2025

Financial Analysis and Supervision Unit

Guidance for Reporting Entities to Raise Awareness on Ongoing Transaction Monitoring under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 7 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	06.08.25	Draft	Asian Development Bank Consultant
2	21.08.25	Draft	FASU
3	30.08.25	Draft	Asian Development Bank Consultant
4	26.09.25	Final	FASU

Table of Contents

Table of Acronyms

Act	Anti-Money Laundering and Countering Terrorist Financing Act 2015
AML/CTF	Anti-Money Laundering/Counter Terrorist Financing
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
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. You must rely on the technical definitions of these terms as stipulated in the Act. Only for the purpose of assisting reporting entities 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 reporting entity carries out a transaction; or with whom a reporting entity 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. **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;
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.

1.4. **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,

[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.

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.

1.5. **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:

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

1.5.2. monitor and enforce compliance with the Act; and

1.5.3. 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.

1.6. **Financial Institutions (FIs),** as defined in Section 5 of Act, includes a commercial bank, micro bank, finance company, savings and loans society, insurance company, insurance agency and broker, brokerage firm, superannuation fund, leasing company, funds management company and money changer.

1.7. **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.

1.8. **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.

1.9. **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.

1.10. **Reporting Entity** means financial institutions and DNFBPs that have a legal requirement to comply with the Act and includes entities that are required to be registered with FASU pursuant to Section 57 of the Act.

1.11. **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.

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

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

2. Note to Reading this Guidance

> **!** **This Guidance intends to raise awareness to reporting entities on the requirements of 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 to both FIs and DNFBPs (hereafter jointly referred to as 'reporting entities').

2.3. This Guidance aims to assist and improve reporting entities' understanding and implementation of ongoing due diligence and transaction monitoring requirements as outlined in the Act.

2.4. Ongoing monitoring of the business relationship with customers helps detect unusual activity. If unusual activity cannot be rationally explained, it may indicate potential money laundering or terrorist financing. Ongoing monitoring of customer activity and transactions that take place throughout a business relationship helps reporting entities' to better know their customers, assess risk more effectively, and provides greater assurance that their products or services are not being exploited to facilitate financial crime.

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

a). *Guidance for Financial Institutions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No. 1 of 2019)* (issued on 20 May 2019);

b). *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

c). *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)*.

2.6. This Guidance intends to provide industry guidance, practical assistance and a means for reporting entities to better comply with their anti-money laundering and counter terrorist financing (AML/CTF) obligations under the Act.

2.7. 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.

2.8. Reporting entities should develop their own AML/CTF internal policies, procedures and controls tailored to their business needs.

2.9. 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 reporting entities 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 reporting entities, including on penalties for non-compliance with obligations under the Act.

3. Requirements under the Act

> *i* *The Act sets the requirements to conduct ongoing due diligence for financial institutions and DNFBPs in Sections 17 and 52, respectively.*

3.1. Under Section 17 of the Act, reporting entities are required to conduct ongoing due diligence in respect of all its business relationships.

3.2. When conducting ongoing due diligence, reporting entities are required to do the following, at a minimum:

3.2.1. maintain current and up to date information and records relating to its customers and their beneficial owners; and

3.2.2. ensure that transactions carried out on behalf of their customers are consistent with their knowledge of the customer, the customer's commercial or personal activities and risk profile, and where necessary, the source of funds; and

3.2.3. ensure that ongoing enhanced customer due diligence (ECDD) is conducted with respect to PEPs in accordance with Section 29(3)(b) of the Act.

3.3. In addition to the above, FIs, as a part of ongoing due diligence obligations, are also required under the Act to ensure that ongoing ECDD is conducted with respect to correspondent banking relationships in accordance with Section 34(2) of the Act.

4. On-going CDD and Monitoring

4.1. What is on-going CDD and monitoring?

4.1.1. In instances where you have an ongoing business relationship with customer, you are obliged to monitor and update the due diligence information on your customer from time to time.

4.1.2. As a part of your ongoing CDD obligations, you must do the following, at a minimum:

a) undertake review of existing records and keep documents, or information obtained for the purposes of applying CDD on your customers and their beneficial owners, up to date;

b) undertake scrutiny of transactions undertaken throughout the course of your business relationship (including, where necessary, the sources of funds) to ensure that transactions are consistent with your knowledge of the customer, their commercial or personal activities ,and their risk profile;

4.1.3. In order to comply, you should:

a) renew and re-evaluate CDD at appropriate intervals (including during the course of a given transaction) while applying a risk-based approach (RBA), which however becomes necessary in certain circumstances as mentioned under What circumstances triggers ongoing monitoring? below; and

b) suspend or terminate a business relationship until you have updated information or documents.

4.1.4. You must put into place appropriate monitoring processes and operate a system of regular review and renewal of CDD and take RBA. *For instance,* 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 should 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 using technology would be appropriate.

4.1.5. 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).

4.1.6. However, 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.

4.1.7. Always remember that the duty to report suspicious matters to FASU is an ongoing one.

4.2. What is ongoing transactions monitoring?

4.2.1. As mentioned under Section 4.1.2. above, where you have ongoing relationships with customers, in addition to regularly updating their CDD on the basis of RBA, you are also required to have procedures for monitoring their transactions so that you can determine if a transaction is out of the norm.

4.2.2. 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.

4.3. What circumstances triggers ongoing monitoring?

4.3.1. 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.

4.3.2. You must update the CDD when you become aware of any changes to customer's identification information. This would include change of name, address, beneficial owner or business.

4.3.3. You must also carry out ongoing monitoring on your existing customers or business relationship in any of the following circumstances:

4.3.3.1. when you become aware that the circumstances of the existing customer have changed (e.g., any indication of the change in the identity of customer or beneficial owner; or any transactions not reasonably consistent with your knowledge of the client); or

4.3.3.2. when there is a material change in the purpose or nature of the relationship with the customer; or

4.3.3.3. 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

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

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

4.3.3.6. any other matter which may affect your assessment of the money laundering or terrorist financing risk in relation to the client.

4.4. What records are to be maintained related to ongoing monitoring?

4.4.1. The following records shall be maintained by the reporting entities each time they engage in ongoing monitoring (which may or may not include full re-verification):

4.4.1.1. what aspects of the issue have been considered;
4.4.1.2. action taken (if any);
4.4.1.3. the reasons for that decision; and
4.4.1.4. who undertook the monitoring and the date on which it was undertaken.

4.4.2. FASU may request the above information from the reporting entities as a part of their supervision and enforcement powers.

5. On-going ECDD

5.1. Ongoing ECDD is automatically required whenever ECDD is applied. This is, for instance, in the case of:

5.1.1. high-risk customers
5.1.2. PEPs
5.1.3. correspondent banking

For more detailed information and guidance on ECDD, 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).**

Whatever controls you have in place to monitor other business relationships, they shall be intensified in order to apply ongoing enhanced monitoring. This may include:

a) requiring a greater level of information and explanation from the customer when activity diverts from that addressed in their client risk assessment;

b) greater frequency of checks on transactions, particularly source of funds; or

c) undertaking more frequent due diligence checks on your client.

5.2. You should ensure that funds involved in the transaction come from an expected source and are for an amount commensurate with the client's known wealth and with what is expected to be deposited in relation to the matters on which you act for them.

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