2025

Financial Analysis and Supervision Unit

Sector Guidance for Legal Professionals to Raise Awareness on Obligations under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 9 of 2025)

Issued by the Financial Analysis and Supervision Unit on 26th of September 2025

Disclaimer: *This Guidance is issued in accordance with Section 72(1)(b),(2)(b) of the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (Act) for awareness raising purposes only and cannot be relied on as evidence of complying with the obligations of the Act. It does not constitute legal advice and cannot be relied on as such. Nor is it intended to be guidance for the purposes of a Compliance Rule under Sections 73 and 74 of the Act. After reading this Guidance, if you do not fully understand your obligations or have any questions, you should contact the Financial Analysis and Supervision Unit on email fasu@bankpng.gov.pg or telephone number +675 322 7147.*

Document Version Control

Version	Date Issued	Document Status	Document Author
1	30.06.25	Draft	FASU
2	30.07.25	Draft	Asian Development Bank Consultant
3	06.08.25	Draft	FASU
4	30.08.25	Draft	Asian Development Bank Consultant
5	26.09.25	Final	FASU

Table of Contents

TABLE OF ACRONYMS **4**

1. KEY CONCEPTS AND TERMS **5**

2. PURPOSE AND SCOPE OF THIS GUIDANCE **8**

3. MONEY LAUNDERING, TERRORIST FINANCING AND LEGAL PROFESSIONALS **10**

3.1. Introduction 10
3.2. What is a legal professional? 10
3.3. What does the AML/CTF regime has to do with legal professionals? 10

4. AML/CTF OBLIGATIONS AND REQUIREMENTS UNDER THE ACT **13**

4.1. Summary of Key Obligations for Legal Professionals 13
4.2. Why do legal professionals have to fulfil these obligations and follow these requirements? 14
4.3. What is FASU? Why is it important for you to know? 14

5. APPOINTING AN AML/CTF COMPLIANCE OFFICER **16**

5.1. Who is AML/CTF compliance officer and what are their duties and obligations? 16
5.2. What are the considerations when appointing a compliance officer? 17
5.3. What happens if you lose your compliance officer? 18

6. PRACTICE/FIRM-LEVEL RISK ASSESSMENT **19**

6.1. Client Risks 20
6.2. Business Activities and Services Risks 21
6.3. Geographical risks 21
6.4. Delivery Channel Risks 22
6.5. Mitigating risk 22
6.6. External audit of risk assessment and AML/CTF Program 23

7. CDD MEASURES: IDENTIFYING, VERIFYING AND MONITORING CLIENTS **24**

7.1. What is customer due diligence? 24
7.2. Undertaking client and matter risk assessments 25
7.3. When should I carry out CDD? 26
7.4. What information must I collect and keep? 26
7.5. Verifying Identity 28
7.6. What is Enhanced Customer Due Diligence ("ECCD")? 28
7.7. When should ECCD measures be applied? 29
7.8 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? 29
7.9. Face to Face Versus Non-Face to Face Clients 30
7.10. Certificate of documents for CDD 30
7.11. What if I cannot get due diligence on the client? 31
7.12. Monitoring and Ongoing CDD 32
7.13. Monitoring transactions 32
7.14. CDD on existing clients or business relationships 33

8. RECORD KEEPING **34**

8.1. What records must a legal professional keep? 34
8.2. How should the records be kept? 35
8.3. How long must records be kept? 35

9. TRAINING **36**

9.1. Why is training important? 36
9.2. Who within my firm must be trained? 37
9.3. What should the training be on? 37

9.4. How often should the training take place? 37
9.5. What records of the training must be kept? 38
9.6. Where can I get training? 38

10. IDENTIFYING AND REPORTING SUSPICIOUS MATTERS 39

10.1. What is a suspicious matter? 39
10.2. What is suspicious activity? 39
10.3. What is suspicious transaction? 39
10.4. Unusual vs. Suspicious 39
10.5. Reporting suspicious matters 40
10.6. Reporting suspicious matter to the FASU if you are a compliance officer 41
10.7. When must I submit a SMR? 41
10.8. Must I report attempted business dealings or transactions that are suspicious? 41
10.9. What information should be submitted when I make a SMR? 42
10.10. Keeping a register of SMRs 42
10.11. What is tipping off? 43
10.12. Is threshold transaction reporting different from SMRs? 43

11. AML/CTF PROGRAM 45

11.1. Creating, implementing, and following written internal policies, processes and procedures 45
11.2. What information should be in your AML/CTF Program? 45

12. TARGETED FINANCIAL SANCTIONS 48

REFERENCES AND CONTACTS 49

Table of Acronyms

Act	Anti-Money Laundering and Countering Terrorist Financing Act 2015
AML/CTF	Anti-Money Laundering/Counter Terrorist Financing
APG	Asia Pacific Group on Money Laundering
CDD	Customer (or Client) Due Diligence
DNFBPs	Designated Non-Financial Businesses or Professions
ECDD	Enhanced Customer Due Diligence
FASU	Financial Analysis and Supervision Unit
FATF	Financial Action Task Force
ID	Identification
KYC	Know Your Customer (or Client)
ML	Money Laundering
PWRA	Practice-wide Risk Assessment
RBA	Risk-based Approach
SMR	Suspicious Matter Report
TF/FT	Terrorist Financing/Financing of Terrorism
UNFSA	United Nations Financial Sanctions Act 2015

1. Key Concepts and Terms

A number of terms used in this Guidance are defined in Section 5 of the Act. Legal professionals must rely on the technical definitions of these terms as stipulated in the Act. Only for the purpose of assisting legal professionals in understanding their obligations, this Guidance provides a lay explanation of some of these key terms above.

1.1. **Beneficial Owner** in the context of **legal persons**, refers to the natural person(s) who ultimately owns[1] or controls[2], directly or indirectly, a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.

In the context of **legal arrangements**, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement. In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.

1.2. **Customer (or client)** as defined in Section 5 of the Act means a customer, person[3] or unincorporated entity for whom a legal professional carries out a transaction; or with whom a legal professional conducts a business relationship, and includes such people or entities who/that attempt to carry out a transaction or business relationship, as well as a new or existing client.

1.3. **Criminal property** adopts the same definition as the definition given in Section 508A of the *Criminal Code Act* Chapter 262 as amended[4], and means property that is, in whole or in part and whether directly or indirectly, derived from, obtained or used in connection with criminal conduct and includes any interest, dividends or other income on or value accruing from or generated by such property, regardless of who carried out the criminal conduct or who benefited from it.

1.4. **Customer Due Diligence (CDD)** is, at a minimum, the process of:

a). identifying a customer and ensuring that they are who they claim to be, i.e. verifying the customer;

[1] "Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.
[2] "Control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to make decisions about financial and operating polices.
[3] Person as defined under Section 5 of the Act means a natural person and a body corporate.
[4] Amended by section 2 of the *Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act* 2015.

b). maintaining current and up to date information and records relating to the customer and (where relevant) their beneficial owners, and the nature and purpose of the business relationship, and the customer's commercial or personal activities; and

c). ensuring that transactions carried out on behalf of a customer are consistent with the financial institution's knowledge of the customer, the customer's commercial or personal activities and risk profile, and where necessary, the source of the funds.

1.5. **Designated Non-Financial Businesses or Professions (DNFBPs)**, as defined in Section 5 of the *Anti-Money Laundering and Combating Terrorist Financing Act 2015* (hereinafter referred to as "Act"), includes a casino, real estate agent, dealer in precious metals or precious stones, lawyers, notary public, other independent legal professional and an accountant when undertaking certain transactions on behalf of a client, a trust or company service provider, and a motor vehicle dealer.

1.6. **Financial Analysis and Supervision Unit (FASU)** is established under Section 61 of the Act whose functions are set out in Section 72(1)(2)(3) of the Act which are to:

1.6.1. carry out financial intelligence and analysis concerning suspected money laundering and associated predicate offences, terrorist financing and proceeds of crime;

1.6.2. monitor and enforce compliance with the Act; and

1.6.3. receive reports and information provided to it under PNG's proceeds of crime law and disseminate such reports and information in accordance with PNG's proceeds of crime law and the Act.

1.7. **Legal Professionals** include barristers, solicitors, other specialist advocates, and notaries that carry out specified services or transactional activities (as outlined in this Guidance) for third parties and do not apply to all activities carried out by legal professionals.

1.8. **Money Laundering (ML)** is the process of hiding the illegal origin of money and making it appear to come from legitimate sources. It usually happens in three stages: (1) Placement – putting the illegal money into the financial system, (2) Layering – moving it around through different transactions to hide its origin, and (3) Integration – bringing it back into the economy as "clean" money that appears to have come from a legitimate source.

1.9. **Politically Exposed Person (PEP),** as defined in Section 5 of the Act, means a person who has been entrusted with prominent public functions in PNG or another country, and an immediate family member or close associate of that person.

1.10. **Proliferation Financing (PF)** is the act of providing funds or financial services which are used, whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biochemical weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

1.11. **Record** means information recorded or retained in any form which can be accessed in or from PNG and which can be read or understood by a person, computer system or other device.

1.12. **Risk** occurs when a threat successfully takes advantage of a vulnerability to produce a consequence. Simply, risk in the context of money laundering (ML) and terrorist financing (TF) can be seen as a function of three factors: threat, vulnerability, and consequence.

a). **threat** is a person or group, object or activity with the potential to cause harm to the state, society or the economy. In the context of ML/TF, 'threat' includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities

b). **vulnerability** refers to those characteristics of a business that can be exploited by the threat or that may support or facilitate its activities. This includes features of a particular sector that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which it deals. Vulnerability is also influenced by the AML/CTF systems and controls in place by the business

c). **consequence** refers to the potential impact or harm that ML/TF activity may cause if it materialises and includes the effect of the underlying criminal activity or terrorist on you and your business or profession.

d). **likelihood** of a risk manifesting is based on the combined assessment of the **threat** to and **vulnerability** of your business or profession to ML and TF activity.

1.13. **Risk Assessment** is the process of identifying, analysing and evaluating, and mitigating and managing risks.

1.14. **Terrorist Financing (TF)** is providing or collecting property to finance terrorist activities, individual terrorists or terrorist organisations.

2. Purpose and Scope of this Guidance

> ! **This Guidance intends to raise awareness and assist legal professionals understand their obligations under the Act and relevant international standards set by FATF. It is not legal advice, and as such, does not intend to replace the Act.**

2.1. This Guidance is developed in accordance with Section 72(1)(b),(2)(b) of the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (hereinafter referred to as 'Act') to raise awareness of money laundering and terrorist financing and obligations on financial institutions (FIs) and designated non-financial businesses or professions (DNFBPs).

2.2. This Guidance applies specifically to lawyers, notary public, and other independent legal professions (hereinafter jointly referred to as 'legal professionals') operating within Papua New Guinea (PNG) who prepare for, engage in, or carry out the provision of services to clients which involve one or more transactions concerning any of the following activities:

- 2.2.1. buying and selling of real estate;
- 2.2.2. managing client money, securities, or other assets;
- 2.2.3. managing bank, savings or securities accounts;
- 2.2.4. organising contributions for the creation, operation or management of bodies corporate;
- 2.2.5. creating, operating or managing bodies corporate or unincorporated entities; and
- 2.2.6. buying and selling of businesses.[5]

2.3. Some legal professionals may draw the conclusion that due to the services their office/practice renders, they do not have any specific anti-money laundering and counter terrorist financing (AML/CTF) obligations considering they do not engage in any of the functions set out at paragraph 2.1. However, although specific AML/CTF obligations may not apply to a legal professional in such instances, implementing safeguards within the practice/firm to ensure that the legal professional'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 professionals that do not engage in the activities specified at paragraph 2.1. should consider what they need to do to guard against that, to not be unwittingly involved in ML/TF.

2.4. It is important to note here that the National Risk Assessment 2017 of PNG (NRA)[6] and PNG's Mutual Evaluation Report (MER) 2024 has identified the legal sector as one of the four very highly vulnerable sectors to ML.[7]

---

[5] Section 5 of the Act

[6] PNG's national risk assessment on money laundering and terrorist financing, published in 2017.

[7] PNG MER, paragraph 22, p.22:
"The NRA reasonably identifies key FIs and DNFBPs overall level of vulnerability; however, the analysis lacks depth in identifying some sector-specific vulnerabilities, particularly for foreign banks, superannuation funds, and DNFBPs. For FIs, domestic banks, and currency transfer and exchange businesses are identified as very highly vulnerable to ML. For DNFBPs, real estate agents, lawyers and accountants, particularly those engaged in commercial activities and company/trust formation and management, and MV dealers are identified as highly vulnerable to ML/TF. Vulnerability of other FIs is discussed in IO.1 and R.1."

2.5. This purpose of this Guidance is thus to assist legal professionals to better understand:

2.5.1. their role in the fight against ML and TF;
2.5.2. their obligations under the Act; and
2.5.3. ensuring effective compliance with their AML/CTF obligations and take practical steps to mitigate ML/TF risks.

2.6. This Guidance should be read in conjunction with the following FASU Guidance, which are available on the website of the Bank of PNG:

a). *Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 2 of 2019)* (issued on 20 May 2019), and
b). *Guidance on Supervision and Enforcement Powers of the Financial Analysis and Supervision Unit under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 3 of 2019)*.

2.7. This Guidance is only meant to provide industry awareness, practical assistance and a basis to improve the ability of legal professionals be able to comply with their AML/CTF obligations.

2.8. For ease of reference, in each Section, where appropriate, you will also find references to the relevant provisions of the Act and cross-references to other related Guidelines.

2.9. This Guidance should also be considered in the context of applicable lawyer-client privilege. Lawyer-client privilege is a protection to the client and a duty of the legal professional to protect client information or advice from being divulged. In instances where legal professionals are claiming lawyer-client privilege or privileged communication, they must be satisfied that the information is protected by lawyer-client privilege and the relevant rules.

2.10. Legal professionals should develop their own internal policies, procedures and controls tailored to their business/firm needs.

2.11. Some of the 'marks' used in the textboxes of this Guidance should be read as below:

i	Textbox in this format provides information to assist legal professionals understand their obligations and the provisions in the Act to which those obligations relate.
e.g.	Textbox in this format provides appropriate examples.
!	Textbox in this format stresses important information for legal professionals, including on penalties for non-compliance with obligations under the Act.

3. Money Laundering, Terrorist Financing and Legal Professionals

3.1. Introduction

3.1.1. Governments and international bodies like the Financial Action Task Force (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 billion) and two trillion dollars (US$2 trillion) 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/CTF measures, which prevent and stop such criminal activity.

3.1.2. Many governments, including the Government of PNG, have implemented these recommendations into law in the form Acts of Parliament. One of these Acts of Parliament is the AMLCTF Act which is supported by other related Guidelines, including *Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 2 of 2019) (issued on 20 May 2019)* (hereinafter, 'DNFBPs Guidance'). The AMLCTF Act and DNFBPs Guidance also specifically apply to legal professionals, as generally they are known to be targeted by money launderers and other criminals to further their illegal activity.

3.1.3. In addition to adopting the Act and the related Guidelines, the Government of PNG via the Act, has given FASU the mandate to monitor and enforce compliance by the registered entities, including legal professionals, with their obligations under the Act.

3.2. What is a legal professional?

3.2.1. In PNG, a legal professional means a person whose name is admitted to the practice of law as a lawyer before the courts of PNG in accordance with Section 1 of the *Lawyers Act 1986*. The term also covers within its scope notaries public; however, these services are also provided by lawyers in PNG.

3.2.2. For the purposes of being subject to specific AML/CTF obligations, a legal professional must be engaging in the activities specified at paragraph 2.1. of this Guidance.

3.2.3. If the activities performed by the legal professional fit this definition, he/she will be required to follow and implement certain rules and obligations which are outlined in later sections of this Guidance below.

3.3. What does the AML/CTF regime has to do with legal professionals?

3.3.1. The FATF in assessing risks and vulnerabilities determined that legal professionals are susceptible to being used not only in the layering and integration stages of the money laundering process, but also in the placement stage, as a means to disguise or conceal the origin of illicit funds and as a conduit to transfer said funds into the financial system. Legal professionals are often the first professionals consulted for general business advice on a wide range of regulatory and compliance matters.

3.3.2. The FATF characterises legal professionals as "gatekeepers" because they "protect the gates of the financial system" through which potential users must pass in order for the users to obtain a level of legitimacy to their businesses. 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 professionals, accountants and trust and company service providers. The FATF has noted that gatekeepers are a common factor in complex money laundering schemes. Gatekeepers' skills are important for creating legal structures that could be used to launder money and for managing and performing transactions efficiently whilst avoiding detection. FATF's Recommendation 22 acknowledges the role that such gatekeepers can play by recommending that such professions have AML/CTF responsibilities when engaged in specific activities.

3.3.3. Consequently, legal professionals must see AML/CTF policies and procedures as part of their operational practice. This is important because the consequences of participating in money laundering 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.

3.3.4. The 2017 NRA[8] and the 2024 MER of PNG has also identified the legal sector in PNG as one of the three very highly vulnerable sectors to ML.[9]

3.3.5. To prevent the misuse of legal sector for ML/TF purposes, the Act applies to legal professionals in the same manner as they apply to financial institutions. Consequently, the obligations imposed upon financial institutions also apply to legal professionals and other DNFBPs. This therefore requires legal professionals to keep client records and perform due diligence procedures in seeking to know their clients. Legal professionals are also required to submit suspicious matter reports (SMRs) to the FASU, when the when the criteria set out in the Act are met. In order to make a proper judgment in this regard, legal professionals will need to avail themselves of training opportunities so that they would be properly equipped to protect themselves and their practices.

3.3.6. The issue of lawyer-client privilege looms greatly over the responsibility of legal professionals to report their clients' suspicious activity to the authorities. This Guidance 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 ML enterprise or a TF act, or a professional who fails to report such activity.

3.3.7. It is imperative to state here that the AML/CTF 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,

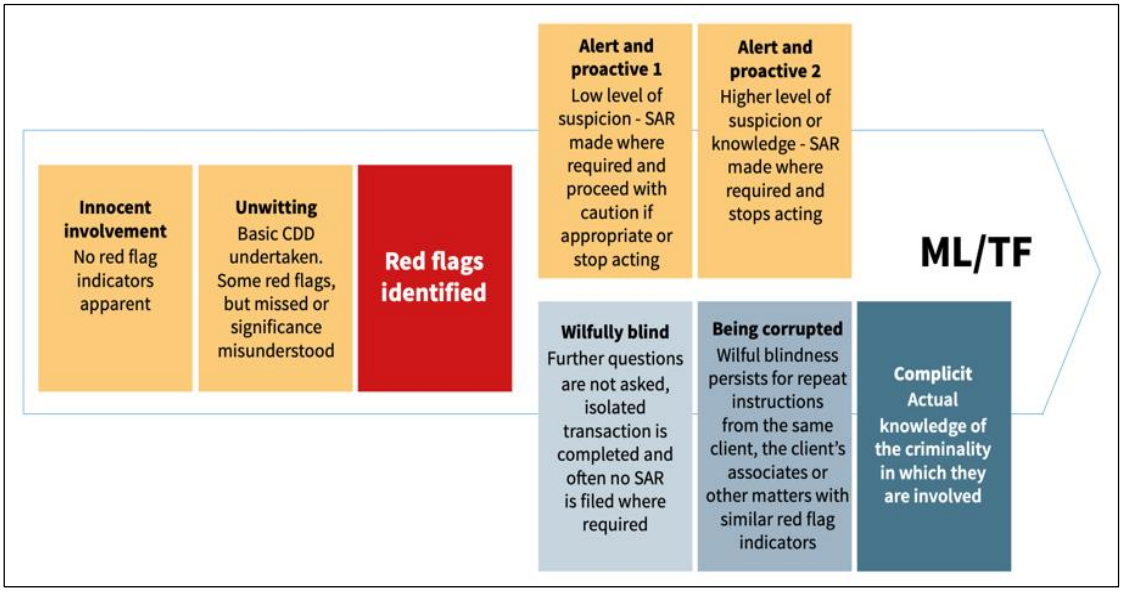
[8] PNG's national risk assessment on money laundering and terrorist financing, published in 2017.
[9] PNG MER, paragraph 22, p.22:
"The NRA reasonably identifies key FIs and DNFBPs overall level of vulnerability; however, the analysis lacks depth in identifying some sector-specific vulnerabilities, particularly for foreign banks, superannuation funds, and DNFBPs. For FIs, domestic banks, and currency transfer and exchange businesses are identified as very highly vulnerable to ML. For DNFBPs, real estate agents, lawyers and accountants, particularly those engaged in commercial activities and company/trust formation and management, and MV dealers are identified as highly vulnerable to ML/TF. Vulnerability of other FIs is discussed in IO.1 and R.1."

shared in confidence, to any authority. However, such interaction should not include advice on how to conduct ML, TF, or the furtherance of any other criminal purpose.

3.3.8. It is worth emphasizing and reiterating that the AML/CTF obligations of a legal professional arise only in the circumstances specified at paragraph 2.1 of this Guidance and not to the general practice of all aspects of legal practice.

3.3.9. Although individual legal professionals or law firms may be able to conclude that specific AML/CTF 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. When legal professionals lack ML/TF awareness, they are more at risk of inadvertently helping criminals.

Figure 1: Involvement of Legal Professionals in ML



Source: International Bar Association, 2014[10]

[10] International Bar Association (2014), *A Lawyer's Guide to Detecting and Preventing Money Laundering* (October 2014), p. 25

4. AML/CTF Obligations and Requirements under the Act

4A. The international recommendations and the AML/CTF legislation of PNG outline ways that are proven to help deter and detect instances of ML and TF. These all form the basis of understanding your AML/CTF obligations and the requirements to be met by a legal professional.

> *i* *The Act sets out specific obligations on financial institutions which also apply to DNFBPs under Part II, except for Subdivisions 3 and 4.*

4B. This Guidance will now take you through the specifics of your AML/CFT obligations as a legal professional.

4C. To provide additional clarity, the key AML/CTF obligations for legal professionals are first summarised in this section below. Later sections of the Guidance will then cover each of these in further detail.

4.1. Summary of Key Obligations for Legal Professionals

4.1.1. As noted previously, if you as a legal professional are performing the activities specified at paragraph 2.1. above, then based on legislation, you are required to implement certain policies, processes and procedures to prevent you or your firm/practice from being used by money launderers and financiers of terrorism to further their illegal activities.

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 hold them accountable. Following these steps will also help to protect you as a legal professional, as it will show that you have taken the required steps to ensure that you are not involved in money laundering or terrorist financing.

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

- 4.1.3.1. Conduct **risk assessment** of your firm/practice to assess the risk you as a legal professional may face from funds linked to money launderers or terrorists and/or be used to fund or support terrorist activity;
- 4.1.3.2. 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 (an **AML/CTF program**);
- 4.1.3.3. Conduct **periodic reviews** of your risk assessment and AML/CTF program to ensure that it is relevant and effective;
- 4.1.3.4. Conduct an **external audit** of your risk assessment and AML/CTF program to ensure your compliance with the Act and related regulations.

4.1.3.5. Appoint an **AML/CTF Compliance Officer**, in accordance with the requirements of the Act;

4.1.3.6. Undertake **CDD** on your clients;

4.1.3.7. Maintain **records** including records of due diligence, transactions, financial transactions and suspicious transactions;

4.1.3.8. Provide **training** and awareness on money laundering and terrorist 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 practice/firm;

4.1.3.9. **Report** suspicions of money laundering and terrorist financing to FASU; and

4.1.3.10. When you have a suspicion of money laundering or terrorist financing, 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 a SMR has been filed on them.

4.2. Why do legal professionals have to fulfil these obligations and follow these requirements?

4.2.1. It is imperative that you fulfil these obligations because if you fail to do so you can be subject to various enforcement actions including penalties under the Act. Such failure can also cause reputational damage, not only to you but to PNG 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 professional, for some reason, becomes involved in a situation involving ML/TF, you may have a defence against prosecution.

4.3. What is FASU? Why is it important for you to know?

i *The Act sets out FASU's supervision and enforcement powers in Part IV:*

- *Division 1 – FASU and its functions (Sections 61 – 78)*
- *Division 2 – Information gathering powers (Sections 79 – 93)*
- *Division 3 – Use and disclosure of confidential information (Section 94 – 98)*
- *Division 4 – Enforcement (Sections 99 – 106)*

4.3.1. FASU is the Financial Intelligence Unit (FIU) of the PNG. It is also responsible for supervising and monitoring DNFBPs, which includes legal professionals, to ensure that they are meeting their obligations in the fight against money laundering and terrorist financing.

4.3.2. **Legal professionals, as a part of DNFBPs sector, are required to register with FASU and be reporting entities under Section 57 of the Act.** You can pick up registration forms at the FASU office in Port Moresby (see contact details on the last page of this Guidance). Upon successful registration, FASU will issue a certificate of registration to the entity in recognition of being a newly registered reporting entity that is required to comply with obligations under the Act. You can pick up certificates of registration at the FASU office or arrange for FASU to send the certificate to you *via* email.

4.3.3. Legal professionals are also required to report any changes in key personnel of the firm, such as principals, partners, or a compliance officer, to FASU. Legal professionals must also report changes in their registered office or principal place of business.

4.3.4. FASU is responsible for monitoring and enforcing compliance by legal professionals with the requirements of the Act, and other applicable legislation. FASU supervises and monitors legal professionals to ensure they comply with their obligations under the Act. It does this by: issuing directions and guidelines, undertaking outreach with legal professionals in order to reduce the risk of them being used for ML/TF, and from time-to time by conducting visits (onsite inspections) to make sure that legal professionals are meeting the requirements of the AMLCTF Act, and by imposing sanctions for non-compliance.

4.3.5. FASU is also the body to whom any suspicious transactions relating to money laundering or terrorist financing, should be reported. Once the FASU receives a SMR, the FASU investigates and analyses the information and takes the necessary action to prevent or combat money laundering or terrorist financing from occurring or continuing.

4.3.6. If you have any questions on your AML/CTF obligations as a legal professional, you should contact FASU in the first instance, who will be able to provide further guidance.

4.3.7. If you have any questions on SMR filing, you should contact the FASU to receive any further guidance.

5. Appointing an AML/CTF Compliance Officer

5.1. Who is AML/CTF compliance officer and what are their duties and obligations?

5.1.1. The Act and DNFBPs Guidance require you to appoint a compliance officer who must have direct access to the senior management. This role may be assigned to one of the firm's lawyers. The compliance officer is responsible for ensuring that its employer/organization complies with its obligations under the Act.

5.1.2. Depending on the size of your firm, you may also appoint a deputy compliance officer to support the functions or role of the compliance officer.

5.1.3. However, if you are a sole practitioner with no employees, you must yourself act as a compliance officer and shall be responsible to ensure compliance with the AML/CTF obligations.

5.1.4. The compliance officer is responsible for:

5.1.4.1. establishing and maintaining internal policies, procedures, processes and control of the practice/firm in accordance with the AML/CTF legislation and regulations;

5.1.4.2. implementing fit and proper procedures when hiring new employees, as well as procedures for the verification of existing employees, which set standards for ensuring ethical and moral integrity and their professional abilities to ensure their integrity;

5.1.4.3. ensuring AML/CTF compliance by employees of the legal professional and implements internal policies, procedures, and controls to deter and detect money laundering, and terrorist financing;

5.1.4.4. making annual reports to senior management concerning level of compliance adherence to policies, procedures, processes and controls;

5.1.4.5. carrying out risk assessments on the clients;

5.1.4.6. ensuring that employees are properly trained on and aware of issues, legislation and internal policies, procedures and processes relating to AML/CTF;

5.1.4.7. being the first point of contact regarding AML/CTF matters and communicating and liaising with the FASU and other competent authorities on behalf of the practice/firm;

5.1.4.8. reporting threshold transactions and suspicious matters to FASU;

5.1.4.9. maintaining a register of SMRs and inquiries from FASU.

5.1.5. Additionally, the compliance officer is the person to whom any suspicions of ML or TF activity should be reported within the practice/firm. The compliance officer is also responsible for investigating and asking appropriate questions to determine whether internally reported unusual or suspicious matters give rise to a suspicion of money laundering or terrorist financing that should be reported to the FASU.

5.1.6. It is not obligatory that the compliance officer pass on to FASU all SMRs the compliance officer receives. Prior to filing a SMR with the FASU, the compliance officer should analyse every SMR they receive internally and apply judgment based on the facts, the statutory obligations, current

policies and internal controls regarding the AML/CTF obligations of the legal professional, to determine if an internal reported suspicion should result in a SMR filing to FASU. There may be instances, where after investigation, a compliance officer finds that there were reasonable explanations for what at first appeared to be suspicious activity, and therefore decides that a SMR to FASU is not required. In these instances, the compliance officer 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 FASU.

5.1.7. However, it is important to know that if the compliance officer in analysing the internal SMR is uncertain that the report amounts to suspicious activity, the SMR filing should be made to the FASU.

5.1.8. Moreover, the compliance officer liaises with and corresponds with FASU and responds to any requests for information, data and documents that FASU may make regarding the activities of the practice/firm.

5.1.9. The compliance officer is also responsible to promptly notify FASU regarding any communication from other authorities or regulators concerning money laundering or terrorist financing matters.

5.2. What are the considerations when appointing a compliance officer?

5.2.1. When appointing a compliance officer, you must ensure that the compliance officer understands your activities and your clients. The person should have an understanding of the requirements of the Act and the DNFBPs Guidance.

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

5.2.2.1. sufficient seniority, meaning that the person appointed must be have direct access to senior management and is fit and proper for the position and capable of fulfilling the role;
5.2.2.2. appropriate qualifications and experience in accordance with DNFBPs Guidance requirements;
5.2.2.3. a good knowledge and understanding of AML/CTF matter, and PNG's AML/CTF laws;
5.2.2.4. fulfils fit and proper criteria issued by FASU; and
5.2.2.5. 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 compliance officer should also be able to directly communicate with, and report to, the Board of Directors/the firm's/practice's management and the FASU and must have sufficient time and resources to fulfil his or her obligations. The compliance officer is not required in all cases to be a member of the Board of Directors.

5.2.4. The compliance officer shall have access to relevant information concerning the practice/firm's clients, representatives of clients, business relationships, transactions and details of such transactions which a practice/firm enters into, or considers entering into, with or for a client.

5.3. What happens if you lose your compliance officer?

5.3.1. If your compliance officer permanently leaves your firm/practice or for some reason stops holding the position of compliance officer, you should appoint the deputy compliance officer (if you have one) to assume the responsibilities of the compliance officer, and replace the compliance officer as soon as possible.

6. Practice/Firm-Level Risk Assessment

> *i* *The Act sets out the obligations on risk assessment and establishing AML/CTF program for financial institutions under Part II (Division 1) Section 6-7, which also apply to DNFBPs, including legal professionals.*

6A. A key element of being able to forestall and prevent money laundering and counter the financing of terrorism is assessing your risk exposure to the same.

6B. This means looking at your practice, its activities, objectives, services provided, clients and transactions and considering what level of risk they may pose to money laundering or terrorist financing. This will often be determined as High, Medium or Low risk.

6C. 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. Your AML/CTF program must be established, implemented and maintained, based on your risk assessment.

6D. 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 or terrorist 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/CTF controls should apply as usual.

6E. Assessing risks requires you as a legal professional to have a sound understanding of the money laundering or terrorist financing risks in general and those applicable to your profession. You should also be able to exercise a good professional judgment. Above all, legal professionals should recognise the importance of a culture of compliance across their practice/firm and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of their practice/firm. This requires the allocation of necessary resources to gather and interpret information on money laundering or terrorist financing risks, both at the country and institutional levels, and to develop procedures and systems.

6F. In addition to assessing the overall risks your practice/firm may be exposed to when it comes to money laundering and terrorist financing, you must also undertake a risk assessment of every client, where they meet the due diligence thresholds. Further details on this are provided in the Client Due Diligence section. This section focuses solely on the overall risks you may face as a legal professional.

6G. You should develop the risk assessment in writing and store it electronically.

6H. When conducting the practice-wide risk assessment,[11] you should consider the following risk factors:

[11] A sample of a risk assessment is attached as ***Appendix A*** to FASU's *Guidance for Designated Non-Financial Businesses or Professions (DNFBPs) on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 2 of 2019).*

a). Client risks
b). Business activities or services risks
c). Geographical risk
d). Delivery channel risk

6.1. Client Risks

6.1.1. Legal professionals should determine based on their own criteria, whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment.

6.1.2. The following issues may indicate that a client is high-risk, such as:

6.1.2.1. Reluctance to provide relevant information or you are having reasonable grounds to suspect that the information provided is incorrect or insufficient;
6.1.2.2. Where a considerable part of their business or affiliations are in countries that may pose higher geographic risk;
6.1.2.3. The structure or nature of the company or relationship makes it difficult to identify the true beneficial owner or controlling interests, or clients attempting to obscure understanding of their business, ownership or the nature of their transactions;
6.1.2.4. PEPs and/or their family members and close associates;
6.1.2.5. Clients who have funds that are clearly and inexplicably disproportionate to their circumstances (e.g., their income, wealth or occupation);
6.1.2.6. Titling a residential property or business venture in the name of a third party (e.g., a friend, relative, business associate or another legal professional);
6.1.2.7. Clients that suddenly request for services in unusual and unconventional circumstances; and
6.1.2.8. Clients that are conduct cash-intensive businesses and are FIs or DNFBPs registered with FASU. These businesses include, for instance,
- money or value transfer services (MVTS);
- operators, brokers and other virtual assets service providers;
- casinos, betting houses and other gambling related institutions;
- dealers in precious metals and stones.

6.1.3. Some questions that you should consider to determine client risks are as follows:

6.1.3.1. Who are your clients? Are they high risk?
6.1.3.2. Are your clients, individuals or companies? If they are companies, do you know who owns or controls the companies?
6.1.3.3. If your clients are companies, are they regulated and required to follow the same or similar AML/CTF law and regulations?
6.1.3.4. Do your clients live locally or overseas?
6.1.3.5. How well do you know them? Do you know them personally or are they complete strangers?
6.1.3.6. Do you transact your business with them face-to-face or non-face to face (by correspondence, over the phone or by internet)?
6.1.3.7. Can you easily verify the information they have given you either because of personal knowledge or reliable documentation or information?

6.1.3.8. Are any of your clients or have any of your clients been previously suspected of illegal/criminal activity?

6.2. Business Activities and Services Risks

6.2.1. 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. When determining the risks associated with the provision of services related to specific activities, consideration and appropriate weight should be given to the following:

6.2.1.1. Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment;
6.2.1.2. Services where the client may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client) (e.g., through the practice/firms' general account and/or a personal or business account held by the legal professional himself/herself);
6.2.1.3. 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;
6.2.1.4. 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
6.2.1.5. 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.

6.2.2. Some questions that you should consider determining business activities and services risks are as follows:

6.2.2.1. What business activities and services do your practice/firm offer?
6.2.2.2. Do these business activities and services carry a higher risk of abuse for the purposes of money laundering or terrorist financing?
6.2.2.3. Do you often deal with clients who deal in large amounts of cash?
6.2.2.4. Are there any complex or unusual transactions occurring?
6.2.2.5. Does payment for your services come from regulated financial institutions such as banks who themselves are legally required to conduct money laundering and terrorist financing checks?
6.2.2.6. Do the services you offer allow you to know your client 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?

6.3. Geographical risks

6.3.1. Geographical risks of money laundering/terrorist financing may arise in a variety of circumstances, including from the domicile of the client, the location of the transaction, or the source of funds or source of wealth.

6.3.2. Countries with AML/CTF 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.

6.3.3. As a legal professional, 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 professional, you should observe the Public Statements issued by the FATF and Asia Pacific Group on Money Laundering (APG) 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. For more details on how to identify high-risk jurisdictions, refer to FASU's **Guidance for Reporting Entities to Raise Awareness on High-Risk Jurisdictions under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 4 of 2025).**

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

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

6.3.5.1. Do you do business with clients who reside in or whose money comes from sanctioned countries?
6.3.5.2. Do the countries where you do business follow and implement international rules and standards adopted to fight money laundering and terrorist financing?
6.3.5.3. Are there high levels of corruption and criminal activity in those countries?

6.4. Delivery Channel Risks

6.4.1. As a part of delivery channel risk, a legal professional should assess how its practice/firm delivers its services. Some questions that you should consider include:

6.4.1.1. The proportion and characteristics of clients you do not meet face-to-face;
6.4.1.2. How many of your matters rely on indirect contact with your client (e.g., via a representative or agent) rather than holding a direct relationship with the client;
6.4.1.3. How much of your activity is delivered online or via any other channel that may facilitate anonymity; and
6.4.1.4. The methods used to undertake identification, verification and general due diligence requirements.

6.5. Mitigating risk

6.5.1. As a legal professional, you should implement appropriate measures and controls to mitigate the potential ML/TF risks for those clients that, 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 employees to be adequately trained to identify and detect relevant changes in client 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 client is engaging in ML/TF activities. As a legal professional, 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 professional, develop a sound risk management policy or AML/CTF program 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.

6.6. External audit of risk assessment and AML/CTF Program

6.6.1. To assess the effectiveness of your risk assessment and AML/CTF program on a periodic basis, you should engage an external auditor, as required under the Act.

6.6.2. The frequency of conducting an external audit of your risk assessment and AML/CTF program varies from firm-to-firm, depending on the risks faced by your firm/practice.

6.6.3. FASU, by written notice, may also require you to engage an external auditor to conduct an audit of your risk assessment and AML/CTF program. The written notice will specify the matters to be covered by the audit, the form of audit report, and the timeframe to provide the audit report to FASU.

7. CDD Measures: Identifying, Verifying and Monitoring Clients

> *i* *The Act sets out the obligations on risk assessment and establishing AML/CTF program for financial institutions under Part II (Division 1) Section 6-7, which also apply to DNFBPs, including legal professionals.*

7A. The Act requires that DNFBPs, which include legal professionals, to apply a minimum standard of Client Due Diligence (CDD) to all business relationships when undertaking the relevant business. For you as a legal professional, this means when undertaking the services described in paragraph 2.1. above.

7B. A risk-based approach (RBA) should be applied to determine the extent of additional CDD measures commensurate with the level of risk posed by the client type, business relationship, transaction or product.

7C. CDD measures should allow you, as a legal professional, to establish with reasonable certainty the true identity of each of your clients.

7D. CDD is a crucial element in the role you can play in helping to identify and combat money laundering and terrorist financing. Knowing your client does not mean knowing your client's name and address. This can only be satisfied by understanding the client's business and his or her desired relationship with your professional service.

7E. You, as a legal professional, should apply each of the following CDD measures:

- Identification and verification of the client's identity;
- Identification of the beneficial owner of your client and taking reasonable measures to verify the identity of beneficial owner;
- Understanding the purpose and intended nature of the business relationship; and
- Conducting on-going due diligence on the business relationship.

7F. CDD measures should also be applied to verify the identity of any person purporting to act on behalf of the client, including if that person is authorised to do so.

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 clients 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. Remember, the purpose of the Act is to ensure that neither you nor your firm/practice inadvertently engages in or assist with money laundering or terrorist financing. Identifying who you, as a legal professional, 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 and terrorist financing. This is an incredibly important step in the fight against money laundering and terrorist financing as persons may try to hide their true identity – therefore, as a legal professional, you must take the necessary steps to establish who your client actually is.

7.1.5. While you, as a legal professional, may be able to obtain the CDD directly by asking the clients to supply the required information, the Act also assists you, and allows you to use reliable evidence as well as independent sources of documents, data or 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 client and matter risk assessments

7.2.1. Before you can undertake any type of due diligence on a client you should first undertake a client and matter risk assessment.

7.2.2. The purpose of the client and matter risk assessment is to determine the existence of any risks – with the client or even with that business 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/CTF requirements.

7.2.4. Risks come from a variety of factors and from different variables. In considering a client, you, as a legal professional, should consider the potential money laundering or terrorist financing risk that client poses. You need to consider, for instance:

7.2.4.1. what the client does and its business profile;
7.2.4.2. whether the structure, complexity or nature of the client entity or relationship makes it difficult to identify the true beneficial owner or any controlling interests;
7.2.4.3. whether the client appears to be attempting to obscure understanding of their business, ownership or the nature of their matters;
7.2.4.4. whether the instruction from the client is channelled through a third party and there is a lack of direct interaction with the client;
7.2.4.5. whether the client is based in a jurisdiction which carries a high risk of money laundering or terrorist financing; and
7.2.4.6. whether the client is a PEP; etc.

7.2.5. Matter risk assessment should focus on the specific risk factors that a matter presents, beyond the client risks already identified. Some of the questions you could ask to assess the matter risk is, for instance:

7.2.5.1. Are there any features in the matter which may represent higher risk?
7.2.5.2. Is the matter generally complex in nature?
7.2.5.3. Is the matter undertaken at short notice, within a short timescale or involving high volumes:

7.2.5.4. Does the matter involve new sources of finance (e.g., involving crowdfunding platforms or some aspects of bitcoins/cryptocurrencies)?

7.2.5.5. Does the matter involve trust or other legal entity company formation, management or service provision?

7.2.5.6. Is the matter routine for the practice, and if not, does the lack of experience or expertise add to the risk?

7.2.5.7. Do the source of funds or the parties to the matter frequently change?

7.2.5.8. Is the matter publicly funded from jurisdictions where corruption is prevalent?

7.2.6. There is no exhaustive list of factors to be considered for assessing client and matter risk. Therefore, you should look at your practice/firm's risk profile and the kinds of risks you are likely to face and then use these to form the basis of your client and matter risk assessment, which will guide you in what due diligence to undertake.

7.3. When should I carry out CDD?

7.3.1. You should undertake CDD **at the time of** establishing a business relationship **or before** effecting an occasional transaction (including wire transfers) which involves funds equal to or above K20,000.00 either as a single transaction or multiple transactions linked together**.**

7.3.2. Additionally, you must also undertake CDD:

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

7.3.2.2. when there are doubts about the integrity or adequacy of previously obtained due diligence data; and

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

7.3.3. When a suspicion of money laundering or terrorist financing arises during the due diligence review process, you should refuse to engage in services with the potential client, so that you do not handle potentially illegal or criminal funds and so that you don't accidently become involved in money laundering or terrorist financing. At this stage, you should also consider whether a SMR should be made to the FASU (further details of this are provided below).

7.4. What information must I collect and keep?

7.4.1. You must collect (and maintain) due diligence on all your clients that requires you to engage in the activities specified at paragraph 2.1. of these Guidance Notes.

7.4.2. **Individuals**

7.4.2.1. You, as a legal professional, should obtain relevant information on the identity of your individual clients and seek to verify the relevant information on a risk sensitive 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 client. The relevant information should include:

7.4.2.1.1. Full legal name;
7.4.2.1.2. Date of birth;
7.4.2.1.3. Place of birth;
7.4.2.1.4. Nationality;
7.4.2.1.5. Residential address;
7.4.2.1.6. Contact details (telephone number, email address);
7.4.2.1.7. Occupation;
7.4.2.1.8. Place of business or employment; and
7.4.2.1.9. Purpose of business.

7.4.3. **Corporate Clients (Companies)**

7.4.3.1. Where the client is a **corporate client/company,** the relevant information should include:

7.4.3.1.1. Full name of the company;
7.4.3.1.2. Company address (principal place of business);
7.4.3.1.3. Type of business the company engages in;
7.4.3.1.4. Company registration/identification number;
7.4.3.1.5. Date and place of incorporation, registration or formation;
7.4.3.1.6. The address of the registered office in the country of incorporation;
7.4.3.1.7. If applicable, the address of the registered agent of the company to whom any correspondence may be sent;
7.4.3.1.8. Details of the identity of each director of the company, and any persons who are beneficial owners of the company; and
7.4.3.1.9. Recent financial information or audited statements, depending on the nature of the transaction.

7.4.3.2. 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.

7.4.4. **Trusts/Foundation**

7.4.4.1. Trust business is typically regarded as inherently risky because of the confidentiality associated with these structures. Where the client is **a trust or a foundation or non-profit organisation,** the following relevant information should be obtained:

7.4.4.1.1. Name of the trust/foundation;
7.4.4.1.2. The date and country of establishment;
7.4.4.1.3. The nature and purpose of the trust/foundation;
7.4.4.1.4. Country of establishment;
7.4.4.1.5. 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;
7.4.4.1.6. Information of person(s) with powers to add beneficiaries, where applicable;

7.4.4.1.7. Information on the person providing the funds, if not the ultimate settlor; and
7.4.4.1.8. If there is an acting agent, their name and address.

7.4.4.2. 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.

7.4.4.3. 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 Act and DNFBPs Guidance set a minimum standard for acting in these cases. If you, as a legal professional, are of the view, based on the circumstances of your client, transaction or matter, that additional information must be sought in order to manage any risks, you should seek and record that information.

7.5. Verifying Identity

7.5.1. Verifying identity effectively means confirming that the persons 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 professional to rely on a client's claim that they are who they say they are. Verification of that information **must** take place.

7.6. What is Enhanced Customer Due Diligence ("ECCD")?

7.6.1. ECDD is the extra due diligence steps a legal professional take when dealing with a client that has a higher risk of money laundering or terrorist financing, irrespective of the nature or form of the transaction. ECDD is applied to all higher risk categories of clients, business relationships, or transactions.

7.6.2. ECDD measures are designed to assist legal professionals 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 professionals to take extra steps and precautions to reduce the likelihood that they may inadvertently aid in money laundering, or terrorist financing.

7.6.3. ECDD measures include:

7.6.3.1. Requesting and receiving additional information and data on the nature of customer's business, administration, as well as the source of funds and source of assets or wealth;

7.6.3.2. 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 professional decide whether or not they want to do business or take money from the client.

7.6.3.3. Escalating internal approval to ensure that senior management is aware of the higher risk a transaction poses and approve in writing doing business or taking funds from them.

7.6.3.4. Increasing your controls and ongoing monitoring of the higher risk clients, business relationships and transactions.

7.6.4. In order to implement ECDD measures, you may also require the physical presence of the customer and its representatives prior to establishing a business relationship.

7.7. When should ECCD measures be applied?

7.7.1. ECDD should be applied in instances where a client is considered high risk or is deemed to carry a higher risk of money laundering or terrorist financing. Each legal professional will have its own criteria for determining risk ratings and what criteria would carry a higher risk.

7.7.2. However, by Act and DNFBPs Guidance, the ECDD measures must be applied by a legal professional when they 'take the view' that the customer is:

7.7.2.1. a resident in a high-risk country or jurisdiction; or
7.7.2.2. involved in a high-risk business activity; or
7.7.2.3. a politically exposed person (PEP); or
7.7.2.4. presents a situation where the money laundering or terrorist financing is high; or
7.7.2.5. not physically present for the purposes of identification.

7.7.3. For more details on the application of ECDD measures by registered entities, refer to FASU's **Guidance for Reporting Entities to Raise Awareness on Enhanced Customer Due Diligence under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 3 of 2025).**

7.8. 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?

7.8.1. As noted above, it remains a fundamental part of an effective AML/CTF regime, that a client is identified, and due diligence undertaken on them. This remains the case even if you know them personally. In essence, the Act requires that you collect appropriate and relevant due diligence information relating to a person's identity and business relationship and verify this information to ensure that the information obtained is correct. However, Section 22 of the Act does allow **simplified due diligence** in certain circumstances when:

7.8.1.1. you do not suspect money laundering or terrorist financing; and

7.8.1.2. the customer is not a resident in a high-risk country;

7.8.1.3. you take the view that the customer is low-risk.

7.8.2. It is also important to keep in mind that, at any given time the FASU or any competent authority may ask to see the documentation you hold on file for a client. It would not be sufficient to say you did not gather the due diligence because you know the client 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 practice/firm.

7.9. Face to Face Versus Non-Face to Face Clients

7.9.1. The Act explicitly provides that non-face to face clients are higher risk than face-to-face. Where a client 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.

7.9.2. If, however, a client is not face-to-face or generally unknown to a legal professional, 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 professional 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 client.

7.9.3. One such additional measure is requiring certified documentation to be presented. In the case of individuals, you shall require a minimum of two pieces of certified formal identification and one formal document to verify the physical address of a non-face-to-face client. For instance, two government issues IDs, and utility or electricity bill. In the case of a legal person, you shall require a certified copy of acceptable identification and address documents to verify the address. For instance, a company certificate or registration document.

7.9.4. In the case of non-face-to-face business relationships, the first payment, at a minimum, shall be carried out through an account in the client's name with a financial institution which is subject to internationally recognised due diligence standards.

7.10. Certificate of documents for CDD

7.10.1. 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.

7.10.2. 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.

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

7.10.3.1. 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:

7.10.3.1.1. judicial officer/senior public officers like a police officer or immigration officer or a registrar;
7.10.3.1.2. a legal professional, medical practitioner or accountant or any profession with established rules of professional conduct; or
7.10.3.1.3. a notary public or commissioner for oaths;

7.10.3.2. 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);

7.10.3.3. 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.

7.11. What if I cannot get due diligence on the client?

7.11.1. If a client 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 or terrorist financing.

7.11.2. 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.

7.11.3. In such instances, the Act require that the legal professional should file a SMR with the FASU. This would generally be undertaken by the compliance officer.

7.11.4. The requirement to file a SMR with FASU also applies where a client fails to provide adequate due diligence information or evidence to verify their identity.

7.11.5. You should, however, look at every situation and every client independently to determine if there are reasonable factors why a client cannot, or is unable to, provide you with the due diligence information or if you can find another way to verify the information the client is providing. For instance, there may be circumstances where some clients are unable to supply the identity documents. Such clients can include a minor, the elderly, the disabled and individuals that are dependent on the care of others. As the legal professional, you will have to determine what alternate identity documentation to accept and what verification procedures to employ.

7.11.6. 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 or terrorist financing, you can continue with the transaction.

7.11.7. However, as a general rule, if a client 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 a SMR with FASU.

7.12. Monitoring and Ongoing CDD

7.12.1. In instances where you have an ongoing business relationship with clients, you will need to monitor and update the due diligence information from time to time depending on the risk profile of the client as you continue the relationship.

7.12.2. If the continuing relationship is considered to present a higher risk, you should review and update the information on them on a more regular basis (e.g., once per year or earlier). Since a high-risk relationship is more at risk of potentially being involved in money laundering or terrorist 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 your client's money. In certain circumstances, you may even consider whether putting in place ongoing monitoring systems would be appropriate.

7.12.3. If the continuing relationship is considered to present a normal or low risk, you must conduct a review and update their information as appropriate (e.g., every three or four years). The existing controls within the firm will determine when to elevate the risk profile of a client.

7.12.4. In the event you suspect that a client, whether high, medium, or low risk, may be involved in money laundering or terrorist financing, or engages in activity that causes a suspicion of the same, you **must** take action immediately. You must review the client and the transactions, address your suspicions, and take the necessary action, even if you are not yet at the annual review or updating period.

7.12.5. Always remember that the duty to report suspicious matters to FASU is an ongoing one. Details on suspicious mater are elaborated in **item 10** of this Guidance.

7.13. Monitoring transactions

7.13.1. Where you have ongoing relationships with clients, in addition to checking due diligence, you are also required to have procedures for monitoring their transactions so that you can determine if a transaction is out of the norm.

7.13.2. Transactions that are out of the norm or deviate from what is a normal pattern of activity should be grounds for further assessment to determine whether it rises to a level of suspicious activity/suspicious transaction to make a report. *For example*, if a client changes how or where the payments are coming from or has someone else make payments for them, that could be considered unusual, and you should ask additional questions. Always verify this or take additional measures to make sure the instructions are genuine. A situation such as this does not automatically mean that money laundering or terrorist financing is occurring as there could

very well be a reasonable explanation for the change, however, in order to prevent any risk of the same, you should ensure that you verify transactions such as these.

7.13.3. The ongoing monitoring requirements are in addition to the updating due diligence requirements above. *For instance*, where a relationship is risk-rated as normal, and due diligence is updated at regular intervals, an instance may occur that is outside of the normal course of business. Therefore, waiting for the normal updating period to update their information would no longer be appropriate and you would be required to take immediate steps to ensure that you or your firm is not at risk of being abused for money laundering or terrorist financing purposes.

7.14. CDD on existing clients or business relationships

7.14.1. A legal professional shall also carry out CDD on the existing clients or business relationships in the following circumstances:

7.14.1.1. When receiving or disbursing funds on behalf of a client in a transaction that singularly, or in several transactions that appear to be linked, equal or exceed K20,000.00; or

7.14.1.2. when there is a material change in the nature of the relationship with the client; or

7.14.1.3. when you become aware that you lack sufficient information about an existing client, or concerned about the accuracy of information recorded in file; or

7.14.1.4. where a SMR has been reported, or a subpoena or production order has been received, or where relevant negative information is known.

8. Record Keeping

8.1. What records must a legal professional keep?

8.1.1. All legal professionals must comply with the record keeping requirements outlined within the Act. The documents you are required to keep, range from CDD-related 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 professionals are required to keep are:

8.1.2.1. Records of all transactions with clients;
8.1.2.2. CDD measures carried out on clients;
8.1.2.3. Copies of all "internal" SMRs made to the compliance officer, and any investigations undertaken; and
8.1.2.4. Copies of all "external" SMRs made to the FASU; and
8.1.2.5. Internal risk assessment, AML/CFT program, and audits undertaken of AML/CTF controls; and
8.1.2.6. Details of any AML/CTF training completed, including dates of training sessions, description of training provided, and name of employees who attended the training.

8.1.3. More specifically, legal professionals shall keep:

8.1.3.1. **Legal professional's organisational records**

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

8.1.3.2. **Due diligence and identity records**

Where you have undertaken due diligence on a client, you must ensure you keep a record of this due diligence. CDD and ECDD are integral to an effective functioning AML/CTF regime. Therefore, it is important that all records are kept in a manner that allows you, as the legal professional, to maintain active oversight in the case of ongoing business relationships.

8.1.3.3. **Transaction records**

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

8.1.4. Additionally, the records must be able to show and explain the legal professional's transactions, within and outside of the territory.

8.2. How should the records be kept?

8.2.1. As a legal professional, 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.

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 professional to decide how it chooses to store and keep these records. However, you must ensure that the criteria provided within the Act and covered above are included.

8.3. How long must records be kept?

8.3.1. Records must be kept for a **minimum of seven (7) years**. For transactions, the time period is seven (7) years after the completion of the last transaction or series of transactions, including occasional transaction.

8.3.2. FASU may ask you to keep records for a longer period in some circumstances.

9. Training

9A. All legal professionals are subject to the employee training requirements outlined within the Act and the DNFBPs Guidance.

9B. With this in mind, you, as a legal professional, are required to ensure that your employees receive appropriate and relevant training so that they understand how your practice/firm can be mis-used to facilitate money laundering and terrorist financing, including money laundering and terrorist financing risks, techniques, methods and trends. They should also understand their obligations in relation to the same as well as the practice/firm's policies, processes and procedures for spotting and stopping potential money launderers or terrorist financiers from abusing your practice/firm.

9C. Training should include information to help employees understand what money laundering and terrorist financing mean and have a knowledge of what AML/CTF laws apply to legal professionals in PNG.

9D. The training requirements applicable are not limited to any particular class or rank of employees, although key training requirements will be applicable to some (e.g., the compliance officer).

9.1. Why is training important?

9.1.1. Training is not only a legal requirement, but it is also what allows employees and senior management to understand concepts that might be new to them, like what is money laundering and terrorist financing. It also helps employees 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 and terrorist financing, and what they should do if they ever come across instances of money laundering and terrorist financing.

9.1.2. Your employees are the frontline defence and are critical in deterring, detecting, and preventing money laundering and terrorist financing. Employees are the ones who generally have client contact or may ultimately accept or process clients' 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 employees 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 or terrorist financing.

9.1.3. In addition, ensuring all employee receive the proper training not only aids in the fight against money laundering and terrorist 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 employees is a breach of legislation that can result in fines and penalties from FASU.

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. All employees within the firm of the legal professional are responsible for this. Therefore, all employees should receive some sort of applicable training.

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

9.2.3. Any new employees joining the firm should be provided training on AML/CTF upon the commencement of their employment.

9.3. What should the training be on?

9.3.1. As noted, it is critical to the prevention and detection of ML/TF that employees understand money laundering and terrorist financing and the issues that arise from those activities. Therefore, training on money laundering and terrorist 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 employee. For instance, the compliance, senior management, or directors will require more in-depth AML/CTF training than more junior level employees 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 and terrorist financing so that the employees understand what these are, how they may affect PNG and the legal professional industry, as well as their role in preventing money laundering and terrorist financing.

9.3.3.2. Relevant legislation on AML/CTF in the PNG, including the provisions of the Act and related guidance.

9.3.3.3. The policies, processes, procedures, and internal controls in place within your organisation to deal with and fight money laundering and terrorist financing, including suspicion escalation procedures and record keeping.

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

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

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

9.4. How often should the training take place?

9.4.1. Training should be provided on regular basis, and it must occur at least annually. 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 employees are aware of their obligations, as it relates to AML/CTF.

9.4.2. Senior managers and compliance officer shall be given AML/CTF training immediately on assumption of their duties.

9.4.3. Any other new employees joining the firm shall be trained on their AML/CFT obligations under the Act and gain an understanding of the ML/TF risks associated both with their sector and the firm.

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

9.5. What records of the training must be kept?

9.5.1. You should keep a record of the training each employee 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 professionals 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 seven (7) years.

9.6. Where can I get training?

9.6.1. If you have someone knowledgeable within your practice/firm, you may be able to have your own internal workshops or seminars on specific AML/CTF concerns relevant to your industry.

9.6.2. There may also be private firms in the PNG that can provide specific training for your practice/firm and employees as well as general online training on AML/CTF 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 to ensure the effectiveness of training.

10. Identifying and Reporting Suspicious Matters

10.1. What is a suspicious matter?

10.1.1. The term *suspicious matters* generally includes both *suspicious activity* and *suspicious transaction*, which are further explained in the sections below.

10.2. What is suspicious activity?

10.2.1. 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 institution/business in undertaking its general operations and activities. Additionally, you will need to factor in the types of customers a reporting entity deals with.

10.2.2. Suspicious activity could refer to any incident, event, individual or activity that seems out of place or at odds with your institution/business usual activity. An *example of suspicious activity* is the reluctance on the part of a potential customer to provide documentation required to conduct CDD/ECDD. Generally, suspicious activity will identify potential instances of money laundering, terrorist financing, or other illegal activity.

10.3. What is suspicious transaction?

10.3.1. Suspicious transactions are transactions in which there are reasonable grounds to suspect that the funds or goods involved are linked to 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).

10.4. Unusual vs. Suspicious

10.4.1. There may be instances where customers 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 a reporting entity is dealing.

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

10.4.3. Unusual activity or an unusual transaction should not automatically result in the filing of a SMR with the FASU. 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, 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 usual transactions. However, it may not be suspicious because there may be a reasonable explanation for the deviation.

10.4.4. 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.

10.4.5. See also section on **What is tipping off?** below.

10.5. Reporting suspicious matters

10.5.1. There are times when a customer, or a potential customer attempts 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 other criminal offence is being attempted or is occurring, this suspicion **must** be reported.

10.5.2. Suspicious matters may also include, but are not limited to, inquiries or actions made by a customer, potential customer or other person; initiation of account-opening business engagement; preparation for the conduct of transactions; or events that may arise out of compliance with Section 19 of the Act - where CDD cannot be completed.

10.5.3. If you are an employee of the reporting entity, your suspicion must be reported to the reporting entity's compliance officer and should be in writing, in accordance with the institution/business' procedures. Most often, firms have an internal suspicious activity or transaction form ready to be used by their employees to report suspicions.

10.5.4. Your compliance officer 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 or terrorist 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 or terrorist financing that would require the filing of a SMR with the FASU.

10.5.5. You should note that determining whether or not a transaction results in a suspicion of money laundering or terrorist financing, is a very objective matter[12]. If you are in any doubt, you should file a report with your reporting entity's compliance officer.

10.5.6. As an employee, once you have submitted your SMR to your compliance officer, your duty to report a suspicion will be discharged, provided you follow the reporting entity's protocols in doing so.

[12] "Objective matter" is based on verifiable data, observable events, and factual evidence.

10.6. Reporting suspicious matter to the FASU if you are a compliance officer

10.6.1. If you are the compliance officer within the a financial institution or a DNFBP, once you make the determination that there are grounds for a suspicion of money laundering, terrorist financing, or other criminal activity, you are required to submit a SMR in writing to the FASU, in the form available from the website of the Bank of PNG.

10.6.2. If after a review and analysis of the facts and circumstances, the compliance officer 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, or some other form of criminal activity, the compliance officer should still, and must under the law, file a SMR with FASU.

10.6.3. The compliance officer's job is not to investigate and then definitively state that money laundering or terrorist financing is occurring. On the contrary, the role of the compliance officer 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 information to support a reasonable suspicion that that information is relevant for the purposes of Section 41(1) (a)-(c) of the Act.

10.6.4. Filing a SMR with FASU and providing the relevant information and reasons for your suspicion or potential suspicion, gives FASU the ability to conduct financial analysis and produce intelligence on possible ML/TF, or other criminal offences for dissemination to law enforcement agencies and stakeholders for further investigation and enforcement action.

10.7. When must I submit a SMR?

10.7.1. A SMR must be made as soon as reasonably practicable and in any event **within five (5) working days** from the date the suspicion[13] first arose.

10.7.2. You must always remember that SMRs are used by FASU and law enforcement for the purposes of AML/CTF. For this to happen, it is imperative that FASU receives information in a timely manner to execute its mandated functions.

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

10.8.1. Yes, under the Act, a reporting entity is 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 conduct financial analysis, produce intelligence and disseminate it to trigger or support law enforcement actions to combat ML/TF or other criminal activity or attempted criminal activity. Also remember, that just because you, as a reporting entity, has turned away a customer, or not gone through with an activity, does not

[13] "Suspicion" in this context refers to a suspicion based on reasonable grounds that the information it knows is relevant for the purposes set out in section 41(1)(a)-(c) of the Act.

mean that they will not attempt to approach another reporting entity 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 a SMR?

10.9.1. When submitting a SMR to FASU, you must remember that you are doing so in large part to assist the authorities to track down and stop any suspected money laundering or terrorist financing from occurring or continuing. Therefore, your SMRs should be clear, provide as many relevant details as possible and most of all must identify the facts or reasons why you suspect that information is relevant for the purposes set out in Section 41 (1) (a)-(c) of the Act.

10.9.2. Please refer to **Appendix E** of FASU's *Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No.1 of 2019)* or the SMR form from the website of the Bank of PNG that you are required to submit to the FASU. It provides details of the information you are required to submit in the SMR if you become aware of suspicious activity or a suspicious transaction.

10.10. Keeping a register of SMRs

10.10.1. As part of the record keeping requirements, you, as a reporting entity, should keep a record of all SMRs submitted to your compliance officer as well as all SMRs submitted to the FASU.

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 SMRs filed.

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 SMRs made to your compliance officer;
- 10.10.3.2. Details of the external SMRs made to FASU;
- 10.10.3.3. Details of the decisions made by the compliance officer in relation to SMRs as well as steps taken with regards to investigating an internal report and the basis for the decisions;
- 10.10.3.4. Date of FASU's acknowledgement/confirmation letter;
- 10.10.3.5. FASU reference number.

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

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

10.11. What is tipping off?

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

10.11.2. Tipping off is a criminal offence under Sections 43 and 44 of the Act, which attracts penalty fines, ranging from K25, 000 – K500, 000 or up to 3 years imprisonment term, or K500,000 – K1,000,000 fine for a body corporate.

10.11.3. When you make a SMR, you must keep the information confidential and not discuss it further unless the relevant persons within the reporting entity or the authorities require you to speak about it, and this must only be in accordance with the direction provided by FASU and in accordance with the Act.

10.12. Is threshold transaction reporting different from SMRs?

10.12.1. The requirement to report SMR is in line with Section 41 of the Act. It is different from the requirement to report a Threshold Transaction Report (TTRs) and an Asset of Designated Persons or Entities Report (ADPER) that are pursuant to Sections 39 and 40 respectively. The Act requires you to file four different types of reports to FASU, which includes:

10.12.1.1. Section 39 – Threshold Transaction Reports (TTRs);

a) Domestic TTR[14]

b) International TTR[15] known as an International Electronic Funds Transfer Report (IEFTR)

10.12.1.2. Section 41 – Suspicious Matter Reports (SMRs); and

10.12.1.3. Section 40 – Asset of Designated Persons or Entities (ADPER).

10.12.2. TTRs are different from SMRs. TTRs have requirement for both domestic and international transactions. A entity **must** report any domestic and international transaction involving a large sum of cash or cash equivalent in the form of a bearer negotiable instrument that is K20,000 or more, even if it is not suspicious. Such a transaction may be carried out as a single transaction, or two or more transactions that appear to be linked. The link between the two transactions can be identified in various ways. *For example*, an individual may carry out a number of transactions from the one account on the same day, or a number of customers may carry out transactions from the same account on the same day. Note that "linked transactions" is not defined under Section 5 of the Act. However, Section 46(2) gives some guidance on information that will be relevant to identify "linked transactions". Linked transactions are an important consideration when submitting TTRs, IEFTRs, SMRs and ADPERs. As for ADPER, the report relates to assets that are in the custody of a reporting entity that belongs to a person that has been designated under Section 12(e)(i) of the *United Nations Financial Sanctions Act* 2015. For more details on linked transactions, refer to FASU's

[14] Section 39 (1) of the Act
[15] Section 39 (2) of the Act

Guidance for Reporting Entities to Raise Awareness on Identification of Linked Transactions under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 5 of 2025).

10.12.3. You must submit a TTR, IEFTR and ADPER to FASU as soon as reasonably practicable, and no later than 10 working days from the date of the transaction(s). Refer to **Appendix C** of *FASU's Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No.2 of 2019)* for a copy of the TTR, IEFTR and ADPER or download TTR form, IEFTR form and ADPER form from the website of the Bank of PNG.

11. AML/CTF Program

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

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

11.1.2. Creating AML/CTF program can often seem like an overwhelming task, but it is nothing more than an internal reference document that explains to everyone what your firm/practice 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 AML/CTF program will differ from firm-to-firm or practice-to-practice because the type of activities, clients and money received or dispersed, will differ.

11.1.4. Your AML/CTF program must be approved by your senior management and the Board of your organisation. You must keep a record of senior management's approval of the AML/CTF program in writing, which includes it being stored electronically, and able to produce it upon request by FASU.

11.2. What information should be in your AML/CTF Program?

11.2.1. Your practice or firm's AML/CTF program will be the main reference document that gives employees the guidance they need to understand their obligations and the internal procedures they must follow in order to meet the required AML/CTF obligations.

11.2.2. As such, it is of vital importance that your practice/firm's AML/CTF program reflects its specific activities and operations.

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

11.2.4. Key elements and sections to focus on in the AML/CTF program include, but are not limited to, the following:[16]

11.2.4.1. **A policy statement:** The policy statement should, among other things, discuss your practice/firm's commitment to fight money laundering and terrorist financing. It should also specifically outline your practice/firm's activities and how and where in those activities the practice/firm may be at risk for money laundering or terrorist financing.

11.2.4.2. **Definitions and explanations of money laundering and terrorist financing:** This section should include the definitions of money laundering and terrorist financing and should specify the PNG's legislation that governs your AML/CTF obligations, as a legal professional. 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 AML/CTF program will essentially explain the requirements, what your practice/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 AML/CTF program and will cover all of the topics covered within this guidance, namely:

11.2.4.4.1. Undertaking risk assessments;
11.2.4.4.2. Establishing internal controls;
11.2.4.4.3. Client Due diligence;
11.2.4.4.4. Compliance Officer;
11.2.4.4.5. Suspicious matter reporting;
11.2.4.4.6. Record keeping; and
11.2.4.4.7. Employee training.

The AML/CTF compliance program shall also include details on targeted financial sanctions, sanctions screening and implementation (see section 12 below).

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

11.2.4.6. **Employee screening:** To ensure that employees are fit and proper, the AML/CTF program shall also include details on conducting screening of potential employees.

[16] Please refer to the sample of an AML/CTF Program attached as ***Appendix B*** to FASU's *Guidance for Designated Non-Financial Businesses or Professions (DNFBPs) on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 2 of 2019).*

11.2.4.7. **Templates:** To assist your employees, you should also consider whether it is appropriate to include your practice/firm's relevant templates in the manual (e.g., internal SMR reporting form).

11.2.5. Please note that each practice/firm's AML/CTF compliance program will need to be specific and tailored to each practice/firm and should detail procedures that are in line with the level of risk your business/firm has to money laundering and terrorist financing.

12. Targeted Financial Sanctions

12A. Legal professionals shall implement a comprehensive Targeted Financial Sanctions Compliance Program.

12B. Legal professionals shall conduct the screening of their clients to determine if their client or their beneficial owner(s) or senior management is designated under the sanctions list, as approved under Part II of the *United Nations Financial Sanctions Act* (UNFSA) *2015*.

12C. Upon screening, if any matches are identified with the sanctions' lists, you shall undertake the following actions, depending on the nature of the match observed (confirmed or partial match where the legal professional is unable to determine if it is a confirmed match or a false hit):

a) Immediately and directly apply adequate TFS measures, as prescribed in the Act and *UNFSA 2015*. These measures include immediately suspending or terminating the business relationship, transaction, transfer, financial or other related services, as well as immediate freezing of the funds and other assets that are owned, directly or indirectly, by such designated individuals and entities;

b) Filing an Asset of a Designated Person or Entity Report (ADPER) Form as soon as is reasonably practicable and in any event within 10 working days from the date it receives notification of a designation under Section 12(e)(i) of the *UNFSA* 2015, without prior notice to the suspected person(s), with FASU. The form is attached as **Appendix E** in FASU's *Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No.1 of 2019)* or download ADPER form from the website of the Bank of PNG.

The report filed to the FASU under b) above should include the data for the identification of assets and other properties, data regarding ownership and other interests thereto, as well as explanations for the motives on which the pertinent TF data were grounded.

12D. Legal professionals are also required to conduct ongoing monitoring of their customers and transactions to ensure compliance with sanctions. This includes screening customers and transactions against updated lists of designated persons and entities provided by the PNG Sanctions Office on their website https://pngsanctionssecretariat.gov.pg/consolidated-list/.

12E. Legal professionals must establish and maintain effective internal controls, policies and procedures to comply with TFS. Employees training on sanctions compliance and the identification of designated persons or entities is also required.

12F. You shall also maintain records of actions taken to comply with sanctions, including identification and freezing of assets, for a specified period as required by applicable laws.

References and Contacts

PNG's AML/CTF Framework

Information on the Act and PNG's regime can be found at www.bankpng.gov.pg

- PNG's *Anti-Money Laundering and Counter Terrorist Financing Act* 2015: https://www.bankpng.gov.pg/sites/default/files/2024-09/1-No-20-of-2015-Anti-Money-LaunderingCounter-Terrorist-Financing-Act-2015.pdf
- PNG's *Criminal Code Act* 1974: http://www.paclii.org/pg/legis/consol_act/cca1974115/
- PNG's *Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act* 2015: https://www.bankpng.gov.pg/sites/default/files/2024-09/No-21-of-2015-Criminal-Code-Money-Laundering-Terrorism-FinancingAmendment_Act-2015.pdf
- PNG's *Mutual Assistance in Criminal Matters (Amendment) Act* 2015: https://www.bankpng.gov.pg/sites/default/files/2024-09/No-22-of-2015-Mutual-Assistance-in-Criminal-Matters-Amendment-Act-2015.pdf
- PNG's *Proceeds of Crime Act* 2005: http://www.paclii.org/pg/legis/consol_act/poca2005160/
- PNG's *Proceeds of Crime Act (Amendment)* 2015: https://www.bankpng.gov.pg/sites/default/files/2024-09/No-23-of-2015-Proceeds-of-Crime-Amendment-Act-20153.pdf
- PNG's *United Nations Financial Sanctions Act* 2015: https://www.bankpng.gov.pg/sites/default/files/2024-09/No-24-of-2015-United-Nations-Financial-Sanctions-Act-20151.pdf

Asia Pacific Group on Money Laundering (APG): http://www,apgml.org

Financial Action Task Force (FATF): http;//www.fatf-gafi.org

For queries about this Guidance, please contact:

Bank of PNG, Financial Analysis and Supervision Unit
PO Box 121, Port Moresby, National Capital District
W: www.bankpng.gov.pg
E: *fasu@bankpng.gov.pg*
T: +675 322 7147