2025

Financial Analysis and Supervision Unit

Guidance for Reporting Entities to Raise Awareness on Suspicious Matters Reporting under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 8 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	03.08.25	Draft	FASU
2	06.08.25	Draft	Asian Development Bank Consultant
3	21.08.25	Draft	FASU
4	30.08.25	Draft	Asian Development Bank Consultant
5	26.09.25	Final	FASU

Table of Contents

Table of Acronyms

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
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 (or client)** means a person 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 customer.

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;
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] "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.

1.5. **Designated Non-Financial Businesses and 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 customer, 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. **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.

1.8. **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. **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.

1.13. **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.

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

1.15. **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. The Guidance aims to enhance reporting entities' understanding and practice of identifying suspicious matters and filing a suspicious matter report to FASU.

2.4. 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)*.

2.5. 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.

2.6. 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.

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

2.8. 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

3.1. The international recommendations and the AML/CTF laws of PNG outline ways that are proven to help deter and detect instances of ML and TF. These all form the basis of your obligations and the requirements which must be followed and implemented by a reporting entity.

> *i* *The Act sets out specific obligations on financial institutions which also apply to DNFBPs under Part II, except for Subdivisions 3 and 4.*
>
> *Part II Division 3, Subdivision 1. – Reporting obligations and offences (Sections 39 – 46)*
>
> *Section 41specifically provides for suspicious matter reporting obligations*

3.2. Section 41 of the Act requires reporting of 'information' known to a reporting entity based on a reasonable suspicion that the information is relevant for the purposes set out in Section 41(1)(a)-(c). Such 'information' includes attempted transactions. To comply with Section 41 of the Act, financial institutions must report attempted transactions in all circumstances, regardless of the amount of the (attempted) transaction.

3.3. Reporting entities must also report an offence under Section 15 or Section 16 of the *United Nations Financial Sanctions Act 2015* or any other indictable offence - while not giving rise to a transaction of any sort.

3.4. Failure to report a suspicion of money laundering or terrorist financing is a criminal offense.

4. Identifying and Reporting Suspicious Matters

4.1. What is a suspicious matter?

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

4.2. What is suspicious activity?

4.2.1. 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.

4.2.2. 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.

4.3. What is suspicious transaction?

4.3.1. 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).

4.4. Unusual vs. Suspicious

4.4.1. 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.

4.4.2. 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.

4.4.3. 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.

4.4.4. 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.

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

4.5. Reporting suspicious matters

4.5.1. 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.

4.5.2. 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.

4.5.3. 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.

4.5.4. 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.

4.5.5. 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[4]. If you are in any doubt, you should file a report with your reporting entity's compliance officer.

4.5.6. 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.

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

4.6.1. 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

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

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.

4.6.2. 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.

4.6.3. 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.

4.6.4. 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.

4.7. When must I submit a SMR?

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

4.7.2. 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.

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

4.8.1. 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 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.

[5] "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.

4.9. What information should be submitted when I make a SMR?

4.9.1. 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.

4.9.2. Please refer to **Appendix E** of FASU's *Guidance for Designated Non-Financial Businesses and 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.

4.10. Keeping a register of SMRs

4.10.1. 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.

4.10.2. 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.

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

- 4.10.3.1. Details of the internal SMRs made to your compliance officer;
- 4.10.3.2. Details of the external SMRs made to FASU;
- 4.10.3.3. 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;
- 4.10.3.4. Date of FASU's acknowledgement/confirmation letter;
- 4.10.3.5. FASU reference number.

4.10.4. 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.

4.10.5. 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.

4.11. What is tipping off?

4.11.1. 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.

4.11.2. 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.

4.11.3. 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.

4.12. Is threshold transaction reporting different from SMRs?

4.12.1. 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:

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

a) Domestic TTR[6]

b) International TTR[7] known as an International Electronic Funds Transfer Report (IEFTR)

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

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

4.12.2. 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 **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).**

4.12.3. 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 and Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No.2 of 2019)* for a copy

[6] Section 39 (1) of the Act
[7] Section 39 (2) of the Act

of the TTR, IEFTR and ADPER or download TTR form, IEFTR form and ADPER form from the website of the Bank of PNG.

5. Tips for Writing a Strong SMR

5.1. What suspicious matter information should I as a compliance officer put down?

5.1.1. As a compliance officer, you must provide background information on the customer by introducing the customer:

- Basic information detailing who the customer is;
- When the relationship with the customer was established;
- Information on the business profile; and
- Explanation of what typical business activity looks like.

5.1.2. As a compliance officer you must also provide information on the suspicious matter:

- The dates of the suspicious activity;
- The amount of money sent in each transaction;
- The mechanisms used for transfers;
- The information on the counterparty(ies) involved in the transactions; and
- The geographic locations involved.

5.2. What type of questions can I use to support my SMR narrative writing?

Use the following questions to support your SMR narrative writing:

5.2.1. Who?

- Did I include information on who is conducting the activity?
- Did I have identifying information on the customer's account and business details?

5.2.2. What?

- Did I include information on what types of methods or operations were used?

5.2.3. Where?

- Did I include information on where the activity (what jurisdictions), including the activities by counterparts?

5.2.4. When?

- Did I include information on when the activity took place? Does this include details on frequency and regularity of these activities?

5.2.5. Why?

- Did I include information on why these activities are unusual?
- Did I include information on why the filing institution thinks this is suspicious?

5.2.6. How?

- Did I include information on what tactics or financial instruments were used to facilitate the activity?
- Did I include information on how the activity occur?

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