2025

Financial Analysis and Supervision Unit

Guidance for Reporting Entities to Raise Awareness on the Use of Digital Identity and Electronic Know-Your-Customer Requirements for Customer Due Diligence (No. 1 of 2025)

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

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

Document Version Control

Version	Date Issued	Document Status	Document Author
1	30.01.24	Draft	FASU Consultant
2	06.02.25	Draft	FASU
3	30.06.25	Draft	FASU
4	30.07.25	Draft	Asian Development Bank Consultant
5	06.08.25	Draft	FASU
6	30.08.25	Draft	Asian Development Bank Consultant
7	26.09.25	Final	FASU

Table of Contents

TABLE OF ACRONYMS 3
1. KEY CONCEPTS AND TERMS 4
2. NOTE TO READING THIS GUIDANCE 7
3. VERIFICATION OF IDENTITY 9
4. DIGITAL IDENTITY SYSTEMS FOR E-KYC 11
5. ONGOING REVIEW OF DIGITAL IDENTITY AND E-KYC SYSTEMS 12
REFERENCES AND CONTACTS 13

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
e-KYC	Electronic Know Your Customer (or Client)
ECDD	Enhanced Customer Due Diligence
FASU	Financial Analysis and Supervision Unit
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
KYC	Know Your Customer (or Client)
LEAs	Law Enforcement Authorities
ML	Money Laundering
PNG	Papua New Guinea
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. **Biometrics** here refers to 'biophysical biometrics' i.e., using the measurement of physiological characteristics including attributes such as fingerprints, iris patterns, voiceprints, or facial recognition – all of which are static – to identify a person.

1.3. **Business relationship** means an on-going business, professional or commercial relationship between a financial institution (FI) or Designated Non-Financial Business or Profession (DNFBP) and a customer.

1.4. **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.

1.5. **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;

[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.

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. **Digital identity system** refers to the use of technology to capture, validate and store data on a person's identity. A person's identity information stored on a digital identity system is referred to as 'digital identity'. A digital identity system can also be used to authenticate someone who claims a 'digital identity'.

1.7. **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.

1.8. "**electronic Know Your Customer" (e-KYC)** means establishing business relationships and conducting CDD by way of electronic means, including online and mobile channels. e-KYC, uses secure digital verification processes, like biometrics, to verify customer identity and ensure compliance with laws and regulations.

1.9. **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:

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

1.9.2. monitor and enforce compliance with the Act; and

1.9.3. 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.

1.10. **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.

1.11. **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.

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

1.15. **Terrorist Financing (TF)** is providing or collecting funds or assets 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 use digital identity and electronic Know-Your-Customer (e-KYC) systems to identify and verify customers or clients for the purpose of customer due diligence (CDD).

2.4. To effectively apply the customer identification and verification measures, a reporting entity must exercise discretion, based on its own risk assessments, to determine the level of customer due diligence measures, whether simplified, standard, or enhanced.

2.5. This Guidance is meant to provide industry guidance, practical assistance and a basis to better make reporting entities able to comply with their anti-money laundering and counter terrorist financing (AML/CTF) obligations by applying e-KYC measures.

2.6. The criteria in this Guidance should however be considered the minimum standard to comply with the Act.

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

2.7.1. *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);

2.7.2. *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

2.7.3. *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)*.

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

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

2.10. 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. Verification of Identity

i *The Act sets out the due diligence obligations in Part II, Division 2 (Sections 15 to 38). Specifically:*

Subdivision 1 – General due diligence requirements (Sections 15 to 19)

Section 16. Basis for verifying identity.

A financial institution must only use reliable and independent source documents, data or information to verify the identity of –

a) a person or unincorporated entity referred to in Section 20(1) in accordance with the requirements of Subdivision 2 of this Division; and

b) a sender or receiver of an electronic funds transfer in accordance with the requirements of Subdivision 3 of this Division; and

c) a respondent financial institution in accordance with the requirements of Section 34.

The minimum (simplified) CDD requirements under the Act are set out in Section 22 of Division 2.

Subdivision 2 – CDD requirements (Sections 20 to 29)

Section 22. Simplified CDD - identity and verification requirements.

(1) A financial institution must obtain such information in relation to a person or unincorporated entity referred to in Section 20(1), as may be necessary to establish his identity.

(2) The information may include –

a) for a natural person, his/her full name and address; and

[…]

(3) A financial institution must verify the identity information obtained under Subsection (2) so it is satisfied that the information obtained is correct.

[….]

The standard CDD requirements under the Act are set out in Section 24 of Division 2.

Section 24. Standard CDD - identity requirements.

(1) A financial institution must obtain such information in relation to a person or unincorporated entity referred to in Section 20(1), as may be necessary to establish his identity, which may include but is not limited to the following

(a) for a natural person, his full name, address, date of birth, place of birth, occupation and such other information as is necessary to establish his identity

[….]

The identify verification requirements under the Act are set out in Section 25 of Division 2.

Section 25. Standard CDD - verification of identity requirements.

(1) A financial institution must, at a minimum, undertake the following verification of identity requirements of a person or unincorporated entity referred to in Section 20(1), when conducting standard due diligence -

(a) *take reasonable steps to satisfy itself that the information obtained under Section 24 is correct; and*

(b) *according to the nature and level of risk involved, take reasonable steps to verify any beneficial owner's identity so that the financial institution is satisfied that it knows who the beneficial owner is; and*

(c) *if the person is acting on behalf of the customer, according to the nature and level of risk involved, take reasonable steps to verify the person's identity and also verify that they are so authorised to act on behalf of the customer.*

[….]

3.1. Pursuant to Section 16 of the Act, a reporting entity must **verify the identity** of the person or entity on the basis of reliable and independent source documents, data or information.

3.2. The reference to "data or information" in Section 16 of the Act supports the use of e-KYC in the process of accurately identifying customers or clients. A reporting entity may use e-KYC in the process of verifying the identity of its customers or clients by confirming biometric data such as finger/palm/handprints; iris scan; facial recognition; voice recognition (or similar) in addition to other identity information and documents. Reporting entities are encouraged to do the verification against system or documents that have the legal mandate to maintain respective data.

3.3. Where a customer uses a non-face-to-face service, the reporting entity may use e-KYC to verify the customer's on-boarding information by relying on one or more of the following checks relating to:

a). A repository of identity (card, token, application and similar);
b). Information known only to the owner of digital identity (a password, PIN or pass phrase);
c). A biometric data (finger/palm/handprints; iris scan; facial recognition; voice recognition or similar); or
d). QR code or OTP sent on the registered phone of the customer.

4. Digital Identity Systems for e-KYC

4.1. A reporting entity may employ a digital identity system to conduct e-KYC. This may be provided by a government, private sector entity, or other agent that provides a reliable, credible and secure service, with a legal mandate to store such data, to the reporting entity. This approach ensures national coverage, facilitates deduplication, and prevents the creation of multiple databases containing the same information.

4.2. Digital identity systems may include the use of artificial intelligence, machine learning, predictive algorithms and other technologies of relevance that may arise.

> **!** **It is the obligation of the reporting entities to assure themselves that the digital identity system has a legal mandate to provide a reliable, credible and secure service. A reporting entity must develop and implement appropriate policies that ensure the use of digital identity systems meet requirements under the Act and any relevant privacy provisions**

4.3. A reporting entity must maintain records on the use and real or potential vulnerabilities of digital identity systems and provide reporting on this at the request of FASU and/or BPNG. **Table 1** below provides an example of a reporting template of e-KYC identification and verification cases that can be used for reporting entities.

Table 1: Example of a reporting template of e-KYC identification and verification cases.

e.g.

	Year			
Data	Jan	Feb	Mar	Total Q1 of Year
Total customers identified and accepted digitally without physical presence.				
Total customers verified by digital identity system of reporting entity				
Comments or comparative analysis per month/quarter/year				

5. Ongoing Review of Digital Identity and e-KYC Systems

5.1. A reporting entity must continuously monitor its digital identity and e-KYC systems and implementation processes to ensure efficacy. Proper records of the customer's identity and evidence of e-KYC must be maintained by reporting entities at all times in digital format.

5.2. A reporting entity must have access to or processes in place that enable regulatory authorities including law enforcement agencies (LEAs) to obtain identity information and evidence for its customers in compliance with the applicable legislations(s).

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