terrorist financing or proliferation financing.

7.7.2.5. Business activities or ownership structures that are complex or unusual when compared with the person's normal business activity or transactions that do not appear to have any visible economic or lawful purpose.

- **Section 20 of the AML Code (as well as the guidance notes)**

7.8. **Simplified due diligence – low risk**

7.8.1. BVI law requires that CDD should be collected by legal practitioners, when undertaking transactions outlined in paragraph 1.1 above. As discussed in previous sections, where a business relationship or transaction poses a higher risk to money laundering, terrorist financing or proliferation financing, then ECDD is required. On the other hand, there are instances where you may determine that a business relationship/transaction poses a low risk. Where this is the case, then a legal practitioner can determine that it can reduce or "simplify" the due diligence it needs to undertake. This is also sometimes referred to as simplified due diligence.

7.8.2. In considering whether a relationship or transaction may be considered to pose a lower risk, various factors can be taken into consideration such as:

7.8.2.1. the payment for services is coming from a source of fixed income or salary from a known/confirmed occupation that confirms that the customer has the means to cover the funds required for the legal services;

7.8.2.2. the corporate customer may be part of a group, which is subject to and is supervised for compliance with AML/CFT/CPF requirements; or

7.8.2.3. the legal practitioner determines that the business relationship or transaction poses little or no money laundering/terrorist financing/proliferation financing risk.

7.8.3. A more detailed list of factors is provided in the AML Code, Section 19(6).

7.8.4. In determining whether simplified due diligence is the appropriate step to take, a legal practitioner must first of all determine the risk rating of the business relationship. In doing so, legal practitioners are asked to always remain vigilant to any money laundering, terrorist financing and proliferation financing risk factors.

- **Sections 19(6) and (7) of the AML Code**

7.9. **What if I already know my client because they are well known in the community and/or personally known to me? Do I still have to collect CDD on them?**

7.9.1. As noted above, it remains a fundamental part of an effective anti-money laundering and counter terrorist financing and proliferation financing regime, that a customer or applicant for business is identified, and due diligence undertaken on them. This remains the case even if you know them personally. In essence, the AML Code requires that you collect appropriate and relevant due diligence information relating to a person's identity and business relationship. However, due diligence rules do allow for simplified due diligence to be undertaken in certain circumstances and you can consider whether this would be appropriate.

7.9.2. It is also important to keep in mind that, at any given time, the police or the Agency may ask to see the documentation you hold on file for a customer/applicant for business. It would not be sufficient to say you did not gather the due diligence because you know the customer/applicant for business personally. You will be required to produce this documentation, and if you are unable to do so, there may be legal implications for you and your firm.

7.10. **When do I have to collect the due diligence?**

7.10.1. You should undertake a risk assessment and obtain CDD/ECDD **before** effecting a one-off transaction which involves funds of $15,000 or above or **at the time of** establishing a business relationship**.**

7.10.2. Additionally, you must also undertake due diligence:

7.10.2.1. when there is a suspicion of money laundering, terrorist financing or proliferation financing, regardless of whether or not the threshold is met or whether or not the risk rating is low;

7.10.2.2. when there are doubts about previously obtained due diligence data; and

7.10.2.3. when the risk rating of any business relationship changes and presents a higher risk than it did before.

7.10.3. Since a review of the information provided during the due diligence process is what often triggers a suspicion of money laundering, terrorist financing or proliferation financing, should a suspicion of money laundering, terrorist financing or proliferation financing arise during that process, you should refuse to engage in services with the potential customer/applicant for business, so that you do not handle potentially illegal or criminal funds and so that you don't accidently become involved in money laundering, terrorist financing or proliferation financing. At this stage, you should also consider whether an STR should be filed with the Agency (further details of this are provided below).

- **Section 19(4) of the AML Code**

7.11. **Is there ever an instance where I shouldn't collect due diligence?**

7.11.1 You should not collect customer due diligence in circumstances where you suspect that a transaction relates to money laundering, terrorist financing or proliferation financing, and you believe that performing customer due diligence will tip-off the customer. In such instances, you

should refrain from collecting customer due diligence on the customer and instead you should file an STR with the Agency.

- **Section 19(9) of the AML Code**

7.12. **Face to Face Versus Non-Face to Face Customer and Applicants for business**

7.12.1. It is generally agreed that non-face to face transactions are riskier than face-to-face transactions. Where a customer/applicant for business with whom you are transacting is face to face, it allows you to ensure that their physical identity matches the identification documentation presented. This generally makes verification easier and more reliable than if they were to send documents without ever being physically seen or known.

7.12.2. If, however, a customer/applicant for business is not face to face or generally unknown to a legal practitioner, there may be difficulties in verifying their identity and there may be issues surrounding the reliability of the information presented by them. In these types of circumstances, the legal practitioner will still be required to follow the due diligence protocols and take **any additional measures** as may be necessary to complete identification and verification. In doing so, you must also keep in mind the overall risk profile of the customer/applicant for business.

7.12.3. One such additional measure is requiring certified documentation to be presented.

- **Section 29 of the AML Code**

7.13. **Certification of documents for due diligence**

7.13.1. As noted above, if you are involved in a transaction which is being undertaken on a non-face to face basis, you will be relying on copies of documents in order to complete the required identification and verification.

7.13.2. To clarify, where you have not physically seen the actual original documentation, then it is considered a copy of the document. Where this occurs, and you have concerns about the authenticity of the document or you have a concern in general about the transaction, you may ask for the documents to be certified.

7.13.3. There is certain language that must be present on documents and certain requirements that must be met for them to be considered properly certified. They are as follows:

7.13.4. Documents should be certified by professionals who are subject to professional rules of conduct, oaths, or statutory obligations, which if breached, would make them subject to fines or penalties. Professions generally accepted as meeting those criteria include:

7.13.4.1. judicial officer/senior public officers like a police officer or immigration officer or a registrar;
7.13.4.2. a legal practitioner, medical practitioner or accountant or any profession with established rules of professional conduct;
7.13.4.3. a notary public or commissioner for oaths;
7.13.4.4. a director, manager or senior officer of a licensed business, including Banks and Trust Companies.

7.13.5. The person certifying must be independent from the person whose documents they are certifying (e.g. the certifier should not be related to the person whose documents they are certifying);

7.13.6. The person certifying the documents should include the date they certify the document and any other required information, sign their name to the documents, and provide adequate information including position and contact details or official registration/license number so that they can be located or contacted in the event of a query regarding the certification.

- **Section 30 of the AML Code**

7.14. **What if I cannot get due diligence on the customer/applicant for business?**

7.14.1. If a customer or applicant for business emphatically and categorically refuses to provide you with the due diligence you have requested, this can be a red flag for suspicious activity or a suspicious transaction of money laundering, terrorist financing or proliferation financing.

7.14.2. Refusal to provide due diligence where there is no reasonable explanation for such refusal, is often linked to an attempt to disguise true ownership or avoid detection where there is some criminal or money laundering activity.

7.14.3. In such instances, the law requires that the legal practitioner should file an STR with the Agency. This would generally be undertaken by the legal practitioner's MLRO.

7.14.4. The requirement to file an STR with the Agency also applies where a customer/applicant for business fails to provide adequate due diligence information or evidence to verify their identity.

7.14.5. You should, however, look at every situation and every customer/applicant for business independently to determine if there are reasonable factors why they cannot, or are unable to, provide you with the due diligence information or if you can find another way to verify the

information they are providing. For instance, there may be circumstances where some customers or applicants for business are unable to supply the identity documents. Such customers or applicants for business can include a minor, the elderly, the disabled and individuals that are dependent on the care of others. As the legal practitioner, you will have to determine what alternate identity documentation to accept and what verification procedures to employ.

7.14.6. If you are able to verify the due diligence by other independent, reliable means, and you are satisfied that there is no activity relating to money laundering, terrorist financing or proliferation financing, you can continue with the transaction.

7.14.7. However, as a general rule if a customer/applicant for business refuses to give you the required due diligence and there is no sensible reason for this refusal, you should not proceed and you should file an STR with the Agency.

- **Sections 13, 18(3), 23(2C) of the AML Code**

7.15. **Monitoring and updating ongoing customer due diligence**

7.15.1. In instances where you have an ongoing business relationship with customers/applicants for business, you will need to monitor and update ongoing customer due diligence information from time to time.

7.15.2. You as a legal practitioner, should conduct ongoing customer due diligence on your business relationships by scrutinizing the transactions undertaken by each customer or applicant for business throughout the course of the relationship; screening to identify the customers and applicants for business that may present a higher risk; and reviewing and updating the customer due diligence information, including information on beneficial ownership. The review and update of the customer due diligence information must be done on a risk sensitive basis, prioritizing the review and update of customers or applicants for business that present a higher risk and upon certain trigger events as determined by senior management of your firm. Since a customer or applicant for business that presents a higher risk is more at risk of potentially being involved in money laundering, terrorist financing or proliferation financing, you will want to monitor them more closely to ensure that there is no information that comes out in the public domain that would make you want to change your mind about accepting that customer or applicant for business. In certain circumstances, you may even consider whether putting in place ongoing monitoring systems would be appropriate.

7.15.3. Please note that in the event you suspect that a customer/applicant for business, may be involved in money laundering, terrorist financing or proliferation financing, or engages in activity that causes a suspicion of same, you **must** take action immediately, whether they are deemed to present a higher risk or not. You must review the customer and the transactions, address your suspicions, and take the necessary action.

7.15.4. Always remember that the duty to report suspicious activity or a suspicious transaction to the Agency is an ongoing one.

- **Section 21 of the AML Code**

7.16. **Retrospective due diligence - collecting due diligence on business relationships established prior to the enactment of the AML legislation**

7.16.1. Legal practitioners have been required to have anti-money laundering and counter terrorist financing measures mentioned in these guidance notes since the AML Code and AML Regulations came into effect ***on 22 February 2008***.

7.16.2. As such, financial record keeping, customer identification information, due diligence and transaction records and all other obligations required under the BVI AML legislation should have been implemented from those times.

7.16.3. The Agency is aware that in practice there may be instances where business relationships were established prior to the enactment of the AML legislation. However, if the business relationship was still in existence after the enactment of the said legislation, the Agency will require a legal practitioner to collect due diligence in those circumstances.

7.16.4. It is therefore expected that all legal practitioners have obtained the required customer due diligence and records and have implemented AML/CFT/CPF measures on all active business relationships even in circumstances where the business relationship started prior to the enactment of the relevant legislation.

SECTION 8 Record Keeping

8.1. What records must a legal practitioner keep?

8.1.1. All legal practitioners must comply with the record keeping requirements outlined within the AML Code. The documents you are required to keep, range from AML documents to other more general transactional and financial records. Ultimately, you must ensure you keep and maintain all necessary records and transactions relative to your dealings.

8.1.2. The types of records legal practitioners are required to keep are:

8.1.2.1. Copies of all "internal" STRs made to the MLRO;
8.1.2.2. Copies of all "external" STRs made to the Agency;
8.1.2.3. Internal policies and procedures i.e. your compliance manual;
8.1.2.4. Records of any large, unusual or complex transactions;
8.1.2.5. Records of transactions with customers and applicants for business; and
8.1.2.6. Details of any AML/CFT/CPF training completed.

8.1.3. More specifically, legal practitioners must keep:

8.1.4. **Legal Practitioner's Organisational Records**

8.1.5. All legal practitioners must ensure that their firms keep records that show the firm's purposes, objectives and activities; the identity of people who control or direct its activities including board members, directors and managers.

8.1.6. **Transaction records**

8.1.7. Records of transactions undertaken by the legal practitioner must include the name and address; the types of currency and the amount; the beneficiary of the transaction (as well as their name and address); any account details including account number, name and identifier; date of transaction; nature of transaction; and any relevant files and correspondence in relation to the transaction. Any records you keep on a transaction must be sufficiently detailed enough so that the transaction could be understood if reviewed.

8.1.8. Additionally, the records must be able to show and explain the legal practitioner's transactions, within and outside of the Territory.

8.1.9. Financial information should also include enough documentation to show that funds that are earmarked or are planned to be used are in fact spent as they were meant to be.

- **Sections 42 and 44 of the AML Code**

8.2. How should the records be kept?

8.2.1. As a legal practitioner, you must ensure that you keep records in an easily retrievable format, which by extension means that the records must be kept in an orderly, sensible manner so that the records and the information in the records can be easily searched, and produced without delay, if required. A legal practitioner must also be able to provide records promptly when requested by the Agency, the FSC, a law enforcement agency or other person entitled to access them.

8.2.2. Records may be kept:

8.2.2.1. as original copies or certified copies of the original copies;
8.2.2.2. as a scanned copy of the original document, which can be certified; or
8.2.2.3. in a computerized or other electronic format.

8.2.3. It will be up to the legal practitioner to decide how it chooses to store and keep these records. What we would say is you must ensure that the criteria provided within the AML Code and specified above are covered.

- **Section 42 of the AML Code**

8.3. How long must records be kept?

8.3.1. Records must be kept for a **minimum of five (5) years**. For transactions, the time period is five (5) years from the completion of the last transaction or series of transactions.

- **Section 45 of the AML Code**

SECTION 9 Training

9.0.1 All legal practitioners are subject to the Employee Training requirements outlined within the AML Code.

9.0.2 With this in mind, you, as a legal practitioner, are required to ensure that your staff receives appropriate and relevant training so that they understand how your firm can be used in money laundering, terrorist financing and proliferation financing. They should also understand their obligations in relation to the same as well as the firm's policies, processes and procedures for spotting and stopping potential money launderers, terrorist financiers or proliferation financiers from using your firm.

9.0.3 Training should include information to help staff understand what money laundering, terrorist financing and proliferation financing mean and have an understanding of what AML/CFT/CPF laws in the BVI apply to legal practitioners.

9.0.4 Training should be provided and held at an appropriate frequency. The Agency does not stipulate how often you provide this training, as this will really depend on the legal practitioner, its operations and the level of risk involved. However, please be advised that from time to time, the Agency may ask a legal practitioner to give details of training held and provide explanations as to the frequency of training.

9.0.5 The training requirements applicable are not limited to any particular class or rank of staff, although key training requirements will be appliable to some (for example the MLRO).

9.1. Why is training important?

9.1.1. Training is not only a legal requirement, but it is also what allows staff and senior management to understand concepts that might be new to them, like what is money laundering, terrorist financing and proliferation financing. It also helps staff and senior management understand what their obligations are under the law; what the firm's policies, processes and procedures are; how they can identify instances or suspicions of money laundering, terrorist financing and proliferation financing and what they should do if they ever come across instances of money laundering, terrorist financing and proliferation financing.

9.1.2. Your staff are the frontline defence and are critical in deterring, detecting, and preventing money laundering, terrorist financing and proliferation financing. Staff are the ones who generally have customer contact or may ultimately accept or process customers' funds. As such, they are in the best position to notice patterns of behaviour or notice when information about funds gives rise to a suspicion of some illegal activity. One of the most effective ways that we can equip staff is by providing them with regular and effective training. This leaves them with the tools, information and understanding so that they can identify activities that may be money laundering, terrorist financing or proliferation financing.

9.1.3. In addition, ensuring all staff receive the proper training not only aids in the fight against money laundering, terrorist financing and proliferation financing, but it also protects you and your firm from becoming complicit in illicit activity.

9.1.4. It is also important to note that failure to train staff and employees is a breach of legislation that can result in fines and penalties from the Agency.

9.2. Who within my firm must be trained?

9.2.1. It is important to understand the purpose behind these requirements, that is to prevent and forestall money laundering and counter terrorist financing and proliferation financing. All staff within the firm of the legal practitioner are responsible for this. Therefore, all staff should receive some sort of applicable training.

9.2.2. This should include directors, senior management, key staff and any temporary or contract staff, as they are at risk of inadvertently being involved in money laundering, terrorist financing or proliferation financing.

9.2.3. Any new staff joining the firm should also be trained within a reasonable period of time within joining.

- **Sections 47(2) and (3) of the AML Code**

9.3. What should the training be on?

9.3.1. As noted, it is critical to the prevention and detection of ML/TF/PF that staff understands money laundering, terrorist financing and proliferation financing and the issues that arise from those activities. Therefore, training on money laundering, terrorist financing and proliferation financing must enable them to not only recognise suspicious situations, but also to understand how to deal with those situations.

9.3.2. The level of training will depend on the responsibilities of each staff member. For instance, the MLRO, senior management, or directors will require more in-depth anti-money laundering and counter terrorist financing and proliferation financing training than more junior level staff will. Therefore, training should be appropriate for each employee's level and responsibilities.

9.3.3. Training should cover at a minimum:

9.3.3.1. Concepts of money laundering, terrorist financing and proliferation financing so that the staff understands what these are, how they may affect the BVI and the legal practitioner

industry, as well as their role in preventing money laundering, terrorist financing and proliferation financing.

9.3.3.2. Relevant BVI legislation on AML/CFT/CPF, including the provisions of the AML Code and the AML Regulations.

9.3.3.3. The policies, processes, procedures, and internal controls in place within your organisation to deal with and fight money laundering, terrorist financing and proliferation financing.

9.3.3.4. Each person's and the legal practitioner's obligations in fighting, detecting, and reporting suspicions of money laundering, terrorist financing and/or proliferation financing.

9.3.3.5. Understanding suspicious activity/suspicious transaction and what to do when there is a suspicion of money laundering, terrorist financing or proliferation financing.

9.3.3.6. Relevant legal developments, international standards, and legislative changes in the BVI and current and emerging trends in money laundering, terrorist financing and proliferation financing.

9.4. How often should the training take place?

9.4.1. Training should be held at an appropriate frequency. In considering and planning training sessions for your firm, you must consider what is most appropriate for your firm, its operations, size, etc. You should aim for regular training to ensure that all staff are aware of their obligations, as it relates to AML/CFT/CPF.

9.4.2. There is nothing to stop you from having more training, especially for more senior staff who may require additional, more in-depth knowledge or understanding or in the event you need to ensure that your staff have a full understanding of AML/CFT/CPF matters.

9.4.3. As part of its supervisory function, and to provide assistance to legal practitioners, the Agency also regularly holds outreach/training sessions. You should encourage your staff to attend these, where possible.

- **Section 48 of the AML Code**

9.5. What records of the training must be kept?

9.5.1. You must keep a record of the training each staff member receives. In particular, you must keep information on:

9.5.1.1. the date any training was held;

9.5.1.2. the names of the attendees;

9.5.1.3. the duration of the training; and

9.5.1.4. the topics covered in the training.

9.5.2. Many legal practitioners find that the most efficient way to keep these training records are in the form of a training log or register, which also includes any training materials, certificates, tests for any given training, etc.

9.5.3. Training records, similar to all other records you are required to keep, must be kept for a period of at least five (5) years.

- **Sections 45(1) and (3) of the AML Code**

9.6. Where Can I Get Training?

9.6.1. If you have someone knowledgeable within your firm, you may be able to have your own internal workshops or seminars on specific anti-money laundering, terrorist financing and proliferation financing concerns relevant to your industry.

9.6.2. There are also private firms in the BVI that can provide specific training for your firm and staff as well as general online training on AML/CFT/CPF topics.

9.6.3. When you choose a training provider, try to ensure that there is some component that allows you to test or evidence the knowledge you receive from the training. Having a way to demonstrate that you tested your knowledge is an important part of the training requirements in the AML/CFT/CPF suite of legislation.

SECTION 10 Reporting Suspicious Activity and Suspicious Transactions

10.1. What is suspicious activity?

10.1.1. Suspicious activity is hard to define as there is no set definition of this. What is suspicious will be largely dependent on what is normal for your firm in undertaking its general operations and activities. Additionally, you will need to factor in the types of customers and applicants for business your firm deals with. Suspicious activity could refer to any incident, event, individual or activity that seems out of place or at odds with your firm's usual activity. An example of suspicious activity is the reluctance on the part of a potential customer/applicant for business to provide documentation required to conduct CDD/ECDD. Generally, suspicious activity will identify potential instances of money laundering, terrorist financing, proliferation financing or other illegal activity.

10.2. What is a suspicious transaction?

10.2.1. Suspicious transactions are transactions in which there are reasonable grounds to suspect that the funds or goods involved are linked to the proceeds of criminal conduct. This could mean the funds have been derived from an illegal activity (and are being laundered) or are intended to be used for an illegal activity (such as terrorism).

10.3. Unusual vs. Suspicious

10.3.1. There may be instances where customers and applicants for business engage in behaviour that is unusual. Unusual activity or an unusual transaction can be any activity or transaction that deviates from the normal behaviour of the person/business with whom your firm is dealing.

10.3.2. As would be expected, unusual activity or an unusual transaction would raise initial concerns. Staff that are familiar with the customers, their behaviours, and transactions, are likely to be the first to notice unusual activity or an unusual transaction.

10.3.3. Unusual activity or an unusual transaction should not automatically result in the filing of an STR with the Agency. However, it should be a trigger to collect further information and facts to understand the overall picture. The gathering and assessment of additional information should be used to determine whether there is a reasonable suspicion that the customer's behaviour or transaction is somehow linked to money laundering, terrorist financing, proliferation financing and/or other illegal activity or whether there is a reasonable explanation for it. For example, there may be a sudden change in the customer's business or transaction activities. This can be considered as unusual, as there is a deviation from the customer's/applicant for business' usual transactions. However, it may not be suspicious because there may be a reasonable explanation for the deviation.

10.3.4. Suspicious activity or a suspicious transaction on the other hand are effectively an unusual activity or unusual transaction, which despite receipt of additional facts, information and assessment cannot be explained in any logical way, by looking at the facts and circumstances. Based on this, there may be instances where unusual activity or an unusual transaction can amount to suspicious activity or a suspicious transaction.

10.3.5. See also section on Tipping Off below.

10.4. Reporting suspicious activity or suspicious transactions

10.4.1. Under BVI law, all persons including legal practitioners have a duty to report suspicious activity or a suspicious transaction, which they reasonably believe may be linked to money laundering, terrorist financing or proliferation financing to the Agency. This requirement extends to the staff of the firm. However, the requirement on staff is to report the suspicious activity/transaction to the MLRO, who will then take the appropriate next steps.

10.4.2. Within the AML Code, there is a general duty to report suspicious activity or a suspicious transaction under sections 17 and 18. There is also a general duty to report suspicious activity or a suspicious transaction under the Counter-Terrorism Act and the Proliferation Financing (Prohibition) Act.

10.4.3. In addition, there are also specific circumstances outlined within the AML Code, Counter-Terrorism Act and Proliferation Financing (Prohibition) Act, which require an STR to be filed.

10.4.4. Failure to report a suspicion of money laundering, terrorist financing or proliferation financing is a criminal offence.

- **Sections 13(2)(f), 17(2) and 18(7) of the AML Code**
- **Section 60 of the Counter-Terrorism Act, 2021**
- **Sections 34 & 35 of the Proliferation Financing (Prohibition) Act, 2021**

10.5. Reporting suspicious activity or suspicious transactions to your MLRO

10.5.1. There are times when a customer/applicant for business, or a potential customer/applicant for business makes an attempt to conduct business or engage in a transaction that raises your suspicion. Where it seems that the activity or transaction, or attempted activity or transaction gives rise to a suspicion or raises initial concerns that money laundering, terrorist financing or proliferation financing is being attempted or is occurring, this suspicion **must** be reported.

10.5.2. If you are a staff member of the firm, your suspicion must be reported to the firm's MLRO and

should be in writing, in accordance with the firm's procedures. Most often, your firm will already have a form ready for you to use to do this.

10.5.3. Your MLRO will take down the details, obtain further information and make an assessment to determine whether or not they subjectively believe the facts give rise to a suspicion of money laundering, terrorist financing or proliferation financing. This further assessment may involve asking additional questions, obtaining additional customer due diligence, and trying to understand the full circumstances, including the background and the events leading up to and surrounding the potential suspicious activity or suspicious transaction. The aim of the further assessment is to look at the totality of the circumstances to determine whether the customer or their transaction is merely unusual, or whether there are subjective grounds for a suspicion of money laundering, terrorist financing or proliferation financing that would require the filing of an STR with the Agency.

10.5.4. You should note that determining whether or not a transaction results in a suspicion of money laundering, terrorist financing or proliferation financing, is a very subjective matter. If you are in any doubt, you should file a report with your firm's MLRO.

10.5.5. As a staff member, once you have submitted your STR to your MLRO, your duty to report a suspicion will be discharged, provided you follow the firm's protocols in doing so.

- **Sections 17, 18 of the AML Code**

10.6. Reporting suspicious activity or suspicious transactions to the Agency if you are an MLRO

10.6.1. If you are the MLRO within the firm, once you make the determination that there are grounds for a suspicion of money laundering, terrorist financing, proliferation financing or other criminal activity, you are required to submit an STR in writing to the Agency, in the form required by the Agency.

10.6.2. If after a review and analysis of the facts and circumstances, the MLRO is still uncertain as to whether or not the details of an activity or transaction reported to them gives rise to a reasonable suspicion of money laundering, terrorist financing, proliferation financing or some other form of criminal activity, the MLRO should still, and must under the law, file an STR with the Agency.

10.6.3. The MLRO's job is not to investigate and then definitively state that money laundering, terrorist financing or proliferation financing is occurring. On the contrary, the role of the MLRO is to investigate the details of the internal report, collect further information, understand the facts, analyse all of that information and then make an assessment as to whether or not there is enough to support a belief or suspicion of money laundering, terrorist financing, proliferation financing or other criminal activity.

10.6.4. Filing an STR with the Agency and providing the relevant information and reasons for your suspicion or potential suspicion, gives the Agency the ability to investigate and determine whether or not there actually is money laundering, terrorist financing, proliferation financing or some other criminal activity occurring.

10.6.5. Filing an STR also protects the legal practitioner, since the failure to file an STR when facts and circumstances warrant one is an offence under the law. Therefore, if in doubt, file an STR with the Agency.

10.6.6. However, there may be instances when the MLRO decides that the information submitted to them does not substantiate a suspicion of money laundering, terrorist financing or proliferation financing. When this happens, the MLRO must make a record and file the matter internally. This is a crucial step to take when deciding not to externalize an STR with the Agency. This decision must be documented, and a record of the decision kept, in case the Agency seeks further information.

- **Sections 17 and 18 of the AML Code**

10.7. When must I submit an STR?

10.7.1. An STR must be made as soon as is reasonably practicable after you become aware of the suspicious activity or suspicious transaction.

10.7.2. You must always remember that STRs are used by the Agency and law enforcement for the purposes of AML/CFT/CPF. For this to happen, it is imperative that the Agency receives information in a timely manner, so that it can take action before it is too late.

- **Section 30A (1) of the POCCA**

10.8. Must I report attempted business dealings or transactions that are suspicious?

10.8.1. Yes, under the law, you/your firm are required to report any attempted activity or transaction that was regarded as suspicious and was turned away or which never went through. Remember, the reporting of suspicious activity or a suspicious transaction contributes to the authorities' ability to investigate criminal activity or attempted criminal activity. Also remember, that just because you, as the legal practitioner, has turned away a customer/applicant for business, or not gone through with an activity, does not mean that they will not attempt to approach another legal practitioner to see if they can succeed with their criminal intentions. Therefore, your reporting of transactions

or business dealings that have been turned away can result in stopping criminal activity.

10.9. What information should be submitted when I make an STR?

10.9.1. When submitting an STR to the Agency, you must remember that you are doing so in large part to assist the authorities to track down and stop any suspected money laundering, terrorist financing or proliferation financing from occurring or continuing. Therefore, your STRs should be clear, provide as many relevant details as possible and most of all must identify the facts or reasons why you suspect money laundering, terrorist financing, proliferation financing or any other type of criminal activity.

10.9.2. To assist regulated and supervised entities and persons, the FIA has drafted Guidance Notes on STRs that your MLRO may use. The guidance can assist you in determining what information you are required to submit in the STR if you become aware of suspicious activity or a suspicious transaction. This STR Guidance can be found on the Agency's website.

10.10. Keeping a register of STRs

10.10.1. As part of the record keeping requirements under the AML Code, you, as the legal practitioner, is required keep a record of all STRs submitted to your MLRO as well as all STRs submitted to the Agency.

10.10.2. For best practice it is recommended that you keep a register of this information so that you can see at a glance the list of STRs filed. The AML Code provides guidance as to the fields and information that should be recorded.

10.10.3. You should record the following information (which can be in the form of a register):

10.10.3.1. Details of the internal STRs made to your MLRO;
10.10.3.2. Details of the external STRs made to the Agency;
10.10.3.3. Details of the decisions made by the MLRO in relation to STRs as well as the basis for the decisions;
10.10.3.4. Date of Agency's acknowledgement/confirmation letter;
10.10.3.5. Agency reference number

10.10.4. The register or your records of STRs should be kept separate from other records. This protects against accidentally tipping off or disclosing confidential information that might occur if copies of STRs or the records of their filings were to be kept with regular records.

10.10.5. The date of receipt of the Agency's acknowledgement/confirmation and the Agency reference number is important to have as this is your evidence that you filed an STR, and that the Agency has received it. The Agency's reference number is also good to have in the register in the event any additional or supplemental STRs need to be filed in the future relating to the same matter.

- **Sections 17, 18 and 45 of the AML Code**

10.11. What is tipping off?

10.11.1. When you report a suspicion of money laundering, terrorist financing or proliferation financing or when you have a suspicion of money laundering, terrorist financing or proliferation financing, **tipping off** is giving information about the suspicion or about the report of the suspicion to the suspected customer/applicant for business or to anyone who might prejudice an investigation into the suspicion of money laundering, terrorist financing or proliferation financing.

10.11.2. Tipping off is a criminal offence and if you are found guilty of tipping off you can spend time in prison or be fined.

10.11.3. When you have a suspicion of money laundering, terrorist financing or proliferation financing and/or when you file an STR, you must keep the information confidential and not discuss it further unless the relevant persons within your firm or the authorities require you to speak about it.

- **Section 31 of POCCA; Section 60 of the Counter-Terrorism Act; Section 36 of the Proliferation Financing (Prohibition) Act**

10.12. Consequences of not reporting a suspicion of money laundering, terrorist financing or proliferation financing

10.12.1. Under the law, a person commits a criminal offence if they know or suspect or have reasonable grounds for suspecting money laundering or terrorist financing and they do not disclose this to the Agency as soon as reasonably practicable once they become aware of it.

10.12.2. Failure to report a suspicion by a legal practitioner, its management or staff members can attract the following penalties:

10.12.2.1. on summary conviction, to a fine not exceeding one hundred and fifty thousand dollars (US$150,000) or imprisonment for a term not exceeding three years, or both; or

10.12.2.2. on conviction on indictment, to a fine not exceeding five hundred thousand dollars (US$500,000) or imprisonment for a term not exceeding five years, or both.

10.12.3. Further, notwithstanding the criminal penalties mentioned under this section, the Agency can also enforce what is termed "administrative penalties" on entities for failure to comply with statutory obligations.

10.12.4. Failure by an employee of the firm to report a suspicious activity or suspicious transaction carries an administrative penalty of seventy thousand dollars ($70,000).

10.12.5. Additionally, failure to report a suspicion of proliferation financing by a firm, its management or staff members can attract the following penalties:

10.12.5.1. for a body corporate, a fine of five hundred thousand dollars (US$500,000); and

10.12.5.2. for an individual, a fine of two hundred and fifty thousand dollars (US$250,000) or 3 years imprisonment, or both.

- **Sections 27(4), 30A(10) of POCCA**
- **Schedule 4 of the AML Code**
- **Schedule 3 of the Proliferation Financing (Prohibition) Act, 2021**

SECTION 11 Compliance Manual: Creating, Implementing and Following Written Procedures and Controls

11.1. Creating, implementing, and following written policies, processes and procedures

11.1.1. As noted previously within this guidance, the AML Code requires legal practitioners to have in place an effective system of written controls, in the form of policies, processes and procedures, for the purposes of AML/CFT/CPF. More specifically, the sections of the AML Code relating to establishing internal controls, effecting due diligence, maintaining records and training apply to legal practitioners, and legal practitioners are required to put in place policies, processes and procedures relating to these. Generally, these policies, processes and procedures are contained within a compliance manual.

11.1.2. Creating a compliance manual can often seem like an overwhelming task but the compliance manual is nothing more than an internal reference document that explains to everyone what your firm does, the risks that it may face and what specific procedures it has put in place to make sure that those risks are managed and mitigated.

11.1.3. The compliance manual will differ from firm to firm because the type of activities, customers and money received or dispersed, will differ.

11.2. What information should be in your compliance manual?

11.2.1. Your firm's compliance manual will be the main reference document that gives staff members the guidance they need to understand their obligations and the internal procedures they must follow in order to meet the required AML/CFT/CPF obligations.

11.2.2. As such, it is of vital importance that your firm's compliance manual reflects its specific activities and operations.

11.2.3. As part of its ongoing supervision of legal practitioners, should the Agency visit your firm, or undertake a review of its activities to ensure that it is meeting the legislative requirements, the Agency looks at the compliance manual as the standard by which it will evaluate the legal practitioner's activities and compliance with the law. If, therefore, the actual procedures in practice do not match what is in the compliance manual, you, as the legal practitioner, may be deemed non-compliant and face further action.

11.2.4. Key elements and sections to focus on in the compliance manual include, but are not limited to, the following:

11.2.4.1. **A policy statement:** The policy statement should, among other things, discuss your firm's commitment to fighting money laundering, terrorist financing and proliferation

financing. It should also specifically outline your firm's activities and how and where in those activities the firm may be at risk for money laundering, terrorist financing or proliferation financing.

11.2.4.2. **Definitions and explanations of money laundering, terrorist financing & proliferation financing:** This section should include the definitions of money laundering, terrorist financing & proliferation financing and should specify the BVI legislation that governs your AML/CFT/CPF obligations, as a legal practitioner. You should also make clear in this section what the consequences are for non-compliance and provide examples of the fines and penalties that can be levied in the event there is non-compliance.

11.2.4.3. **Policies, Processes and Procedures – the controls:** The policies, processes and procedures within the compliance manual will essentially explain the requirements, what your firm's approach is to meet the requirements (the policy), the steps needed to ensure the policy is adhered to (the process), and the step-by-step detail as to what must be done in order to ensure the legal and regulatory requirements are met (the procedure).

11.2.4.4. This is the main and most important part of your firm's compliance manual and will cover all of the topics covered within this guidance, namely:

11.2.4.4.1. Establishing internal controls;
11.2.4.4.2. Undertaking risk assessments;
11.2.4.4.3. Due diligence;
11.2.4.4.4. MLRO;
11.2.4.4.5. Suspicious transaction reporting;
11.2.4.4.6. Record keeping; and
11.2.4.4.7. Employee/staff training.

11.2.4.5. **Reviews of Procedures:** Additionally, your compliance manual should include details of how often the firm, or its management will review the manual and its internal procedures to ensure they continue to meet the AML/CFT/CPF requirements.

11.2.4.6. **Templates:** To assist your staff, you should also consider whether it is appropriate to include your firm's relevant templates in the manual.

11.2.5. In order to assist legal practitioners in meeting their legal and regulatory obligations, the Agency has created a "Compliance Manual Checklist" which your firm can use to ensure that you have the required policies, processes and procedures in place. Please contact the Agency's Supervision and Enforcement Unit for a copy of the checklist.

11.2.6. Notwithstanding the checklist, as stated above, each compliance manual will need to be specific and tailored to each firm and should detail procedures that are in line with the level of risk your firm has to money laundering, terrorist financing and proliferation financing.

SECTION 12 Consequences of non-compliance with the AML/CFT/CPF obligations

12.0.1. Failing to comply with your AML/CFT/CPF obligations can result in warning letters, fines, penalties (against you and/or your firm), damage to your reputation as a legal practitioner, damage to the BVI's reputation, criminal prosecution and even jail time.

12.0.2. The following is an indication of some of the specific fines and penalties that apply. Please note that the fines and penalties are correct as at the date of publication of this guidance. We ask you to refer to the actual legislation for up-to-date information on the fines and penalties, as these may have changed.

12.1. **Administrative Penalties under the AML Code**

	Type of Breach	Penalty for Corporate Body	Penalty for Individuals
Sections 4A (3), (5), (6) and (8)	Failure to comply with requirements of subsection (1), or carry out customer due diligence and record keeping measures, or accepting donations linked to money laundering, terrorist financing or proliferation financing	$100,000	$80,000
Section 11	Failure to comply with the requirements of section 11	$100,000	$80,000
Section 12	Failure to carry out money laundering, terrorist financing and proliferation financing risk assessments	$100,000	$80,000
Section 14	Failure to comply with the measures required under section 14(2)	$100,000	$80,000
Section 15	Failure by an employee to comply with the requirements under section 15	-	$75,000
Section 16 (3)	Failure to comply with the prescribed obligations in relation to a Reporting Officer	$65,000	$60,000
Section 18 (1)	Failure by an employee to report a suspicious activity or transaction		$80,000
Sections 19 (2), (4) and (5)	Failure to engage in or undertake customer due diligence, or additional customer due diligence in the case of a trustee of a trust or a legal Person	$100,000	$80,000
Section 20	Failure to engage in enhanced customer due Diligence	$100,000	$80,000

Section 21	Failure to undertake ongoing customer due diligence	$75,000	$70,000
Sections 29 (2) and (4)	Failure to adopt relevant measures or additional measures or checks in non-face to face relationships	$100,000	$80,000
Section 30 (1)	Failure to ensure proper certification of document, or accepting certified document contrary to the section	$100,000	$80,000
Section 31 (2) and (5)	Failure to record an introduction of an applicant for business or a customer, or to ensure that an introducer reviews and maintains customer due diligence information as required	$70,000	$65,000
Section 31A (4)	Failure to amend or revise a written agreement within the prescribed period to comply with a condition stipulated in section 31A	$100,000	$60,000
Section 31B (1)	Failure to test a business relationship with a third party	$75,000	$70,000
Section 31B (5)	Failure to prepare a report of testing of business relationship with a third party or to provide copy of report to the Commission	$70,000	$65,000
Section 32	Failure to take post verification steps required under the section	$65,000	$60,000
Section 36	Failure by a correspondent bank to satisfy itself regarding necessary customer due diligence measures required to be undertaken by a respondent bank	$100,000	$100,000
Sections 39(1) and (3)	Failure to ensure transfer of funds accompanied by full originator information and full beneficiary information, or to verify full originator information	$80,000	$75,000
Section 39 (6)	Failure to keep records of full originator information on payer and full beneficiary information on the payee	$100,000	$80,000
Sections 41 (2) and (5)	Failure to keep information received on payer with the transfer of funds, or to provide upon request within the specified time information on payer that the intermediary payment service provider has received	$80,000	$75,000
Section 41 (6)	Failure to keep records of information on payer and the payee for the specified period	$100,000	$80,000
Section 42 (2)	Failure to maintain records in the required form	$60,000	$60,000
Section 44	Failure to maintain transaction records	$100,000	$80,000

Section 46 (2)	Entering into an outsourcing agreement for the retention of records whereby access to such records is impeded by confidentiality or data protection restrictions, or the outsourcing prevents or impedes the implementation of the Anti-money Laundering Regulations Revised Edition 2020, this Code or other enactment relating to money laundering, terrorist financing or proliferation financing	$100,000	$80,000
Section 47(1)	Failure to train employees	$80,000	$75,000
Sections 48 (1) and (2)	Failure to provide training at appropriate frequencies or to the desired level and standard	$80,000	$75,000
Section 55 (1) and (2)	Failure to make or submit a report in the proper form	$60,000	$60,000
Miscellaneous	The breach of or non-compliance with any provision for which a penalty is not specifically provided	$60,000	$60,000

12.2. **Criminal Penalties under the AML Code**

	Type of Breach	**Penalty**
Section 9(5)	Failure to comply with a report providing remedial action within a specified period for which such action must be taken	**Summary conviction:** • Fine not exceeding $150,000; or • Prison term not exceeding 2 years; or • Both
Section 11	Failure to establish and maintain a written and effective system of internal controls (otherwise known as a Compliance Manual)	**Summary conviction:** • Fine not exceeding $150,000; or • Prison term not exceeding 2 years; or • Both

Section 17(1)	Failure by the MLRO to submit a report to the FIA in accordance with section 55 of the AML Code	**Summary conviction:** • Fine not exceeding $150,000; or • Prison term not exceeding 2 years; or • Both

12.3. **Criminal Penalties under the Proceeds of Criminal Conduct Act**

	Type of Breach	Penalty
Section 27(4)	Failure by a person to comply with the Anti-Money Laundering and Terrorist Financing Code of Practice	**Summary Conviction:** • Fine not exceeding $150,000; or • Prison term not exceeding 2 years; or • Both
Sections 31(1)(2)&(3)	(1) When a person knows or suspects that a money laundering investigation will commence, and that person discloses this information to anyone who may prejudice the outcome of the investigation; (2) When a person knows or suspects that a report is about to be made to the Agency and that person discloses this information to anyone who may prejudice the investigation; (3) When a person knows or suspects that a disclosure will not be treated as a breach of any restriction imposed by statute or otherwise and that person discloses to anyone information which is likely to prejudice any investigation which might be conducted following the disclosure **(Tipping Off Offences for ML)**	**Summary Conviction:** • Fine not exceeding $250,000; or • Prison term not exceeding 2 years; or • Both **Conviction on Indictment:** • Fine not exceeding $500,000; or • Prison term not exceeding 5 years; or • Both

12.4. **Tipping Off Offences for TF under the Counter-Terrorism Act, 2021**

	Type of Breach	Penalty
Section 60(4)	• A person commits an offence if: (a) he knows or suspects that a report of suspicious information is being or had been made to the Financial Investigation Agency under subsections (2) and (3); and (b) he discloses to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following the report of suspicious information.	**Summary Conviction:** • Fine not exceeding $150,000; or • Prison term not exceeding 3 years; or both **Conviction on Indictment:** • Fine not exceeding $500,000; or • Prison term not exceeding 5 years; or both

12.5. **Penalties under the Proliferation Financing (Prohibition) Act, 2021**

Section	Type of Offence	Penalty for Corporate Body	Penalty for Individuals
15 (1) & (3)	Dealing with an asset knowingly or recklessly with a designated person or entity, etc.	$500,000	$250,000 or 3 years imprisonment, or both
16 (1) & (3)	Making an asset available knowingly or recklessly to a designated person or entity	$500,000	$250,000 or 3 years imprisonment, or both
19 (1) & (3)	Knowingly or recklessly making available an asset or financial service to a designated person or entity that could contribute to an activity listed in subsection (2)	$500,000	$250,000 or 3 years imprisonment, or both
20 (1) & (3)	Knowingly or recklessly conducting specified transaction that could contribute to an activity in subsection (2)	$500,000	$250,000 or 3 years imprisonment, or both

21 (1) & (2)	Knowingly or recklessly providing an asset or financial service intended to facilitate trade with a designated country person or entity	$500,000	$250,000 or 3 years imprisonment, or both
22 (1) & (2)	Establishing or maintaining a joint venture knowingly or recklessly as to whether certain identified persons or entities are a party to the joint venture	$500,000	$250,000 or 3 years imprisonment, or both
26 (1) & (2)	Conducting financial transaction relating to professional or commercial profit- making activities in relation to a designated country's diplomatic agents, etc.	$400,000	$200,000 or 2 years imprisonment, or both
28(1) & (2)	Dealing with or insuring a designated country's flagged vessel	$300,000	$200,000 or 2 years imprisonment, or both
34(1) & (5)	Intentionally or negligently failing to report the holding of an asset of a designated person or entity	$500,000	$250,000 or 3 years imprisonment, or both
35 (4) & (8)	Intentionally or negligently failing to make a suspicious transaction report	$500,000	$250,000 or 3 years imprisonment, or both
36(1) & (4)	Intentionally or negligently disclosing information contrary to subsection (1) (**Tipping Off Offences for PF**)	$500,000	$250,000 or 3 years imprisonment, or both
37 (1) & (4)	Intentionally or negligently failing to make an enhanced report	$500,000	$250,000 or 3 years imprisonment, or both
43 (4)	Giving information or procuring document knowing it to be false in a material particular, or destroying, mutilating, defacing, etc. a document with intention of evading a request	$500,000	$250,000 or 3 years imprisonment, or both

50(1)	Knowingly or recklessly providing information that is false in a material particular or a document that is not what it purports to be, for the purpose of obtaining an authorisation	$500,000	$250,000 or 3 years imprisonment, or both
61(4)	Failing to immediately comply with a direction issued by the Governor	$100,000	$50,000 or 1 year imprisonment, or both

SECTION 13 Where Can I Get Help?

13.1. Various resources are available to assist legal practitioners to better understand their AML/CFT/CPF obligations and how to implement the measures and policies required under the law.

13.2. **The Agency**

13.2.1. The Agency strives to work with its supervised entities to ensure they understand the risks they face and the obligations and measures they are expected to implement. Whilst the Agency cannot specifically tell you or your firm what to do, because the obligation remains with the legal practitioner to ensure the requirements are met, the Agency can provide support and guidance, wherever possible.

13.2.2. The Agency has devised documents such as this Guidance and the compliance manual checklist with a view to assisting legal practitioners. The Agency is also available to answer questions you as a legal practitioner may have about the AML/CFT/CPF obligations or any suspicions you may have. You can contact us on:

Email: complianceunit@fiabvi.vg
Tel: 284-852-3200

13.2.3. From time to time, the Agency will also hold outreach and training sessions aimed at legal practitioners and we would encourage you to attend these.

13.3. **Volunteers and other local resources**

13.3.1. There are often experienced and knowledgeable companies or individuals, who as part of their community service, may be willing to provide training or advice that would help your firm with its compliance obligations.

13.4. **Private sector businesses and consulting firms**

13.4.1. Various private sector businesses and firms in the BVI provide training, assistance in drafting procedures, and other services to assist legal practitioners in meeting AML/CFT/CPF obligations. As the supervisory authority, the Agency is not in a position to make recommendations or provide names of these firms.