2025

Financial Analysis and Supervision Unit

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)

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/CFT	Anti-Money Laundering/Counter Terrorist Financing
CDD	Customer (or Client) Due Diligence
DNFBPs	Designated Non-Financial Businesses or Professions
ECDD	Enhanced Customer Due Diligence
EU	European Union
FASU	Financial Analysis and Supervision Unit
FATF	Financial Action Task Force
FI	Financial Institution
IMF	International Monetary Fund
ML	Money Laundering
PNG	Papua New Guinea
RBA	Risk-based Approach
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. **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 (AML/CFT) Act 2015*, includes a

[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.

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.

1.5. **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 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.

1.7. **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. **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.

1.9. **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.

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

1.11. **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 strengthen reporting entities' understanding and practice of identifying and maintaining the list of high-risk jurisdictions.

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

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

2.6. Some of the 'marks' used in the Textbox 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 financial institutions, including on penalties for non-compliance with obligations under the Act.

3. Requirements under the Act

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

3.1. Under Section 26 of the Act, one of the circumstances where reporting entities are required to apply enhanced customer due diligence (ECDD) measures in relation to high-risk jurisdictions. This obligation is in addition to the requirement to apply ECDD when there is an assessed high risk of money laundering (ML) or terrorist financing (TF), including geographical risk based on credible sources.

3.2. In order to demonstrate compliance with Sections 7 and 26 of the Act, FASU requires reporting entities to do the following:

3.2.1. Maintain a register of high-risk jurisdictions;

3.2.2. Document whether or not the reporting entity has 'taken the view' that the jurisdictions listed on the 'High-Risk Jurisdictions Register' involve a high risk of ML or TF pursuant to Section 26(1)(e);

3.2.3. Conduct ECDD and enhanced ongoing monitoring on all business relationships, either new or existing, and transactions that involve high-risk jurisdictions either directly, or indirectly through legal persons or legal arrangements that are established or registered in them; and

3.2.4. Maintain records of ECDD decisions and processes conducted under point c). above.

3.3. Business relationships and transactions involve a high-risk jurisdiction if:

3.3.1. the funds were generated in, are received from or are destined for a high-risk jurisdiction;

3.3.2. the reporting entity is dealing with a natural person or legal person resident or established[4] in a high-risk jurisdiction; or

3.3.3. the reporting entity is dealing with a legal arrangement (e.g., express trust) established or governed by the law of a high-risk jurisdiction or is administered in a high-risk jurisdiction.

3.4. Reporting entities should be prepared for FASU to examine the register of high-risk jurisdictions, and the records of ECDD measures during onsite visits.

[4] In the case of a legal person, being established in a high-risk jurisdiction means being incorporated in or having its principal place of business in that jurisdiction, or in the case of financial institution, having its principal regulatory authority in that country.

4. High-Risk Jurisdictions

4.1. What is a 'high-risk jurisdiction'?

4.1.1. High-risk jurisdictions are those jurisdictions whose anti-money laundering and counter terrorist financing (AML/CTF) frameworks and systems have been found to have strategic deficiencies, thereby posing a **high risk** of ML and TF to the international financial system. They include tax-havens, secrecy-havens, and other jurisdictions identified as having weaknesses in their AML/CTF regimes.

4.2. How to identify a high-risk jurisdiction?

4.2.1. A high-risk jurisdiction may be identified by a number of features including:

a). Listing by FATF as high-risk i.e., a jurisdiction named on either of the following lists published by the FATF as they have effect from time to time – a) high-risk jurisdictions subject to a call for action; and b) jurisdictions under increased monitoring;[5]
b). Listing as a tax or secrecy haven by foreign governments; NGOs[6]; the World Bank[7], International Monetary Fund (IMF), the European Union (EU)[8] or the United Nations[9];
c). Listing as a country of concern with respect to money laundering or terrorist financing by foreign governments[10] and NGOs[11];
d). List as a country with the highest corruption in the Corruption Perceptions Index issued by Transparency International[12];
e). Repeated reports in the media of involvement in money laundering or terrorist financing[13]; and
f). Described as 'high-risk' in the Thematic Risk Assessment on Offshore Financial Centres released by FASU or another jurisdiction.

4.2.2. Reporting entities have to refer directly to the lists published by the FATF and other relevant institutions, such as the World Bank, IMF, EU and the United Nations. These lists are updated from time to time in a year. *For instance*, the lists published by the FATF are updated three times a year, on the final day of each FATF Plenary meeting, held every February, June and October.[14]

4.3. What are tax havens?

4.3.1. Although there is no universally agreed definition of what a tax haven is, a tax haven generally refers to a country or jurisdiction that seeks to attract foreign (or non-resident) companies and individuals by offering facilities that enable them to avoid paying taxes in countries where

[5] FATF High-Risk and Other Monitored Jurisdiction: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html
[6] Such as, the Tax Justice Network https://fsi.taxjustice.net/en/introduction/fsi-results;
[7] The Stolen Assets Recovery Initiative operates out of the World Bank https://star.worldbank.org/
[8] https://ec.europa.eu/taxation_customs/tax-common-eu-list_en
[9] Countries subject to Sanctions by the UN Security Council: https://main.un.org/securitycouncil/en/sanctions/information
[10] Such as the US Department of State Bureau of International Narcotics and Law Enforcement Affairs produces a report titled the 'International Narcotics Control Strategy Report in which it names major money laundering countries - https://2009-2017.state.gov/j/inl/rls/nrcrpt/2016/vol2/253367.htm
[11] Based Institute on Governance – Basel AML Index: https://baselgovernance.org/publications/basel-aml-index-2024
[12] Transparency International – Corruption Perception Index: https://www.transparency.org/en/cpi/2023
[13] Such as those publicised by the International Consortium of Investigative Journalists https://www.icij.org/
[14] The dates of these meetings are published several months in advance, in the events calendar on the FATF website: https://www.fatf-gafi.org/en/calendars/events.html

they operate and live, and to pay less tax than they should in those countries, and do not share any financial or banking information with foreign tax authorities, according to the Financial Secrecy Index issued by the Tax Justice Network.[15]

4.3.2. Tax havens may be identified by several unique features (the list below is not exhaustive):

a). They offer low tax, or zero tax regimes to foreigners that they typically do not offer to their own citizens;

b). They refuse to share taxation information with other jurisdictions without the client's consent;

c). They offer legal structures such as companies and trusts to foreigners that are not offered to their own citizens;

d). They do not require companies to actually operate in the jurisdiction; or

e). They may offer methods of holding assets anonymously.

4.4. What are secrecy havens?

4.4.1. Secrecy-havens refers to jurisdictions that provide facilities allowing people or entities to evade or circumvent the laws, rules and regulations of other jurisdictions. These jurisdictions rely heavily on secrecy and anonymity as a tool to conceal wealth and financial affairs – distinct from tax havens, which primarily enable people or entities to shifting of profits to low-or no-tax jurisdictions to reduce tax obligations.[16]

4.4.2. Secrecy-haven jurisdictions routinely 'ring-fence' their own economies from the facilities they offer, to protect themselves from the harm caused by the products and services that they offer.

4.4.3. Secrecy havens provide products and services to allow foreigners to hold and move assets anonymously, and/or avoid confiscation by law enforcement.

a). They offer methods of avoiding asset confiscation by refusing to recognise foreign court orders or by allowing assets to be moved in the event that a foreign jurisdiction attempts to confiscate them (sometimes called 'spendthrift clauses');

b). They offer legal structures, such as companies and trusts, that are owned, directed or controlled through nominees. The nominees are merely names registered in the official documentation to avoid the beneficial owner being identified. The nominee may, or may not, actually exist;

c). They enforce strict 'privacy laws' that include gaoling people for releasing banking or other financial information that might identify beneficial owners and their link to assets;

d). They offer anonymous transfer of assets through things like bearer shares; and

e). They offer anonymous banking through services such as debit cards issued in company names which have nominee shareholders and directors.

4.4.4. Secrecy havens may be identified by advertisements offering 'anonymity' or 'privacy' in banking or company ownership or control.

4.4.5. A jurisdiction may be a tax haven as well as a secrecy haven.

[15] Tax Justice Network – what is a tax haven?: https://taxjustice.net/faq/what-is-a-tax-haven/
[16] Tax Justice Network – what is a tax haven?: https://taxjustice.net/faq/what-is-a-tax-haven/

4.5. How to maintain a list of high-risk jurisdictions?

4.5.1. To ensure compliance with the risk-based approach (RBA) required by the Act, reporting entities should periodically conduct open-source searches to identify high-risk jurisdictions. There are a number of institutions/companies, as discussed above under **Section 4.2.1.**, that conduct such research and provide lists of high-risk jurisdictions, but reporting entities should supplement these with their own research.

4.5.2. Jurisdictions identified by FASU's thematic risk assessment as 'high-risk', as well as jurisdictions identified by the FATF in its two publications, as highlighted above under **Section 4.2.1.**, shall definitely be included in the reporting entities' list of high-risk jurisdictions.

4.5.3. It must be noted that the inclusion in, or removal from a list, is insufficient alone to provide assurance that a jurisdiction is, or is not, a high-risk jurisdiction. Reporting entities will need to look to the substance of the jurisdiction's behaviour to determine the risk that it presents to PNG and to the reporting entity.

4.5.4. Reporting entities may maintain an expanded list of high-risk jurisdictions (based on their own internal risk assessment) or subscribe to a commercially available database, but they must be in a position to provide a list of high-risk jurisdictions and prove that the list has been applied to business or profession's customers, when required by FASU.

4.5.5. Reporting entities that maintain a High-risk Jurisdiction list should ensure that the reason and/or source of information used for the inclusion on the list is recorded on the list.

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

Suggested List of Keywords for Open-Source Search of High-Risk Jurisdictions

Below is a list of suggested 'keywords' for open-source searches that may be of assistance in identifying and assessing high-risk jurisdictions. These terms are indicative only as at the time of issuing this policy. New ML/TF products and services are being developed constantly, and the search terms will need to be updated to stay current as ML and TF evolves.

e.g.

a) Tax-haven
b) Secrecy-haven
c) Anonymous banking
d) Anonymous bank account
e) Anonymous company formation
f) Anonymous company ownership
g) Nominee directors/shareholders
h) Offshore company formation
i) Numbered bank accounts
j) Tax-haven /secrecy-haven blacklist
k) Tax minimisation strategies
l) Circumvention of sanctions/anti-money laundering control

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