2025

Financial Analysis and Supervision Unit

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)

Issued by the Financial Analysis and Supervision Unit 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

Act	Anti-Money Laundering and Counter 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
FI	Financial Institution
KYC	Know Your Customer (or Client)
ML	Money Laundering
PNG	Papua New Guinea
RBA	Risk-based Approach
SMR	Suspicious Matter Report
TF/FT	Terrorist Financing/Financing of Terrorism

1. Key Concepts and Terms

> ! **A number of terms used in this Guidance are defined in Section 5 of the *Anti-Money Laundering and Combating Terrorist Financing Act 2015*. 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 below.**

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. **Criminal conduct** is a conduct which constitutes an offence in Papua New Guinea (PNG) for which the maximum penalty is death or a term of imprisonment for at least six months; or would constitute an offence in PNG if it occurred in PNG and for which the maximum penalty under the law of PNG is death or a term of imprisonment for at least six months.

1.4. **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] "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.

1.5. **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.

1.6. **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.

1.7. **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:

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

1.7.2. monitor and enforce compliance with the Act; and

1.7.3. 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.

1.8. **Financial Institutions (FIs),** as defined in Section 5 of the 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.

1.9. **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. **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.

1.11. **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.

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

1.13. **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.

1.14. **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.

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

1.16. **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 the reporting entities to accurately, consistently and effectively conduct Enhanced Customer Due Diligence (ECDD) in compliance with Sections 27 and 28 of the Act.

2.4. Section 26 of the Act places requirements on reporting entities to undertake certain actions in relation to customers where they 'take the view' that the customer is:

2.4.1. a resident in a high-risk country or jurisdiction; or

2.4.2. involved in a high-risk business activity; or

2.4.3. a politically exposed person (PEP); or

2.4.4. presents a situation where the money laundering or terrorist financing is high; or

2.4.5. not physically present for the purposes of identification.

2.5. For such customers, Sections 27 and 28 of the Act requires reporting entities to obtain information relating to the source of the assets or the wealth of the customer, and to take reasonable steps to verify that information.

2.6. This Guidance is meant to provide practical assistance, clear direction, and a basis to make reporting entities to effectively comply with their anti-money laundering and counter terrorist financing (AML/CTF) obligations by navigating through various concepts and process that have not been elaborated in the legislation. These include, for instance, the identification of a "high-risk country" or a "high-risk business activity" or a "high-risk customer" or to identify a situation that presents a situation where money laundering or terrorist financing is high. The guidance also provides details on, for instance, the information that should be collected in relation to the source of assets and source of wealth or what might be considered to be 'reasonable steps' in verifying that information.

2.7. This Guidance expands the sections relating to ECDD in the 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); and

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).

2.8. It provides more clarification on the processes behind ECDD and Targeted Financial Sanctions (TFS) for terrorist financing (TF) to assist reporting entities to comply with the various requirements of the Act, *Criminal Code (Money Laundering and Terrorist Financing)(Amendment) Act* 2015 and the *United Nations Financial Sanctions Act* 2015.

2.9. 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.

2.10. Reporting entities should develop their own AML/CTF internal policies, procedures and controls tailored to their business 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 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. As noted above, PNG has in place a legislative framework to fight ML and TF that has incorporated and adopted international standards and recommendations to apply ECDD measures in certain circumstances.

> *i* *The Act sets the requirements to establish a risk-based AML/CTF Program under Section 7 and circumstances where Enhanced Due Diligence applies under Section 26.*

3.2. A number of sections of the Act relate to the effective conduct of ECCD. These are:

a). Risk assessments (Section 6);
b). AML/CTF programs (Section 7);
c). Ongoing due diligence (Section 17);
d). Enhanced Customer Due Diligence (Sections 26-29); and
e). Rejection or termination of business (Section 19).

3.3. The requirements of the sections listed above cascade in a way that ensures reporting entities to consistently, reliably and accurately apply and document actions taken when the ML/TF risk is high. ECDD involves conducting extra checks on a customer identification, collecting additional information and doing further verification. Customers must be monitored and the appropriate measures applied may change over time and as the ML/TF risk profile of a customer changes. When ECDD is applied, it also allows you to decide whether a Suspicious Matter Report (SMR) is required.

3.4. The means by which the Act assists reporting entities to achieve these objectives is by providing a legal requirement to identify and reject transactions, and terminate business relationships, where information relating to a legitimate source of wealth and assets cannot be obtained or verified.

3.5. None of the processes articulated in the Act are intended to support defensive reporting[5], or the continuation of business relationships in circumstances where illicit sources of customer or client wealth or assets are identified.

[5] 'Defensive reporting' is the reporting of all of the transactions of a customer where an illicit source of wealth is identified and the reporting entity continues the business relationship in violation of the Act and the Criminal Code, or, reporting of matters where no reasonable suspicion exists and reports are submitted in order to either, bolster statistics or, avoid the process of obtaining and verifying information relating to a legitimate source of wealth or assets.

4. When must a reporting entity "take the view"?

4.1. What is the criterion to 'take the view'?

4.1.1. Section 26 of the Act requires reporting entities to conduct ECDD in circumstances where the entity "takes the view" that certain criteria exist.

4.1.2. Certain objective criteria exist that *require* an entity covered under the Act to take such a view in order to comply with the requirement to maintain an effective AML/CTF program. They are:

a). where the customer satisfies the definition of a 'politically exposed person' (PEP) as articulated in Section 5 of the Act
b). where the customer is not physically present.

4.1.3. Other, less objective criteria exist for other categories of customers. These are:

a). where the customer is a resident in a high-risk country or jurisdiction;
b). where the customer is involved in a high-risk business activity;
c). where the customer is high-risk;
d). where the risk of money laundering or terrorist financing is high.

4.1.4. These four criteria mentioned under 4.1.3 above require reporting entities to determine when a:

a). country is 'high-risk';
b). a business activity is 'high-risk';
c). when a customer is 'high-risk'; and
d). when the risk of money laundering or terrorist financing is 'high'.

4.2. Can a reporting entity avoid ECDD obligations by not 'taking the view'?

4.2.1. The wording of the Act appears to provide considerable leeway to reporting entities in conducting ECDD by not 'taking the view' that a customer fits the subjective criteria articulated in Section 26(1).

4.2.2. This is, however, mitigated by the requirement under Section 7 of the Act which requires the reporting entities to have "*effective procedures, policies and controls for determining when enhanced customer due diligence must be conducted under Section 26*"

4.2.3. A failure to 'take the view' that a customer is 'high-risk' in circumstances where that customer has, for example, been charged with a financially motivated offence, may avoid a contravention of Sections 27 and 28 but may place the reporting entity at risk of prosecution for a contravention of Section 7. The penalties under each of these sections are the same.

5. What does 'high-risk' mean?

5.1. What does 'high-risk' means under the Act?

5.1.1. The Act does not define the term 'high-risk' and the term has multiple meanings depending upon the context in which it is used.

5.1.2. For the purposes of this Guidance, **"high-risk", as it pertains to customers**, means:

> *"an elevated probability that the customer will engage in significant financially motivated criminal conduct."*

5.1.3. '**High-risk' as it pertains to countries and regions** mean:

> *"a country that has laws that allow the registration and supply of legal structures that can, and have been, used to hold assets and operate bank accounts anonymously".*
>
> *"countries and regions may be considered high-risk if they are one or more of the following:*
> - *deemed a high-risk or non-cooperative jurisdiction by the Financial Action Task Force (FATF);*
> - *prescribed foreign countries;*
> - *subject to sanctions;*
> - *known tax havens; and*
> - *known to provide support to terrorist organizations."*

5.1.4. **'High-risk' as it pertains to business activities** means:

> *"business activity that has been identified as being a source of significant criminal property or a conduit for, or facilitator of, criminal conduct".*

5.2. Identifying High-Risk Countries/Jurisdictions

5.2.1. Reporting entities should refer to the following sources for determining when a country or a jurisdiction is high-risk.

- FASU's risk assessment on high-risk jurisdictions;
- FASU's guidance on high-risk jurisdictions;
- Tax Justice Network's Financial Secrecy Index;
- Open-source research on tax and money-laundering havens; and
- FATF's list of high-risk jurisdictions subject to a call for action and jurisdictions under increased monitoring[6].

5.2.2. FASU's *Risk assessment on High-Risk Jurisdictions* identified that, in PNG's context, 'high-risk countries' are those that offer products and services that allow bank accounts, companies and assets to be held and used anonymously.

5.2.3. Reporting entities must include the jurisdictions that FATF has identified as having deficiencies in their AML/CFT system as "high-risk".

[6] FATF High-Risk and Other Monitored Jurisdiction: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html

5.2.4. As part of their AML/CTF program, reporting entities should maintain a list of high-risk jurisdictions and use that list in their transaction monitoring, on-boarding, and ECDD processes.

5.2.5. For more detailed information and guidance on High-Risk Countries or 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).**

5.3. Identifying High-Risk Business Activities

5.3.1. Reporting entities must be capable of identifying customers involved in high-risk business activities.

5.3.2. In determining high-risk business activities, there are a number of sources that the reporting entities should refer to, which includes:

a). The Papua New Guinea National Risk Assessment on Money Laundering and Terrorist Financing 2017 (NRA)[7];

b). Thematic or sectoral risk assessments (published from time to time by FASU or other FIUs in the region);

c). Commissions of Inquiry;

d). Parliamentary Public Accounts;

e). Open-source reports and media.

5.3.3. The 2017 NRA of PNG has identified the following business activities as 'high-risk'.

a). Public service (employees and departments)
b). Domestic commercial banking
c). Company and trust formation agents
d). Real estate agents
e). Lawyers and law firms
f). Accountants and accounting firms
g). Motor vehicle dealers
h). Forestry – (employees, companies, office-holders and public servants)
i). Large-scale commercial fishing

5.3.4. The business activities listed under 5.3.3. above should be considered, in the current context, to be high-risk business activities for the purpose of *Section 26(1)(b)* of the Act.

5.3.5. Reporting entities should also use their own risk assessment process to determine if there are additional business activities that present an elevated risk.

5.4. It should be noted here that high-risk business activities are not limited to private enterprise. Customers who are public servants or employed by State-Owned Enterprises (SOE) in PNG may be considered to be involved in a 'high-risk business activity', particularly if they have access to funds or assets which have the potential to be misappropriated.

[7] https://www.bankpng.gov.pg/sites/default/files/2024-09/Money-Laundering-and-Financing-of-Terrorism-National-Risk-Assessment-4.pdf

5.4.1. Reporting entities should maintain a list of high-risk business activities and use that list in their risk assessments; on-boarding and ECDD processes.

5.4.2. Registered should ensure that the reason/source of information used to classify a particular business activity as 'high-risk' is included in the list.

5.4.3. Reporting entities must periodically review the list to ensure that it is reasonably up-to-date.

5.5. Identifying Politically Exposed Persons (PEPs)

5.5.1. A **PEP** means a person who is or has been entrusted with prominent public functions in PNG or a foreign country, as well as family members and close associates of that person.

5.5.2. Types of **prominent public functions**[8] for both domestic, foreign, and international organisation PEPs include the following:

- a head of state or head of a government;
- a senior politician;
- a senior government official;
- a senior judicial or senior military official;
- a senior executive of a state-owned company;
- a senior political party official;
- any person who is or has been a senior executive of a State-owned company in PNG or a foreign country; and
- a person who has been entrusted with a prominent function by an international organisation, including directors, deputy directors and members of the board or equivalent positions; and

5.5.3. Given that the main sources of criminal property in PNG are from domestic corruption, domestic PEPs pose a significantly high risk in PNG.[9]

5.5.4. An audit of proprietary PEP databases indicates that PNG PEPs are not accurately represented or recorded within such databases. In addition to not containing the correct names and dates of birth for PNG PEPs, commercial databases typically do not include the entities that are owned and controlled by PNG PEPs and do not include the names of family members and close associates.

5.5.5. As a result, reporting entities cannot rely on proprietary databases for their identification of domestic PEPs.

5.5.6. Reporting entities should maintain their own PEPs list, which may be combined with their high-risk customer list.

5.5.7. The source of information for those lists, especially for domestic PEPs, should be

a). The PNG electoral roll;

b). The Electoral Commission;

[8] Definition of Public Office Holders in PNG. Section 221 of the PNG Constitution defines a constitutional office holder to mean *"a Judge, the Public Prosecutor or Public Solicitor, the Chief Magistrate, a member of the Ombudsman Commission, a member of the Electoral Commission, the Clerk of Parliament; a member of the Public Services Commissioner; the Auditor General or the holder of any other office declared by an Organic Law or an Act of Parliament to be a constitutional office."*

[9] NRA of PNG 2017.

c). Government compendiums;

d). Investment and Promotion Authority (IPA) database; and

e). other reliable open-source information.

5.5.8. The information held by the reporting entity – such as account opening information – should also be used to identify PEPs.

5.5.9. PEPs list must contain the following information about each PEP:

a). Full name;
b). Date of birth;
c). Address;
d). Unique Digital Number, if available;
e). Names, dates of birth and addresses of family members (spouse, siblings, children);
f). Name, entity number (where relevant) and addresses of companies and other legal entities where a PEP, family member or close associates of the PEP.
g). The reason why the person, their family, close associates and companies are recorded on PEPs list and the link to the PEP.

5.5.10. The PEPs list shall form part of a reporting entity's AML/CTF Program and be used in transaction monitoring as well as on-boarding and ECDD.

5.5.11. For more detailed information AML/CFT obligations of reporting entities on relating to PEPs, refer to FASU's **Guidance for Reporting Entities on their Obligations under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 for "Conducting Enhanced Customer Due Diligence Measures on Politically Exposed Persons" (No.2 of 2025).**

5.6. Identifying high-risk customers

5.6.1. High-risk customers are those who are likely to be involved in money laundering, fraud, tax evasion, bribery and corruption, terrorist financing or other criminal conduct. High-risk customers are also those that engage with or are from high-risk jurisdictions.

5.6.2. Conducting an internal risk assessment will assist reporting entities in identifying high-risk customers.

5.6.3. Significant financially motivated criminal conduct is criminal conduct of a type that generates significant volumes of criminal property. In the current PNG context significant financially-motivated criminal conduct would be any criminal conduct that generates in excess of funds determined by the risk assessment in any given year.

5.6.4. Therefore, high-risk customers are those that present an elevated probability of engaging in criminal conduct that generates, or facilitates the generation of money or other assets worth more than the amount determined in the risk assessment, or is involved in the financing of terrorism in any 12-month period.

5.6.5. Reporting entities are required to maintain a list of high-risk customers.

5.6.6. The list must contain the following information on each high-risk customer:

a). Full name;

b). Date of birth;

c). Address(es);

d). Unique Digitial ID number, if available;

e). Name, entity number (where relevant) and address (es) of companies and other legal entities where the high-risk customer or close associate is a director or shareholder; and

f). The high-risk country; high-risk business activities, conviction, allegations or other reason for the customer's inclusion on the list.

5.7. When might the probability of criminal conduct be elevated?

5.7.1. Determining when a customer is more likely to engage in criminal conduct is a subjective process. No person's actions can be precisely predicted, however, in order to provide a reasonable level of certainty for reporting entities in their application of the Act a delineation must be made.

5.7.2. Based on the concept that past behaviour is generally considered to be a reliable indicator of future behaviour, a person who has engaged in criminal conduct in the past presents a greater level of risk than those customers who have not.

5.7.3. For the purposes of this guideline, the probability of criminal conduct may be elevated if, in the previous five years:

i) The customer has been charged with, or convicted of, criminal conduct[10] related to a significant financially motivated crime;
ii) The customer is the subject of allegations of corruption or other financially motivated crime published in domestic or international media;
iii) The customer is the subject of a Suspicious Matter Report submitted to FASU;

5.8. Identifying when the risk of money laundering or terrorist financing is 'high'

5.8.1. The risk of ML/TF may be assessed as high if one or more of the risk factors listed above, or in Section 26 of the Act, exist. That is;

- The customer is high-risk
- The customer is engaged in a high-risk business activity
- The customer is resident in a high-risk country (or jurisdiction)
- The customer is a PEP
- The customer is not physically present

5.8.2. These risks are compounded where the categories listed above intersect. That is, if a customer is high-risk and a PEP and is also engaged in a high-risk business activity, the risks increase with each additional criterion.

5.8.3. In addition, the following circumstances may mean that the risk of ML/TF is high:

- The customer refuses to provide information or explanations for the source or application of funds;

[10] "Criminal conduct" is defined in the Criminal Code S508A as conduct that constitutes an offence in Papua New Guinea for which the term of imprisonment is least six months or conduct offshore that would attract an equivalent penalty had it been committed in Papua New Guinea.

- The customer receives large amounts from a government department or State-owned enterprise – particularly if those amounts are in round-numbers and are received repeatedly;
- The customer receives large amounts of money from an entity that is engaged in a high-risk business activity;
- The customer sends or receives large amounts of money from a high-risk jurisdiction;
- The customer sends funds to or receive funds from a jurisdiction at high risk for terrorism financing
- The customer uses a debit or credit card issued in a high-risk jurisdiction, to move large amounts of money;
- The customer makes repeated payments to a member of the Royal Papua New Guinea Constabulary, a member of the judiciary, a member of parliament, or any other public servant;
- The customer uses high amounts of cash; and
- The customer uses complex or opaque business ownership structures.

! **Failure by reporting entities to comply with ECDD obligations set out in the Act, any offence and penalty provision applicable for financial institutions and also applicable to a DNFBP can result in penalties and sanctions.**

6. Legitimate Source of Funds and Source of Assets or Wealth

i The *Criminal Code (Money Laundering and Terrorist Financing)(Amendment) Act* 2015 applies to all people and corporate bodies in PNG.

Section 508B of the *Criminal Code (Money Laundering and Terrorist Financing)(Amendment) Act* 2015 states that:

> *"a person who deals with property that is criminal property and who knows or reasonably ought to know that the property is criminal property is guilty of an offence*".

The *Criminal Code (Money Laundering and Terrorist Financing)(Amendment) Act* 2015 defines 'dealing with property' as doing one or more of the following things with criminal property:

- *acquiring;*
- *receiving;*
- *possessing;*
- *using;*
- *concealing;*
- *disguising;*
- *converting;*
- *transferring, or moving into or out of PNG; and*
- *consenting to, or enabling such actions.*

In the Criminal Code's definition of money laundering, the terms "concealing or disguising" refer to concealing or disguising the:

> *"nature, source, location, disposition, movement or ownership or any rights with respect to criminal property".*

Furthermore, Section 508C states that:

> *"A person who deals with property in circumstances where it is reasonable to suspect that the property is criminal property is guilty of an offence*".

That offence is 'dealing with property reasonably suspected to be criminal property'.

6.1. In order to comply with Sections 27 and 28 of the Act, reporting entities must not just obtain and verify information on any source of assets or wealth of a customer, but reporting entities must obtain and verify information relating to a legitimate source of assets or wealth of the customer.

6.2. Failure to verify the legitimate source of assets or wealth of a customer not only constitutes a breach of obligations under the Act, but it also exposes reporting entities, their staff and officers to potential prosecution under *the Criminal Code (Money Laundering and Terrorist Financing)(Amendment) Act 2015*. This includes offences related to dealing with criminal property, which carry penalties ranging from 3 to 25 years' imprisonment and fines between K100,000 to K1,000,000.

7. Source of Funds and Source of Assets or Wealth Related to the Entity Interaction with the Customer

i

Sections 27 and 28 of the Act use the terminology "*source of the assets or the wealth of the customer*" with respect to the conduct of ECDD.

Section 17 (2) (b) however refers to the ***source of funds***, as follows:
"When conducting ongoing due diligence, a financial institution must, at a minimum, do the following:
…
ensure that transactions carried out on behalf of its customers 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****."*

7.1. What is the difference between assets, funds and wealth of a customer?

7.1.1. The term 'assets" is defined under Section 5 of the Act, whereas the terms "funds" and "wealth" are not explicitly defined. However, the definition of "assets" under the Act is broad and encompasses funds, property and financial resources of any kind.

i

Section 5 of the Act provides that:

"assets" means funds, property and financial resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in such assets, including but not limited to currency, bank credits, deposits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, and any interest, dividends, income or value accruing from, generated by or derived from such assets;

7.1.2. The Act provides no further explanation with respect the "source of funds" or whether that is intended to be interpreted differently from the assets or wealth of the customer.

7.1.3. For the purposes of this guidance, the term "assets" (as defined in the Act) is considered synonymous of "wealth", which is a broader term than "funds". All deposits or "funds" into a customer's account form part of the total assets or wealth of a customer.

7.1.4. Consequently, source of funds and source of wealth do not mean the same thing, although there can be significant overlap between the two and they do not exist in isolation to each other. The 2013 FATF Guidance on PEPs has explained these terms, as detailed in of this Guidance below.

Source of Funds and Source of Wealth

Source of Funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between the PEP and the financial institution or DNFBP (e.g., the amounts being invested, deposited, or wired as part of the business relationship).

Source of Wealth refers to the origin of the PEP's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the PEP acquired such wealth.

Source: The FATF Guidance on PEPs, 2013[11]

7.1.5. To effectively comply with Sections 27 and 28 of the Act, reporting entities shall obtain, and take reasonable steps to verify, information relating to both the source of funds and source of wealth as a part of ECDD measures.

7.2. Establishing Source of Funds

7.2.1. To establish the source of funds, reporting entities should not simply try to answer *where did the funds for the transaction come from* but also *how and from where did the customer get the funds for this transaction or business relationship?* For instance, it is not enough to know that the funds came from a bank account.

7.2.2. The source of funds pertains directly to the funds that are being used to fund the specific transaction in hand i.e., the origin of the funds used for the transaction(s) or activities that occur within the customer's business relationship with the reporting entity. Checking this means ascertaining where those funds came from, how they were accumulated by the customer and ensuring that they are not the proceeds of crime by applying a RBA.

7.2.3. The types of data and documents that reporting entities may use for verification of source of funds will vary depending on the circumstances and the information that the customer provides to the reporting entity.

7.2.4. As stated above, the verification of the source of funds should go beyond simply identifying the financial institution from which the funds were transferred, except in cases where the institution is directly financing the transaction, such as through a mortgage. It should also extend beyond merely confirming that the customer's name matches the name on the account. In addition to recording details such as the transaction amount, currency, and remitting account information (including the bank name, account number, sort code, and account holder's name), the reporting entity should obtain substantive information to establish the origin and purpose of the funds, such as whether they were acquired through salary, a gift, or other means.

7.2.5. Documents that may assist in verifying the source of funds include bank statements, a copy of will(s), full payslips, audited financial records showing disbursed funds, sales or purchase agreements, transaction receipts, and similar evidence. Identifying income derived from share capital, business activities, inheritance, or gifts can also support this verification process.

[11] The 2013 FATF Guidance on PEPs, p. 20.

7.2.6. If a customer states that funds for a transaction were received from a third party, the reporting entity should also document details of that original transaction. Verification may involve requesting bank statements and other relevant supporting documents related to the transfer.

7.2.7. Determining the source of funds can sometimes be challenging without a broader understanding of the individual's source of wealth, particularly when funds from different sources have been combined in an account. In such cases, the reporting entity may need to assess the individual's overall wealth origin to gain clarity on the source of funds. However, the extent to which the reporting entity relies on this information should be guided by a risk-based approach.

7.3. Establishing Source of Wealth

7.3.1. You should seek to answer the question: "*why and how does the individual have the amount of overall assets they do – and how did they accumulate/generate these?*"

7.3.2. Source of wealth is a holistic appraisal as to where an individual or an entity has derived their overall wealth (i.e., the origin of their entire body of assets), rather than any specific portion of it. It describes the economic, business and/or commercial activities that generated, or significantly contributed to, the customer's overall net worth/entire body of wealth. This should recognize that the composition of wealth generating activities may change over time, as new activities are identified, and additional wealth is accumulated.

7.3.3. As part of your ECDD process, a reporting entity should verify the customer's source of wealth using evidence provided by the customer and/or independent sources. This verification should continue until the entity has a clear understanding of the origin of the customer's overall wealth and is reasonably assured of its legitimacy. The reporting entity should document its rationale and findings in a formal record/file note.

7.3.4. When verifying the source of wealth, the reporting entity should consider whether the explanation provided aligns with the customer's profile – does it logically follow that the customer has accumulated wealth in the manner they have described?

7.3.5. The source of wealth refers to the origin of a customer's entire body of wealth (i.e., total assets). This information will usually provide an understanding and insight into the overall volume of wealth the customer is expected to have, and how it was acquired.[12] However, this does not require a reporting entity to get an exhaustive account of all assets, but rather a reasoned assessment that demonstrates the legitimacy of the wealth and ensures the transaction is consistent with the customer's financial profile.

7.3.6. In complex cases, tracing the original source of wealth—especially if it was accumulated over a long period—can be challenging. In such instances, reasonable efforts should be made to gather relevant information from the customer, while also considering other risk factors such as geographic or jurisdictional risks, negative media coverage, PEP status, and the nature of the transaction (particularly if it could obscure asset ownership or transfer).

[12] Ibid.

7.3.7. Although a reporting entity may not have direct access to all assets held by a customer, general information can often be obtained from commercial databases or publicly available sources.

7.3.8. Where a customer's source of wealth is not immediately evident, the first step should involve direct inquiries with the customer, followed by independent verification and cross-referencing of information from multiple sources. This helps to develop a comprehensive understanding of the customer's financial background and circumstances.

7.3.9. All actions taken, documents reviewed, and decisions made—including the rationale behind them—must be clearly recorded, as they may be subject to review by FASU or other relevant bodies. If the source of wealth cannot be satisfactorily established, the reporting entity should consider terminating the business relationship with a PEP and assessing whether SMR should be filed to the FASU.

7.3.10. For more detailed guidance verifying on Source of Wealth and Source of Funds, please refer to the Wolfsberg Group Guidance on this topic.[13]

7.4. Information relating to an external source

7.4.1. Reporting entities when obtaining and verifying information relating to a legitimate source, may also need to identify a source that is outside of the customer's direct control.

7.4.2. *For example*, where a high-risk customer makes deposits into their personal bank account from another account that they own or control (for example a business account), the process of obtaining and verifying information must extend to the source of the funds that entered the account customer's business account. For transactions that may be moved through multiple accounts that are under the control of the customer, the process must be continued through the chain of transactions to the point where the funds first came under the control of the customer.

7.5. What types of information relates to a legitimate source of wealth or assets?

7.5.1. The following information relates to a legitimate source of wealth:

a). Bank statements
b). Payslips
c). Tax returns
d). A Will (or a certified copy)
e). Court order (e.g. divorce settlement)
f). A trust deed (or a certified copy)
g). Audited financial accounts showing funds disbursed to the customer
h). Contracts (e.g. sale/purchase agreements)
i). Loan documents
j). Asset declarations
k). Royalties
l). Business registration documents

[13] Wolfsberg Group (2020) *Frequently Asked Questions (FAQs) – Source of Wealth and Source of Funds* (August 2020): Available at:https://db.wolfsberg-group.org/assets/a27f9bf6-b4a8-41d2-a390-6f1aaf797241/Wolfsberg%20SoW%20and%20SoF%20FAQs%20August%202020%20(FFP).pdf

m). Receipts of other transactions or similar documents
n). Share portfolio documents
o). Title deeds
p). Vehicle registration documents
q). Insurance policy documents
r). Mortgage
s). Invoices
t). Affidavits

7.6. Source of Information

7.6.1. The first source of information on source of funds and source of wealth or assets should be customer. The customer has access to the widest possible range of information, and they have the ability to grant permission for the reporting entity to contact third parties (such as financial institutions) to obtain and verify the information provided.

7.6.2. A refusal by the customer to provide information relating to a legitimate source of wealth or assets, or a refusal to grant permission to contact unrelated third parties to verify information, will place the reporting entity in a position of being unable to complete ECDD. The inability to complete ECDD triggers the requirement to terminate the business relationship pursuant to Section 19 of the Act. and assessing whether SMR should be filed to the FASU.

7.7. What are 'reasonable steps' to verify information?

7.7.1. A reporting entity must take 'reasonable steps' to verify the information relating to a legitimate source of funds and source of wealth/assets.

7.7.2. Since the term 'reasonable steps' has not been explained in the Act, this guidance elaborates on what might constitute 'reasonable steps' in the process of verifying information relating to a legitimate source of wealth and assets:

a). Examination and comparison of documents and information provided by the customer with other information obtained from unrelated third-parties to determine whether the information provided by the customer is logical, reasonable and consistent;
b). Examination of written responses from the customer and comparison of such information with other sources to ensure that it is consistent and logical;
c). Examination of information provided during conversations and interviews with, the customer and comparison of such information with other sources to ensure that it is consistent and logical;
d). Confirmation of the accuracy of information provided by the customer by reference to an arms-length, unrelated third-party over which the customer has no significant influence or control;
e). Extracting documents from government websites and comparing them with other documentation obtained or provided by the customer;
f). Calculations on such things as the balances of accounts; increases in value of properties; sales values; valuations of inventories; expenditure on projects to ensure that it is logical and consistent with other known information;
g). Examination of, and calculations on, information from documents such as invoices; receipts; delivery dockets; payment advice; contacts and projects to ensure they do not conflict with other information;

h). Examination of documents such as contracts; certificates of title; bank statements; timesheets, payslips; project documentation etc. to ensure they do not conflict with other information and provide a reasonable indication of a legitimate source of assets and wealth.

8. Targeted Financial Sanctions

Section 40 of the Act sets out the obligation to report on asset of a designated person or entity and makes reference to the *United Nations Financial Sanctions Act* 2015 (*UNFS Act*) The UNFS Act is applied in PNG, its citizens and bodies corporate incorporated under a law of PNG wherever located.

Key terms to understanding the reporting obligation in relation to the financing of terrorism.

Asset is defined in Section 5 of the *UNFS Act* and means funds, property and financial resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to currency, bank credits, deposits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit and any interest, dividends, income or value accruing from, generated by or derived from such asset.

i

Designated person or entity is defined in Section 5 of the *United Nations Financial Sanctions Act* 2015 and means a person or entity –

- designated by the Prime Minister or the court under the United Nations Financial Sanctions Act 2015 (UNFS Act); or
- designated by the United Nations Security Council or its Committees pursuant to Resolutions listed in Schedule 1 to the UNFS Act or prescribed by Regulations made under Subsection 29(2) of the UNFS Act.

The Designation Process is set out in Part II of the UNSF Act.

8.1. A reporting entity is required to report to FASU any assets of a designated person or entity which it holds, 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 *UNSF Act* 2015.

8.2. A reporting entity must fill out and submit an Asset of a Designated Person or Entity Report (ADPER) Form to FASU within the specified timeframe mentioned above. The form is attached as **Appendix E** in FASU's *Guidance for Financial Institutions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (No.1 of 2019).*[14]

!

Failure to comply with this reporting obligation is a crime punishable by up to 5 years imprisonment and fines of K500,000.00 for an individual and K1,000,000.00 for a body corporate.

[14] https://www.bankpng.gov.pg/sites/default/files/2024-09/1.-Guidance-for-Financial-Institutions-on-their-Obligations-under-the-Anti-Money-Laundering-and-Counter-Terrorist-Financing-Act-2015-No.-1-of-2019-2_0.pdf

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