2025

Financial Analysis and Supervision Unit

Guidance for Reporting Entities to Raise Awareness on the Identification of Linked Transactions (No. 5 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	31.08.22	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

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
NBFI	Non-Bank Financial Institutions
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. **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.

1.3. **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.

1.4. **Customer Due Diligence** (CDD) is, at a minimum, the process of:

a). identifying a customer and ensuring that they are who they claim to be, i.e. verifying the customer;

b). maintaining current and up to date information and records relating to the customer and (where relevant) their beneficial owners, and the nature and purpose of the business relationship, and the customer's commercial or personal activities; and

c). ensuring that transactions carried out on behalf of a customer are consistent with the financial institution's knowledge of the customer, the customer's commercial or personal activities and risk profile, and where necessary, the source of the funds.

[1] "Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.
[2] "Control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to make decisions about financial and operating polices.
[3] Person as defined under Section 5 of the Act means a natural person and a body corporate.

1.5. **Designated Non-Financial Businesses 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.

1.6. **Financial Analysis and Supervision Unit (FASU)** is established under Section 61 of the Act whose functions are set out in Section 72(1)(2)(3) of the Act which are to:

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

1.6.2. monitor and enforce compliance with the Act; and

1.6.3. receive reports and information provided to it under PNG's proceeds of crime law and disseminate such reports and information in accordance with PNG's proceeds of crime law and the Act.

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

1.8. **Geographic feature** means transaction(s) linked to customer connected with countries that are known to have relaxed anti-money laundering and combating terrorist financing (AML/CTF) controls.

1.9. **Occasional transactions** mean a transaction that takes place outside an existing business relationship.

1.10. **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.

1.11. **Reporting Entity** means financial institutions and DNFBPs that have a legal requirement to comply with the Act and an entity that has registered with FASU pursuant to Section 57 of the Act.

1.12. **Transaction** means a purchase, sale, loan, pledge, gift, transfer, delivery or other disposition or the arrangement of such purchase, sale, loan, pledge, gift, transfer, delivery or other disposition and includes, but is not limited to the opening of an account; any deposit, withdrawal, exchange or transfer of assets in any currency whether in physical currency or by cheque or other bearer negotiable instrument or in non-physical currency. It also includes the use of a safety deposit box or other form of safe deposit; entering into any fiduciary relationship; any payment made or received in satisfaction, in whole or in part of any contractual or other legal obligation; any payment made in respect of a lottery, bet or other game of chance; establishing or creating a body corporate or unincorporated entity.

i	In the Act, reference to a 'transaction' includes a reference to an attempted transaction.

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 in PNG to effectively comply with their obligations under Sections 23, 39, and 48 of the Act by properly and consistently identifying linked transactions.

2.4. The identification of linked transactions is crucial to prevent customers from structuring their transactions to circumvent the reporting requirements under the Act, and /or relevant domestic or international laws. Evidence shows that sometimes international transactions are deliberately structured to evade threshold reporting obligations in other jurisdictions.

2.5. To ensure compliance with the Act, reporting entities must implement approved processes, procedures and robust systems to identify transactions intended to avoid identification or other due diligence measures.

2.6. FASU has analysed a range of information and intelligence in the development of this Guidance. The criteria outlined below for identifying linked transactions is accurate at the time of the publication of this guideline but may change over time. Reporting entities shall use discretion, combined with the results of their own risk assessments, to determine the applicability of the specific criteria to their own customer or client population. The criteria in this guidance should however be considered the minimum.

2.7. This Guidance intends to provide industry guidance, practical assistance and a means for reporting entities to better comply with their anti-money laundering and counter terrorist financing (AML/CTF) obligations under the Act. The Guidance should be read in conjunction with the following FASU Guidance below, which are available on the website of the Bank of PNG:

2.6.1. *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); and

2.6.2. *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).

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

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

2.9. Some of the 'marks' used in the textboxes of this Guidance should be read as below:

i	Textbox in this format provides information to assist reporting entities understand their obligations and the provisions in the Act to which those obligations relate.
e.g.	Textbox in this format provides appropriate examples.
!	Textbox in this format stresses important information for reporting entities, including on penalties for non-compliance with obligations under the Act.

3. Requirements under the Act

3.1. The term "**transactions that appear to be linked**" is referred to in three sections of the Act:

a). **Section 23**: Circumstances where standard CDD applies

b). **Section 39**: Threshold reporting obligations

c). **Section 48**: Obligation to keep identity and verification records

3.2. While Sections 23, 39, and 48 outline the obligations of financial institutions, Section 52(1) of the Act explicitly states that these provisions apply equally to DNFBPs.

3.3. The details of the above relevant sections are provided in **Table 1** below.

Table 1: Relevant Provisions from the Act

Section 23: Circumstances where standard customer due diligence applies

(1) A financial institution must conduct standard customer due diligence in accordance with the requirements of Sections 24 and 25 in the following circumstances:
[…] (b) if a customer wishes to carry out an occasional transaction of an amount in currency equal to or greater than K20,000.00, whether conducted as a single transaction or by way of ***several transactions that appear to be linked****; or*

Section 39: Threshold reporting obligations

(1) A financial institution must report to FASU a transaction of an amount in physical currency, or in the form of a bearer negotiable instrument, equal to or greater than K20,000.00 that is carried out as a single transaction or ***two or more transactions that appear to be linked.***

(2) A financial institution must report to FASU an international electronic funds transfer of an amount in currency equal to or greater than K20,000.00, that is carried out as a single transaction or ***two or more transactions that appear to be linked****.*

(3) A financial institution must report to FASU under Subsection (l) or (2), as soon as reasonably practicable and in any event within 10 working days from the date of the transaction where it is a single transaction, or from the date of the last transaction, where there are ***two or more transactions that appear to be linked.***

Section 48: Obligations to keep identity and verification records

[…] (b) after carrying out an occasional transaction of an amount in currency equal to or greater than K20,000.00, whether conducted as a single transaction or by way of ***several transactions that appear to be linked****; or […]*

Failure to comply with threshold reporting obligations

! **A person who intentionally and/or recklessly fails to make a report to FASU under Section 39 (1) or (2) is guilty of a crime punishable by fines of K500,000.00 for an individual and K1,000,000.00 for a body corporate pursuant to Section 39(6) of the Act.**

4. Factors to Determine Identification of Linked Transactions

Based on the analysis of current intelligence available to FASU, linked transactions may be identified by reference to the **timeframe**, **amount**, and **nature and circumstances** of the transactions.

4.1. Timeframe

4.1.1. Transactions can only be practically and reasonably assessed as being linked if they occur within a reasonable timeframe. While linked transactions might occur over a longer period, FASU has selected the timeframes provided below in Table 2 for the identification of transactions that may be identified as linked.

Table 2: Timeframe to identify linked transactions

Number of transactions	Timeframe of Transactions
2 or more	24 hours
2 or more	48 hours
2 or more	72 hours
2 or more	96 hours

4.1.2. Table 2 above shows the number of transactions and the timeframe. If two transactions are conducted within 24 hours of each other (and they satisfy the criteria with respect to the amount and the nature and circumstances) they should be considered to be linked. Similarly, if two or more transactions are conducted within 48 hours; two or more transactions within 72 hours and so on.

4.1.3. Each group of two or more linked transactions may be reported as a single linked transaction. However, reporting entities that identify two or more linked transactions (or repeated groups of two or more) should consider submitting a Suspicious Matter Report (SMR) and initiating Enhanced Customer Due Diligence (ECDD) to determine the reason behind the linked transactions.

4.1.4. While there are undoubtedly other timeframes by which transactions might be argued to be linked, the timeframes listed above are intended to achieve a pragmatic balance between the need to identify a financially motivated crime and the need to have a process that is realistically actionable by reporting entities.

4.1.5. Table 2 above can be used to guide REs when developing internal policies or standard operating procedures to deal with assessments of linked transactions for the different timeframes.

4.2. Amount Transacted

4.2.1. The primary purpose behind the requirement for reporting entities to identify linked transactions is to identify the structuring behaviour. This structuring might be undertaken to avoid AML/CTF reporting requirements, or there may be reporting requirements under other legislation such as exchange controls or taxation legislation. These reporting requirements may be in PNG or another jurisdiction.

4.2.2. To be reportable, linked transactions must exceed the reporting threshold limit for PNG. That is, the cumulative total must be equivalent to or more than K20,000.00 *For example*, if three cash deposits or international funds transfers are conducted within a 24-hour period and their total amount is K20,000.00 or more, they must be reported as linked transactions.

4.3. Nature and Circumstances

4.3.1. The nature and circumstances of linked transactions is that they involve common people, accounts and/or entities. This may be a single individual breaking up an amount into multiple transactions to avoid triggering the submission of a threshold transaction report (by exceeding the K20,000.00 limit with any one transaction).

4.3.2. Linked transactions may also occur where an individual or entity uses a group of people to make multiple deposits into multiple accounts – in such a case, it is the source of the funds that is the commonality. Multiple people making deposits from a single source of cash or funds is known as 'smurfing'.

4.3.3. Linked transactions may also occur where multiple people make transactions to a single account/person/entity offshore. In such circumstances, it is the offshore entity that is the commonality.

4.3.4. In all cases of linked transactions there is a single person, entity or account at one end or the other of the transactions. This person/entity/account may be located domestically or offshore.

5. Linked Transactions and Suspicious Matter Reports

5.1. Reporting entities that identify possible linked transactions that appear to have been conducted in order to avoid triggering the submission of a threshold transaction report must consider submitting a SMR, in addition to any other reporting requirements.

5.2. In deciding whether there is a risk that transactions are being deliberately split into separate operations, the reporting entity needs to consider the circumstances of the transactions. *For example*:

a). Are a number of transactions carried out by the same customer within a short span of time?

b). Could a number of customers be carrying out transactions on behalf of the same individual or group of individuals?

c). In the case of money transmission, are a number of customers sending payments to the same individual?

5.3. Reporting entities must be able to demonstrate to FASU that they have adequate checks and controls in place to detect/identify such indicators where there is a risk of transaction(s) (that is, transactions equal to or over K20,000.00) being disguised as smaller transactions. The systemic controls and processes would include transaction monitoring and/or obtaining information on the source of funds and the purpose of the transactions from the customer. The indicators of risk and the appropriate enquiries to be made should be specified in the reporting entity's risk profiling, policies and procedures.

e.g. *1*	Multiple deposits or withdrawals within a 24-hour period by the same customer that in total equals to or exceeds K20,000.00
e.g. *2*	Multiple international electronic funds transfers, made or received, in a 48-hour period by the same sender or to the same recipient where the cumulative total is equal to or more than K20,000.00;
e.g. *3*	Multiple domestic cash transactions, or international electronic funds transfers, made or received, in a 48-hour period where either the payees or beneficiaries are groups of related or associated people/entities and there is reasonable suspicion that they are being controlled or influenced by a single person or entity.

6. Annexure 1 – More Clarification on Reporting Obligation

6.1. This annexure aims to enable reporting entities to submit consistent and effective reporting of Threshold Transaction Reports (TTR), International Electronic Funds Transfer Reports (IEFTR) under Section 39, and SMR under Section 41 of the Act to FASU.

6.2. The following are circumstances/ examples to provide clarity and guide reporting entities to comply with the reporting requirements pertaining to Part II, Division 3 – Reporting Obligations (Sections 39 to 46) under the Act.

Threshold Reporting Obligations – Section 39	**TTR (Y/N)**	**Instrument used**	**Comments/Description**
(1) A financial institution must report to FASU a transaction of an amount in physical currency, or in the form of a bearer negotiable instrument, equal to or greater than K20,000-00 that is carried out as a single transaction or two or more transactions that appear to be linked.	Y	Physical currency (PC), Bearer negotiable instrument (BNI), electronic fund transfer (EFT), mobile banking transfer (MBT)	Subsection 1 covers a domestic single transaction or two or more transactions that appear to be linked and totalling ≤ K20, 000.00 to be reported to FASU as a Threshold Transaction Report (TTR). The transactions covered may include; • cash deposit/withdrawal • cheque deposit/withdrawal • electronic banking transfer (in/out) • mobile banking transfer (in/out) BNI is to be understood within the meaning of "BNI" in section 5 to mean, "a bill of exchange, or a cheque, or a promissory note, or a bearer bond, or a traveller's cheque, or a money order, postal order or similar order, or a negotiable instrument not covered by any of the above paragraphs" **Note:** The definition of "transaction" under Section 5, includes "transfer". For the purposes of the AMLCTF Act, a "transaction" or a "transfer" should include an "EFT", which is also define in section 5 and is a means by which the transaction or transfer occurs. This applies to Section 39(1) and (2) transactions. 1. Although EFT is not specifically mentioned in s.39 (1), it is a primary *means* through which a Section 39(1) and (2) transaction occurs. The EFT encompasses any money transfer domestically and across national borders, including TT and other methods like wire transfers. 2. Like EFT, MBT is not specifically mentioned in Section 39(1), MBT and similar others, are a type of service that comes within the definition of "EFT". Therefore, by their nature, they would be considered a Section 39(1)(2) transaction.

Threshold Reporting Obligations – Section 39	TTR (Y/N)	Instrument used	Comments/Description
(2) A financial institution must report to FASU an **international electronic funds transfer** (IEFT) of an amount in currency equal to or greater than K20,000-00 that is carried out as a single transaction or two or more transactions that appear to be linked.	Y and N	International electronic funds transfer (IEFT), Internet Banking (IBT) transfer, Mobile Banking (MBT) Transfer.	Section 39(2) is specific to IEFT however the following examples can be used as a guide for a RE to identify circumstances where more than one IEFT is carried out below the threshold of K20, 000.00 but totaling ≥ K20, 000.00 and are assessed by the RE to be linked; and also circumstances where TTR may be required to be reported to FASU. This is to avoid possible duplicate reporting of TTR and IEFT where an IEFT amount is ≥ K20, 000.00. **Example 1** Joe has more than K20, 000.00 in his local bank account and carries out an international wire transfer via a *Telegraphic Transfer (TT*) for K20, 000.00 by signing a debit to his account for funds to be remitted to his overseas bank account. **Reports to be submitted to FASU**; 1) IEFTR to report K20, 000.00 offshore remittance from local account to overseas account via ***telegraphic transfer (TT).*** *There is no need to report the IEFT as a TTR as well for the same amount unless there was a corresponding prior credit made to the account if there was insufficient balance to cover for the IEFT.* **Example 2** Joe has more than K20, 000.00 in his local bank account and carries out an international fund transfer of K20, 000.00 via *internet banking* by transferring the funds from his local account to his overseas bank account **Reports to be submitted to FASU;** 1) IEFTR to report the cross-border internet banking transfer of K20, 000.00 from Joe's local account to his overseas account. *There is no need to report the IEFT as a TTR as well for the same amount unless there was a corresponding prior credit made to the account if there was insufficient balance to cover for the IEFT.* **Example 3** Joe maintains his salary account for an average daily balance of K600.00. However, he receives three (3) lots of deposits into his personal account over a period of three days and conducts an

Threshold Reporting Obligations – Section 39	TTR (Y/N)	Instrument used	Comments/Description
			international fund transfer on the fourth day as follows; **Day 1** - deposit of K7, 000.00 **Day 2** - deposit of K10, 000.00 **Day 3** - deposit of K5, 000.00 **Day 4** - International fund transfer to his offshore bank account for K22, 000.00 **Reports to be submitted to FASU;** 1) TTR for K22, 000.00 (sufficient information to suggest that the three deposits are linked hence the requirement to report TTR) 2) IEFTR to report K22, 000.00 offshore remittance from local account to overseas account. 3) Suspicious Matter Report (SMR) to report any suspicion arising from the RE's assessment of the sudden change of account activity that may alter the RE's view of the customer's risk profile. **Circumstances of prior transactions on domestic account before conducting cross-border transaction** The following scenarios maybe useful for a RE to gain a better understanding; and determine instances when **NOT** to submit a TTR and when to submit both a TTR, IEFTR and/or SMR to FASU. If a prior transaction of ≤ K20, 000.00, or more than one transaction of amounts totaling ≤ K20, 000.00 has occurred to credit an account that was or will be debited for an IEFT transaction, then **ONLY** that prior **credit** transaction can be reported as a TTR to FASU and **NOT** the **debit** transaction to facilitate the IEFT. This debit transaction can be reported as an IEFT report to FASU. **Example 4** Joe ***deposited*** K20, 000.00 (cash) in his account. He also requested an international wire transfer for the same amount by authorizing a debit to his local account to ***remit the funds offshore via telegraphic transfer (TT).*** **Reports to be submitted to FASU;** 1) TTR to report K20, 000.00 cash deposit;

Threshold Reporting Obligations – Section 39	TTR (Y/N)	Instrument used	Comments/Description
			2) IEFTR to report K20, 000.00 offshore remittance from local account via ***telegraphic transfer (TT).*** 3) SMR to report any suspicion arising from the RE's customer due diligence (CDD) assessment of the customer's cash deposit transaction. **Example 5** Joe made numerous ***small deposits*** totaling K20, 000.00 (cash) in a day into his account. He also conducted an ***international electronic fund transfer*** for the same amount through *internet banking* to an offshore bank account**.** **Reports to be submitted to FASU;** 1) TTR to report K20, 000.00 cash deposits *(numerous structured deposits that appear to be linked);* 2) IEFTR to report K20, 000.00 offshore remittance from local account via ***telegraphic transfer (TT).*** 3) SMR to report any suspicion arising from the RE's CDD assessment of the structuring of small cash deposits prior to remitting funds offshore. **Example 6** **Using a combination of different channels to conduct linked transactions, use of mobile banking transfers, KATS and internet banking transfer into account;** Joe maintains his salary account for an average daily balance of K500.00. However, he receives three (3) lots of credits into his personal account from different bank account holders. Two (2) of those transactions were received on the same day but at different times using KATS transfer and internet banking transfer. Another credit was received on the third day via mobile banking transfer. He then carries out an international fund transfer via TT on the fourth day as follows; **Day 1** - deposit of K8, 000.00 **Day 2** - deposit of K12, 000.00 **Day 3** - deposit of K1,000.00 **Day 4** - International fund transfer to his offshore bank account for K21, 000.00 **Reports to be submitted to FASU;**

Threshold Reporting Obligations – Section 39	TTR (Y/N)	Instrument used	Comments/Description
			1) TTR for K21, 000.00 (sufficient information to suggest that the three credits/inflows are linked hence the requirement to report TTR) 2) IEFTR to report K21, 000.00 offshore remittance from local account to overseas account. 3) SMR to FASU for credits into Joe's account with no clear transaction description as well sudden change on inflow into his account.
(3) A financial institution must report to FASU under Subsection (1) or (2), as soon as reasonably practicable and in any event within 10 working days from the date of the transaction where it is a single transaction. Or from the date of the last transaction, where there are two or more transactions that appear to be linked.	N/A	All. (PC, BNI,IEFT)	FI must have internal policies that guide the institution with a clear process for meeting this requirement.
(4) A financial institution must provide a report required under Subsection (1), in accordance with any form and procedure specified by FASU	N/A	All. (PC, BNI,IEFT)	TTR should be provided in line with the TTR specifications. FASU will consult with all reporting entities to communicate any changes to the reporting formats
(5) Compliance with Subsection (1) does not affect the obligation of a financial institution to make a suspicious matter report under Section 41 (4).		All. (PC, BNI,IEFT)	Reporting a TTR is a mandatory report for transactions that meet the threshold requirement of ≤K20, 000.00, and should be made as a separate report even-though the RE has formed a suspicion that is subject to SMR reporting requirements.
(6) A person who intentionally fails to make a report under subsection (1) or (2), is guilty of a crime.	N/A	All. (PC, BNI,EFT, MBT, IEFT)	FASU will undertake an approach for imposing penalties in line with its internal policy/process relating to the enforcement of the Act.

Suspicious Matter Reporting- Section 41	**TTR/ IEFT (Y/N)**	**Instrument used**	**Comments/Description**
(1) This section applies where a financial institution has reasonable grounds to suspect that information that is known to it may- *(a)* be relevant to the detection, investigation or prosecution of a person for money laundering , terrorist financing, an offence under Section 15 or 16 of the United Nations Financial Sanctions Act 2015 or any other indictable offence; and *(b)* be relevant to the detection, investigation or prosecution of a person for a foreign indictable offence; *(c)* concern criminal property	Y – if transaction completed and meets TTR/IEFT requirements N- if transaction not complete	All. (PC, BNI,EFT, MBT, IEFT)	A reporting entity may form a suspicion based on the following examples but not limited to; • a customer's conduct of a transaction or behaviour; • assessment or review of the customer's transactions or behavioural patterns through monitoring based on the customer's risk profile; • open source information (internet, mainstream and social media) known to the RE • human source intelligence gathered through formal or informal gathering/discussions • known associations with other known high risk customers Submission of a SMR in line with the above examples may be relevant to; a) Providing information that may be useful for appropriate PNG law enforcement authorities to detect, investigate and prosecute any person that may have committed a possible indictable offence in PNG b) Providing information that may be useful for appropriate PNG law enforcement authorities to detect, investigate and prosecute; or support international counterpart law enforcement authorities to detect, investigate and prosecute any person that may have committed a possible foreign indictable offence in the concerned jurisdiction c) Providing information that may be useful for relevant PNG law enforcement authorities to trace funds to identify property that is linked to criminal conduct, where according to s.5 of the AMLCTF ACT, "criminal property" and "criminal conduct" have the meaning given by s. 508A of the Criminal Code Act as amended.; "Criminal Property" and "Criminal Conduct" are 2 important elements in proving both s.508B and s.508C money laundering offences in the Criminal Code as amended.

			Both offences are also "serious offences" and "indictable offences" that if committed, could form the basis of recovery action under the POCA 2022. An illegally obtained asset is regarded as criminal property and may be subject to a proceeds of crime (POC) action undertaken by relevant PNG law enforcement authorities, relevant government agencies and international partners when pursuing assets in other jurisdictions
(2) For the avoidance of doubt, Subsection (1) applies where a suspicion is formed after this Act comes into operation, but that suspicion may be based on information obtained before this Act came into operation.			The Act gazette by the National Executive Council in February 4, 2016. Hence, the Act came into operation after its gazettal in 2016. The following is an example of an instance where Section 41 (2) may be applicable; **Example:** In 2015, Company A, a high valued customer for the Bank received a government cheque payment worth K10 million to construct a new bridge outside of Port Moresby and provided all necessary supporting documents required when the Bank conducted its due diligence. Company A satisfied CDD requirements prompting limited to no further monitoring of the customer's transactional behavior. In 2016, after the Act came into operation, the Bank while carrying out periodic reviews of its high valued customers, identified several internet banking transfers by Company A after receiving the K10 million, to various personal accounts owned by officials within the responsible government departments that facilitate government tender and project/contract funds. The review further uncovered that the officials who had received funds from Company A were officers empowered with authority within the government's procurement process hence there is sufficient grounds to form a suspicion and report a SMR to FASU based on the initial deposit of K10 million carried out in 2015.

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