Financial Analysis and Supervision Unit

Guidance for Financial Institutions on their Obligations under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 1 of 2019)

Issued by the Financial Analysis and Supervision Unit on 20th of May 2019

DOCUMENT VERSION CONTROL

Version	Date Issued	Document Status	Document Author
1	14.05.2018	Draft	FASU & DJAG
2	31.05.2018	Draft	FASU & DJAG
3	13.02.2019	Draft	FASU
4	20.05.2019	Final	FASU

Table of Contents

1 Note to reading this Guidance

This Guidance uses the following acronyms:

Act	*Anti-Money Laundering and Counter Terrorist Financing Act* 2015
AML/CTF	anti-money laundering and counter terrorist financing
DNFBP	A designated non-financial business or profession in PNG, as defined in section 5 of the Act.
FASU	Financial Analysis and Supervision Unit
Financial Institution	A financial instituion, as defined in section 5 of the Act.
Guidance	Guidance for Financial Institutions on their Obligations under the *Anti-Money Laundering and Terrorist Financing Act* 2015 (No.1 of 2019)
i	Textbox in this format provides information to assist financial institutions, including on 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.

All references to section numbering are to sections in the Act, unless stated otherwise.

2 Purpose of this Guidance

This Guidance provides clarification to financial institutions on their obligations under the Act, and sets out FASU's expectations of industry. Assisting financial institutions to comply with the Act will support PNG's efforts in helping to reduce corruption and tax avoidance, and protect PNG against financial criminal activities.

The obligations incurred by financial institutions are primarily set out in Part II (Sections 6 to 51), Part IV (Sections 54 to 58) and Part V (Section 59) of the Act. Additional obligations are set out in Part VI of the Act. These measures introduce a comprehensive legal framework to detect and deter money laundering and terrorist financing.

Under the Act you must:

- conduct a risk assessment and put in place an AML/CTF program;
- conduct customer due diligence;
- conduct due diligence on domestic and international electronic fund transfers;;
- report threshold transactions and suspicious and other matters;
- maintain adequate records;
- ensure foreign branches and majority-owned subsidiaries implement measures equivalent to those in the Act;
- comply with beneficial ownership requirements and ensure directors, chief executives, senior managers or persons in other equivalent positions meet fit and proper criteria;
- register with FASU;
- provide requested information and records to FASU; and
- comply with compliance and enforcement measures imposed by FASU.

! **This Guidance is intended to assist you in complying with the Act. It is not legal advice, and as such, is not intended to replace the Act.**

3 Overview

Money laundering and terrorist financing present a global problem for criminal justice systems and a macro-economic problem, as these activities have the capacity to destabilise financial institutions and financial systems. As part of the international community's response to fight transnational crime, PNG became a member of the Asia/Pacific Group on Money Laundering (APG) in December 2008. The APG is an autonomous and collaborative international organisation founded in 1997. It consists of member countries within the Asia Pacific region and a number of international and regional observers.

By virtue of its membership with the APG, PNG is required to implement the *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* set by the Financial Action Task Force (FATF). FATF is an international and inter-governmental body established in 1989 by the Ministers of its member jurisdictions. FATF ensures that member countries, including international and regional bodies, implement appropriate measures globally to combat money laundering and terrorist financing. Therefore, PNG, through its membership with APG, is under the purview of both APG and FATF.

PNG's robust AML/CTF regime

To implement the FATF standards in line with international best practice, PNG's Parliament passed five important laws in 2015, which came into operation on 4 February 2016. The laws introduced a comprehensive framework to detect and deter money laundering and terrorist financing, strengthened the criminal offences of money laundering, and introduced a new terrorist financing offence. By introducing measures to prevent the flow of illicit funds and to combat transnational crime, these laws increase the financial integrity of Papua New Guinea's financial system.

PNG's anti-money laundering and counter terrorist financing (AML/CTF) regime is a whole-of-government led approach, which includes all its key agencies in regulating against money laundering and terrorist financing.

The regime seeks to secure the economy and safeguard the integrity of the financial system from being abused by money launderers or used for terrorist financing, while ensuring the financial system is safe and accessible for both national and international investors.

In addition, the regime ensures the financial system is safe and secure for businesses, investors and traders. This is important because financial sectors are most vulnerable to money laundering and terrorist financing due to the inherent nature of their businesses.

Therefore, financial institutions must conduct risk assessments to identify the nature and level of money laundering and terrorist financing risks they may reasonably expect to face in the course of their businesses. To do so, financial institutions must consider their customers, products, delivery channels, and geographical location of their customers and beneficiaries of funds.

This will ensure financial institutions target their resources more effectively and apply preventative measures to mitigate money laundering and terrorist financing risks involved in their businesses.

PNG's Anti-Money Laundering and Counter Terrorist Financing Act 2015

PNG's ***Anti-Money Laundering and Counter Terrorist Financing Act*** **2015** (Act) replaced certain provisions in PNG's ***Proceeds of Crime Act*** **2005**. It introduced a robust regulatory framework consistent with the FATF standards to prevent money laundering and terrorist financing. The measures apply to financial institutions and designated non-financial businesses or professions (DNFBPs).

Importantly, the Act established the Financial Analysis and Supervision Unit (FASU), an operationally independent financial intelligence unit within the Bank of PNG. Previously, the financial intelligence unit was housed in the Royal PNG Constabulary (RPNGC). Under the Act, FASU collects, analyses and disseminates financial intelligence, including to the RPNGC for investigative purposes. In addition, FASU supervises financial institutions and DNFBPs for compliance with their obligations under the Act.

The Act will be strengthened by subsidiary instruments, including regulations, AML/CTF compliance rules and guidance developed by FASU over time, and in consultation with industry. In addition, FASU has developed and issued reporting forms to assist financial institutions and DNFBPs to comply with their reporting obligations under the Act.

4 Application of the Act

i

The Act applies to a domestic and foreign financial institution located in PNG (Section 4).

In addition, a financial institution of PNG must ensure its foreign branches and majority-owned subsidiaries located outside PNG apply measures broadly equivalent to those in Part II of the Act (Section 54).

You must comply with the obligations in the Act if you are a 'financial institution'. You are a financial institution if you are a natural person, legal person or unincorporated entity (such as a trust or partnership) that conducts certain types of activities for or on behalf of a customer. These activities include:

- the acceptance of deposits and other repayable funds from the public, including private banking;
- lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;
- financial leasing other than with respect to arrangements relating to consumer products
- the transfer of currency or value;
- issuing and managing means of payment including, but not limited to, credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and currency in non-physical form;
- issuing financial guarantees and commitments;
- trading in-
  - bearer negotiable instruments;
  - foreign exchange;
  - exchange, interest rate and index instruments;
  - transferable securities; or
  - commodity futures trading.
- participation in securities issues and the provision of financial services related to such issues;
- individual and collective portfolio management;

- safekeeping and administration of physical currency, bearer negotiable instruments or liquid securities on behalf of other persons;
- investing, administering or managing assets on behalf of other persons;
- underwriting and placement of insurance, including insurance intermediation by agents and brokers; and
- currency changing.

You must comply with the Act if you are operating your business within PNG. This is the case even if you are, for example, a foreign company based in PNG. This is important because it will ensure the preventative measures in the legislation are applied consistently in the country, which will increase the effectiveness of the regime. In addition, you must apply certain measures to any foreign branches and majority-owned foreign subsidiaries you operate outside of PNG.

5 Key concepts and terms

i

A number of terms are defined in Section 5 (Interpretation). You must rely on the technical definitions of these terms.

For the purpose of assisting financial institutions in understanding their obligations, this Guidance provides a lay explanation of some of these key terms.

Customer means a person or unincorporated ent strengthening ity who does business with a financial institution or DNFBP and includes a new or existing customer. A person who has ultimate control and/or ownership of a customer is known as the **beneficial owner** of the customer.

Customer due diligence (CDD) is the process of identifying your customer and ensuring that they are who they claim to be, i.e. verifying the customer. CDD also includes maintaining current identification and records of the customer.

DNFBP means a designated non-financial business or profession in Papua New Guinea. These include real estate agents, dealers in precious metals or precious stones, lawyers, notary public or other independent legal professionals when undertaking transactions on behalf of a client, trusts or company service providers and motor vehicle dealers.

Financial institution includes commercial banks, micro banks, finance companies, savings and loans societies, insurance companies, insurance agents and brokers, brokerage firms, superannuation funds, leasing companies, funds management companies and money changers.

Money laundering is the process of making dirty money appear clean. **Terrorist financing** is providing or collecting property to finance terrorist activities, individual terrorists or terrorist organisations.

Politically exposed person 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.

Premises include a structure, building, vehicle, aircraft or vessel; or a place, whether or not it is enclosed; or built upon or a part of a premise.

Regulatory authority includes the Bank of PNG, Investment Promotion Authority, National Gaming and Control Board, Certified Practising Accountants PNG, PNG Law Society, Office of the Insurance Commission, Securities Commission of PNG, and other agencies or bodies that grant licences, practising certificates and registrations.

Risk can mean the likelihood of an event and its consequences. Simply, risk in the context of money laundering and terrorist financing is determined by two concerns:

- the **threat** posed by people who are or may be your customers and how **vulnerable** your business is to possible exploitation by your customers; and
- the consequence or **impact** to you and your business if it does occur.

Threat: this could be a person, group, or object that could cause harm. A threat could be criminals, facilitators, their funds or even terrorist groups.

Vulnerability: elements of a business that could be exploited by the threat. A vulnerability could be weak controls within a financial institution, or offering high risks products or services, etc.

Impact: this refers to the seriousness of the damage that would occur if the risk materialises.

Risk assessment is the process of identifying, analysing and evaluating, and mitigating and managing risks.

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 devise.

Suspicious matter refers to a questionable transaction or action by a customer that raises reasonable doubts and/or suspicions by the financial institution.

6 Understanding money laundering and terrorist financing

! **Understanding the nature of money laundering and terrorist financing is fundamental to assessing the risk your business reasonably faces in relation to these criminal activities, and to developing and implementing effective measures to address these risks.**

The vast majority of criminals would not be in the "business" of crime if it were not for the tremendous profits to be made. The sheer magnitude of money laundering activities demonstrates the importance of implementing strong anti-money laundering regimes in countries throughout the world. The economic and political influence of criminal organisations can potentially weaken the social fabric, collective ethical standards, and ultimately, the democratic institutions of society.

Money laundering activities have the potential to distort economic data and cause economic growth to suffer. The relationship between gross domestic product growth and money laundering in industrial countries results in significant reductions in annual gross domestic product growth rates.

The main objective of terrorist activity is to intimidate a population or compel a government to do something. This is done by intentionally killing, seriously harming or endangering an individual or causing substantial property damage that is likely to seriously harm people. It can also be done by seriously interfering with or disrupting essential services, facilities or systems.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organisation, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to obtain whatever goods or services needed to commit terrorist acts.

The fundamental aim of terrorist financing is to obtain resources to support terrorist activities. The sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex.

What is money laundering

Simply, **money laundering** is the process of converting the proceeds of crime or money derived from criminal activities into legitimate funds through various creative methods. A person is a money launderer if the person disguises, conceals, converts, transfers, removes, receives or acquires currency, assets or cash that comes from crime.

Criminals deal mostly with cash because their illegal activity, i.e. dealing in drugs, prostitution, smuggling and human trafficking, are not paid for by credit card or cheque. Money from these crimes is called 'dirty money'. This dirty money or assets are now placed, layered and integrated through the various financial institutions and professions to make them appear clean – laundered.

To launder money, criminals can simply deposit the money in a bank (placement), move the money between accounts and credit cards (layering), and invest the money in the share market and buy assets such as real estate, cars and expensive jewellery (integration).

Example of how illegal drug sales can easily by converted into an asset like a property

Crooks sells drugs for cash | Piles of illegal cash | Pay cash for real estate

The ***Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act* 2015** strengthened the crimes of money laundering in the ***Criminal Code Act* 1974.** It is a crime under new Section 508B of the Criminal Code Act for a natural person or body corporate to **know or reasonably ought to know** that the property is criminal property (i.e. dirty money) at any stage or part of the laundering process. Under new Section 508C of the Criminal Code Act it is a crime for a natural person or body corporate to deal with property **in circumstances where it is reasonable to suspect** that the property is criminal property.

People who commit crimes can launder the proceeds themselves ('self-laundering'), or they can launder their money through a third party who was not involved in the commission of the predicate offence ('third party money laundering'). The third party could be described as a facilitator, who could be guilty of either money laundering offence.

!

Money laundering is a crime punishable by up to 25 years imprisonment and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 508B of the *Criminal Code Act* 1974).

Dealing with property reasonably suspected to be criminal property is a crime punishable by up to 3 years imprisonment, and fines of K100,000 for an individual and K200,000 for a body corporate (Section 508C of the *Criminal Code Act* 1974).

Example of knowingly dealing with criminal property

e.g.

A bank clerk has a brother that she knows is mixed-up with a group of rascals selling drugs in the local bars over the weekend. On Monday morning the brother approaches his sister with his share of the dirty money and asks her to deposit it into her bank account. He does this as she has a proper job and can explain any money in her account. Because she knows her brother is unemployed and that the money is from the sale of drugs – this is knowingly dealing with criminal property (dirty money).

Example of reasonably suspecting property is criminal property

e.g.

A customer walks into Toyota Dealership with cash to purchase a top-of-the-line Toyota Prado. The dealer estimates his age to be approximately 25 years old and also he knows the client has a local trade store that doesn't make much money. The customer's cousin is a known smuggler. It is unlikely that the young man should have enough cash for a Toyota Prado. A reasonable person in the dealer's position should reasonably suspect that the cash is criminal property (dirty money).

What is terrorist financing?

Both individuals and organisations can be guilty of terrorist financing. This occurs where a person **directly or indirectly** provides or collects property (which includes funds) with the **intention or knowledge** that the property will be used to finance a terrorist act, a terrorist or a terrorist organisation. These funds may be legitimate monies, for example, raised through donations or illegitimate funds raised through crime. Property used in this context includes a wide range of assets such as cash, real estate, shares, vehicles, and other tangible and intangible assets.

Example of terrorist financing

Collecting money


Financing terrorists

Terrorist attacks

The ***Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act*** **2015** introduced comprehensive and effective criminal law provisions to create a comprehensive offence for terrorist financing in the ***Criminal Code Act*** **1974**. Section 508J makes it a crime for a person who by any means, directly or indirectly, provides or collects property with the intention or knowledge that it be used to finance a terrorist act, a terrorist (without lawful justification) or a terrorist organisation. Property has a broad definition in the Criminal Code Act.

> **!** **Terrorist financing is a crime punishable by up to 25 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 508J of the *Criminal Code Act* 1974).**

While terrorist financing has not been identified as currently a high risk in PNG's National Risk Assessment, this does not mean the financial system cannot be vulnerable to terrorist financing. Terrorist financiers usually provide or collect funds or assets at places such as:

- banks;
- charities;
- non-governmental organisations;
- offices of stock brokers, real estate agents, lawyers and accountants;
- when carrying out credit card fraud and credit card cloning;

- when moving physical cash across borders using formal or informal money remittance services; or
- establishing fake charities and non-governmental organisations.

Example of directly collecting and providing funds

e.g.	A terrorist group sympathiser wants to support his terrorist group that needs funds. He earns a good salary and has access to a network of remittance providers. He gives his money to the money remitter and asks that the equivalent funds be made available in the country where the terrorist organisation operates.

Example of indirectly collecting and providing property

e.g.	A terrorist sympathiser wants to support his terrorist group that needs funds. He doesn't earn much or have access to funds, but does have a warehouse that imports food. He arranges for a shipment of his foods to be exported to the country where his terrorist organisation operates to assist them feed their terrorists.

7 Risk assessments and AML/CTF programs

i The Act sets out the obligations on risk assessments and AML/CTF programs in Part II, Division 1 (Sections 6 to 14).

Assessing your risk of money laundering and terrorist financing

i The Act defines a risk assessment in Section 5(1) as:

> *A risk assessment means an assessment of the risk of money laundering and terrorist financing undertaken in accordance with Section 6.*

'Money laundering' and 'terrorist financing' are also defined in the Act. These definitions link to the offences of money laundering and terrorist financing in the *Criminal Code Act* 1974.

It is essential you identify and assess the nature and level of money laundering and terrorist financing risk you can reasonably expect to face in the course of your business. This is a 'risk assessment', which must be documented in writing (this includes being stored electronically).

Your risk assessment is an analysis of potential threats and vulnerabilities of money laundering and terrorist financing that your business is or may be exposed to, and their impact or consequences. The complexity of the assessment depends on the size and nature of your business, geographic areas in which you operate, products and services you offer, the delivery methods you use, the types of customers you have, including politically exposed persons, residents of high risk countries, and customers involved in high risk business activities. In addition, you need to consider any other risk factors relevant to your business.

Your risk assessment will underpin your AML/CTF program and assist you in determining the appropriate due diligence measures.

Appendix A provides a sample risk assessment.

AML/CTF programs

> *i*
>
> Key concepts to understanding the requirements of AML/CTF programs are:
>
> **Policy** means a general cause of action adopted by business
>
> **Procedure** means a set of series of actions
>
> **Control** means a standard for checking results
>
> **Effective** means producing intended results
>
> **Risk Mitigation** means implementing controls to limit the money laundering and terrorist financing risks identified in your risk assessment
>
> **Risk Management** means the ongoing management of risks after the controls are implemented
>
> **Risk Monitoring** means monitoring your risks to ensure your risk assessment is current; and
>
> **Due diligence** means demonstrating an appropriate thoroughness of knowing who your customer is and includes complete and up to date information on your customer.

You must **establish**, **implement** and **maintain** a written AML/CTF program based on your risk assessment:

- **establish** means setting up the AML/CTF program;
- **implement** means to carry the AML/CTF program into effect; and
- **maintain** means to keep the AML/CTF program relevant and up to date.

Your AML/CTF program must include effective **procedures**, **policies** and **controls** for:

- managing and mitigating the risks identified in your risk assessment;
- monitoring those identified risks;
- ensuring customer **due diligence** is carried out, including **ongoing due diligence;**
- Specifically, your AML/CTF program must set out-
    - when you may rely on a third party to conduct customer due diligence;
    - when you may conduct simplified customer due diligence;
    - when you must conduct enhanced customer due diligence; and
    - when you may complete the verification of the identity of a customer after the establishment of a business relationship
- complying with other requirements of the Act. These include appointing an AML/CTF compliance officer, reporting suspicious and other matters, and keeping records in a way that is auditable and retrievable;

- vetting your employees to ensure they are fit and proper to engage in AML/CTF related duties. FASU's expectation is you will establish a system to manage an employee who is found not to be fit and proper; and

- providing relevant and appropriate AML/CTF training to your employees on an initial and ongoing basis.

Your AML/CTF program must be consistent with any regulations, AML/CTF compliance rules and applicable guidance, forms or other directions issued by FASU and your regulatory authority. This risk-based framework will ensure you target your resources most effectively, and apply measures commensurate with the risks you identified.

> *i*
>
> The *Anti-Money Laundering and Counter Terrorist Financing Compliance (AML/CTF program) Rule 2018 (No. 1)* sets out how you can comply with the fit and proper criteria, and training requirements, in Section 7.
>
> In addition, the AML/CTF compliance rule sets out how to address any deficiencies identified in the effectiveness of your risk assessment and AML/CTF program, as required by Section 9.

Your AML/CTF program must be **approved** by senior management and the Board of your organisation. **Approve** means authorised and endorsed by senior management and the Board. This may be demonstrated by senior management's signature, stamp or email, or minutes of a meeting or conversation, or by other means.

FASU expects you keep a record of the senior management's approval of the AML/CTF program in writing, which incudes it being stored electronically. FASU expects you can retrieve the AML/CTF program and a record of its approval by senior management upon request.

Senior management and the Board must maintain an ongoing awareness of the risk assessment and AML/CTF program to ensure they are current.

Group-wide AML/CTF programs

A financial group must have a **group wide AML/CTF program**. A financial group is made up of a parent company that exercises control and co-ordinating functions over the rest of the group, and includes foreign branches and majority-owned subsidiaries (Section 5). A group wide AML/CTF program must:

- be applicable and appropriate to all foreign branches and majority-owned subsidiaries of the financial group;

- cover the AML/CTF program components described above;

- include policies and procedures for sharing information among the group, which includes providing customer account and transaction information; and

- have adequate safeguards on the confidentiality and use of information exchange.

Appendix B provides a sample AML/CTF program.

AML/CTF compliance officer

You must appoint an AML/CTF compliance officer who has qualifications and experience necessary for that position. The compliance officer will be someone who has a detailed background knowledge of AML/CTF laws and regulations and fit and proper criteria issued by FASU or your regulatory authority. The compliance officer must have high ethical and moral principles. This officer may be an employee of, or external to, your financial institution.

The compliance officer will be responsible for the administration and management of AML/CTF programs. To effectively administer these roles, the compliance officer must have direct access to the senior management of your institution without any restrictions.

You may appoint more than one compliance officer.

Review and audit of risk assessments and AML/CTF programs

You must review your risk assessment and AML/CTF program on a regular basis. This is to ensure any new or emerging risks are identified, and to address any deficiencies that might have arisen through your risk assessment and AML/CTF program.

FASU expects you to keep a written record of how you maintain and update your risk assessment and AML/CTF program. This will assist you in demonstrating to FASU, your regulatory authority and any external auditors the steps taken to ensure these documents remain current.

You must engage an external auditor to assess the effectiveness of your risk assessment and AML/CTF program on a periodical basis. How often you need to review your risk assessment and AML/CTF program, and engage an external auditor, will depend on the risks faced by your institution.

Appointment of an external auditor to conduct independent audit

FASU may, by way of a written notice, require you to engage an external auditor. The written notice will specify the matters to be covered by the audit, the form of the audit report, and the timeframe to provide the audit report to FASU.

FASU will prescribe a list of suitable auditors. You must select an auditor from the prescribed list, unless FASU appoints another auditor outside of the list.

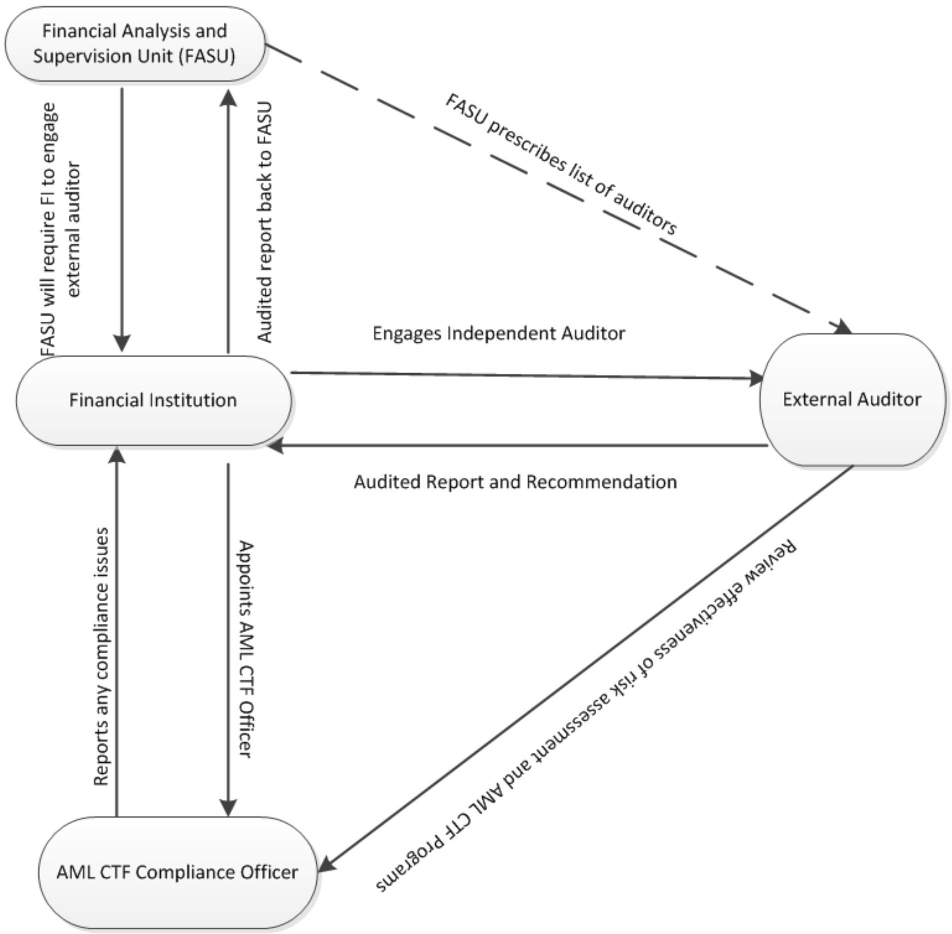
The external auditor will conduct an independent audit of your risk assessment and AML/CTF program. This will ensure your risk assessment and AML/CTF program are current, and will identify any deficiencies in the effective application of your risk assessment and AML/CTF program.

You must provide a copy of the auditor's report, together with any recommendations made by the auditor to FASU. You must consider the recommendations to improve your risk assessment and AML/CTF program.

The external auditor has the liberty to consider prior auditing reports completed within the last preceding two years or if satisfied the report is still relevant.

You must pay all costs incurred in engaging the external auditor including costs that you will incur in implementing the recommendations.

Role of AML/CTF compliance officer and external auditor



> ❗ **Failure to comply with the risk assessment, AML/CTF program, AML/CTF compliance officer, and review and audit of the risk assessment and AML/CTF program requirements is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 14).**
>
> **Failure to comply with the appointment of the external auditor requirements is a crime punishable by fines up to K100,000 for an individual and K200,000 for a body corporate (Section 14).**

8 Due diligence

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);
- Subdivision 2 – Customer due diligence requirements (Sections 20 to 29);
- Subdivision 3 – Customer due diligence requirements for electronic funds transfers (Sections 30 to 33);
- Subdivision 4 – Due diligence requirements for correspondent banking relationships (Sections 34 to 35); and
- Subdivision 5 – Offences (Sections 36 to 38).

Overview

i

Key terms defined in Section 5 which you need to understand are:

Asset, bearer negotiable instrument, currency and **transaction;**

Beneficial owner, **customer**, **business relationship** and **occasional transaction;**

Correspondent banking relationship and **shell bank;**

Domestic electronic funds transfer and **international electronic funds transfer;**

Person and **unincorporated entity**; and

Politically exposed person.

One of the core obligations in the Act is that you must conduct **customer due diligence.** This is the process by which you satisfy yourself that your customers are who they purport to be, and that their financial transactions are legitimate. It is also the process by which you determine that another financial institution is legitimate and is not, for example, a shell bank. In essence, this means you must undertake a process of **asking questions and gathering information** about your customer or another financial institution. This will enable you to identify the appropriate measures to apply in response to the information you have obtained.

The purpose of customer due diligence includes ensuring that:

- you do not open or maintain an account in an anonymous or fictitious name;
- you have accurately categorised a person or entity with whom you have a business relationship, or for whom you conduct a transaction, as a low, medium or high risk; and
- you maintain an appropriate level of ongoing monitoring of such persons or entities.

You may rely on an intermediary or third party financial institution or DNFBP to conduct customer due diligence in certain circumstances for ensuring compliance with the Act. These circumstances are set out in Section 18 of the Act. However, you have ultimate responsibility for ensuring compliance with the requirements of the Act.

Identifying and assessing risk

In order to effectively apply the customer due diligence measures, you must first identify and assess the nature and level of risk you can reasonably expect to face in the course of your business. You must base this on your assessment and AML/CTF program, and will include categorising persons or entities as a low, medium or high risk. The following is intended as guidance in terms of how you categorise persons or entities with whom who have a business relationship, or for whom you conduct a transaction:

- **Low risk persons or entities** – these are generally individuals and entities whose identities and sources of wealth can be easily identified, and whose transactions conform to their customer profile. For example, salaried employees and persons with low value credit card accounts.
- **Medium risk persons or entities** – these are generally individuals and entities whose business activities may involve varying factors around the person or entity's including:
    - customer profile, background, country of origin;
    - sources of wealth and funds;
    - nature and location of activity and
    - Substantial dealings with government agencies or departments.
- **High risk persons or entities** – these are generally individuals and entities that engage in the following activities:
    - money changers, bullion dealers, money transfer agencies, payday lenders;
    - jewellery or gold dealers;
    - gaming establishments, nightclubs, bars;
    - non-resident customers;
    - high net worth individuals;
    - trusts, charities, non-government organisations including those receiving donations;
    - companies having close family shareholding or beneficial ownership;
    - politically exposed persons;
    - law firms, real estate agents and other entities that operate trust accounts through which clients' funds may be moved anonymously; and

    - known criminals or those with dubious reputation as per public information available or individuals who are known to have been exited by other financial institutions, etc.

Persons and entities subject to customer due diligence

Further to Section 20, you must conduct customer due diligence on:

- a **customer**. A 'customer' includes a person or unincorporated entity for whom you carry out a transaction, or with whom you conduct a business relationship. In addition, a 'customer' includes a person or unincorporated entity who *attempts* to carry out a transaction or business relationship with you.

- any **beneficial owner** of a customer. A 'beneficial owner' means a natural person who has ultimate **control** of a customer (whether directly or indirectly), *or* a natural person who ultimately **owns** the customer (whether directly or indirectly).

    - '**Control**' includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. This includes exercising control through the capacity to make decisions about financial and operating policies.

    - '**Owns**' means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.

- any **person or unincorporated entity** acting on behalf of a customer. A **person** means a natural person and a body corporate. An '**unincorporated entity'** includes any unincorporated group, undertaking, organisation or legal arrangement such as a trust or an unincorporated partnership.

- a **beneficiary of an insurance policy**.

> *i* For ease to the reader, a customer, beneficial owner of a customer, person acting on behalf of a customer, and a beneficiary of an insurance policy are referred to as a '**person or entity**' in this Guidance.

Types of customer due diligence

> *i*
>
> The circumstances in which **simplified customer due diligence** can be conducted, and the requirements to obtain and verify identity information, are set out in Sections 21 and 22.
>
> The circumstances in which **standard customer due diligence** can be conducted, and the requirements to obtain and verify identify information, are set out in Sections 23 to 25.
>
> The circumstances in which **enhanced due diligence** can be conducted, and the requirements to obtain and verify identity information, are set out in Sections 26 to 29.
>
> All types of customer due diligence must be conducted on a person or entity, as required by Section 20.

Depending on the type of and risk attaching to the person or entity on whose behalf you are acting, the nature or circumstances of the transaction, and the level of risk involved, there are different types of customer due diligence that may apply. These are:

- simplified customer due diligence;
- standard customer due diligence; or
- enhanced customer due diligence.

Simplified customer due diligence

In the interests of implementing PNG's AML/CTF regime in a pragmatic manner, the Act allows you to apply simplified customer due diligence before you conduct a transaction for a person or entity. Importantly, you can only apply simplified customer due diligence if standard and enhanced due diligence are not required, the customer is **low risk** and is not resident in a high risk country, and you do not suspect money laundering or terrorist financing.

If you are permitted to apply simplified due diligence, you must obtain the following information to identify a person or entity:

- for a natural person – the person's full name and address;
- for a body corporate – its corporate name, address of the registered office, proof of incorporation, identities of directors, provisions governing the authority to bind the body corporate and such information as is necessary to understand the ownership and control of the body corporate;
- for an unincorporated entity – the name of the trustees, settlor and beneficiaries of any trusts or persons in equivalent or similar positions, and any other parties with authority to manage, vary or otherwise control the entity; and
- for a person who is not the customer – the person's relationship to the customer.

In addition, you must **verify the identity** of the person or entity on the basis of reliable and independent source documents, data or information. You must be satisfied that the information you have obtained is correct.

Standard customer due diligence

> *i* In most instances, the starting point will be to conduct standard customer due diligence on a person or entity. This will often involve conducting due diligence on a person or entity who is classified as **medium risk**.

You must conduct standard customer due diligence on a person or entity when:

- you establish a business relationship, including when opening an account or establishing an insurance policy;
- carrying out an occasional transaction of an amount equal to or greater than K20,000, whether conducted as a single transaction or by way of several transactions that appear to be linked;
- you doubt the adequacy or veracity of the documents, data or information previously obtained; or
- you form a suspicion of money laundering or terrorist financing.

To **establish** the person or entity's **identity** in accordance with standard customer due diligence requirements, you must obtain the following information:

- for a natural person – the person's full name, address, date of birth, place of birth, occupation and sufficient information to understand the purpose and nature of the intended business relationship, and such other information as is necessary to establish identity;
- for a body corporate – its corporate name, address of the registered office, proof of incorporation, identities of directors, provisions governing the authority to bind the body corporate and sufficient information to understand the nature and business of the body corporate and such other information as is necessary to understand the ownership and control of the body corporate;
- for an unincorporated entity – the name of trustees, the settlor and the beneficiary of any trusts, or persons in equivalent or similar positions and any other parties with authority to manage, vary or otherwise control the entity including sufficient information to understand the nature and business of the unincorporated entity; and
- for a person who is not the customer – the person's relationship to the customer.

In addition, you must **verify the identity** of the person or entity on the basis of reliable and independent source documents, data or information. You must take reasonable steps:

- to be satisfied that the information you have obtained is correct;
- to verify any beneficial owner's identity, so that you are satisfied that you know who the beneficial owner; and
- to verify that a person is authorised to act on behalf of the customer.

!

You must verify the identity of a person or unincorporated entity *before* you:

- **establish a business relationship;**
- **carry out an occasional transaction; or**
- **make a payment to a beneficiary pursuant to an insurance policy**

unless

- **the risk of money laundering or terrorist financing is not high and is effectively managed by you; and**
- **a delay in verification is essential in order not to interrupt your regular conduct of business.**

In such a case, you must verify the identity of a person or unincorporated entity as soon as practicable after the establishment of a business relationship (Section 25).

Enhanced customer due diligence

i

If enhanced customer due diligence is required, you must do this *in addition* to conducting standard due diligence. This will usually involve conducting due diligence on a person or entity who is classified as **high risk**.

To assist in preventing against the risk of money laundering and terrorist financing, you must conduct enhanced customer due diligence when:

- you take the view that a customer is a resident in a high risk country;
- you take the view that a customer is involved in a high risk business activity;
- you take the view that a customer is a politically exposed person;
- you take the view that a customer or a beneficiary of an insurance policy is a high risk;
- you take the view that the risk of money laundering or terrorist financing is high; or
- the customer is not physically present for the purposes of identification.

To **establish** the person or entity's **identity** in accordance with enhanced customer due diligence requirements, you must:

- obtain the identity information required for standard customer due diligence;
- obtain information relating to the source of the assets or the wealth of the customer; and
- where the beneficiary of an insurance policy is a body corporate or an unincorporated entity, take steps to identify the beneficial owner of the beneficiary.

In addition, you must **verify the identity** of the person or entity on the basis of reliable and independent source documents, data or information. You must:

- conduct the verification of identity requirements for standard customer due diligence;
- take reasonable steps to verify information relating to the source of the assets or the wealth of the customer;
- where the beneficiary of an insurance policy is a body corporate or an unincorporated entity, take steps to verify the identity of the beneficial owner of the beneficiary;
- verify any beneficial owner's identity, so that you are satisfied that you know who the beneficial owner is; and
- verify that a person is authorised to act on behalf of the customer.

!

You must verify the identity of a person or unincorporated entity *before* you:

- **establish a new business relationship;**
- **carry out an occasional transaction of K20,000 or more, in any currency; or**
- **make a payment to a beneficiary pursuant to an insurance policy**

unless

- **the risk of money laundering or terrorist financing is not high and is effectively managed by you; and**
- **a delay in verification is essential in order not to interrupt your normal conduct of business.**

In such a case, you must verify the identity of a person or unincorporated entity as soon as practicable after the establishment of a business relationship (Section 28).

Enhanced customer due diligence for politically exposed persons

> *i*
>
> A 'politically exposed person' is defined in Section 5(1). It means:
>
> - a person who is or has been entrusted in a foreign country with prominent public functions, including but not limited to, a Head of State of the head of a government, a senior politician, a senior government official, a senior judicial official or a senior military official;
> - a person who is or has been a senior executive in a foreign country of a state-owned company of that foreign country;
> - a person who is or who has been a senior political party official in a foreign country;
> - a person who is or has been entrusted with a prominent function by an international organisation, including but not limited to directors, deputy directors and members of the board or equivalent positions;
> - a person who is or has been entrusted in Papua New Guinea with prominent public functions, including but not limited to a Head of State, a politician, a senior political party official, a senior government official, a senior judicial official, a senior military official or any person who is or has been a senior executive of a State-owned company; or
> - any person who is a family member of close associate of a person mentioned above.

You must take reasonable steps to identify whether a person or entity is a **politically exposed person**.

Where you take the view that a **customer or beneficial owner** with whom you are establishing a business relationship, or you have established a business relationship, is a politically exposed person, you must:

- obtain the approval of senior management to commence or continue the business relationship with the customer or the beneficial owner; and
- conduct ongoing enhanced customer due diligence of the business relationship.

Where you take the view that a **beneficiary of an insurance policy** or **beneficial owner of the beneficiary is a politically exposed person**, and the **nature and level of risk is high**, you must, before making a payment to the beneficiary under the insurance policy:

- obtain the approval of senior management to make the payment;
- conduct enhanced due diligence of the business relationship relating to the insurance policy; and
- consider making a suspicious matter report to FASU. See ***Appendix F.***

When customer due diligence cannot be completed, or must be ceased

> *i* Details on what you must do if customer due diligence cannot be completed, or when you must cease customer due diligence, are set out in Section 19.

To help prevent the commission of money laundering or terrorist financing, you must take certain action if you are **unable to complete customer due diligence**, namely:

- you must not establish a business relationship with the new customer;
- you must terminate any existing business relationship with the customer;
- you must not carry out an occasional transaction with or for the customer;
- you must consider whether to make a suspicious matter report; and
- you may communicate to FASU any suspicions you have prior to making a suspicious matter report.

> **!** **Where you form a suspicion of money laundering or terrorist financing, and you have reasonable grounds to believe that performing customer due diligence will "tip-off" the customer, you:**
>
> - **must cease conducting customer due diligence;**
> - **must not establish a business relationship or terminate an existing relationship;**
> - **must not carry out an occasional transaction; and**
> - **you must file a suspicious matter report with FASU (Section 19).**

Ongoing Due Diligence

> *i* Details on the obligation to conduct ongoing due diligence are set out in Section 17.

To adequately guard against money laundering and terrorist financing, the Act requires that you conduct on-going due diligence on all your business relationships, particularly high risk customers. At a minimum, you must do the following:

- maintain current and up-to-date information and records relating to your customers and their beneficial owners;

- ensure that transactions carried out on behalf of your customers are consistent with your knowledge of the customer, the customer's commercial or personal activities and risk profile, and where necessary, the source of the funds;

- ensure that ongoing enhanced due diligence is conducted with respect to politically exposed persons; and

- ensure that ongoing due diligence is conducted with respect to correspondent banking relationships.

Customer due diligence on electronic funds transfers

> *i*
>
> The Act sets out the obligations to conduct customer due diligence in relation to electronic funds transfers, including international electronic funds transfers, in Sections 30 to 33.
>
> In addition, Section 19 sets out what you must do if you are unable to comply with the customer due diligence requirements in relation to electronic funds transfers.

An **electronic funds transfer** is defined in the Act as a transaction carried out on behalf of a person (the **sender**) through a financial institution, by electronic means, with a view to making an amount of money available to a person (the **receiver**, who may also be the sender) at another financial institution. It excludes transfers and settlements between financial institutions if both the sender and the receiver are financial institutions acting on their own behalf. It also excludes credit and debit card transactions if the credit or debit card number accompanies the transaction. An electronic funds transfer can be carried out by money or value transfer service providers (if they fall within the definition of 'financial institution' under the Act) if they transfer currency by electronic means to another money or value transfer service provider.

Electronic funds transfers are regarded as high risk. For this reason, you must conduct enhanced customer due diligence when acting as an ordering, intermediary or beneficiary financial institution in relation to an electronic funds transfer of K2,500 or more, in any currency. In addition, more stringent requirements apply to international electronic funds transfers.

Your obligations are set out below.

If you receive a request to execute an electronic funds transfer of K2,500 or more, in any currency, from a **'sender'** such as a natural person or a company, you are classified as an '**ordering financial institution**' under the Act. When you receive such a request you must:

- identify the sender by obtaining:
    - the sender's full name;
    - the sender's account number, or such other identifying information that allows the transaction to be traced back to the sender; and
    - the sender's address, customer identification number, or place and date of birth.
- if the request relates to an international electronic funds transfer, identify the receiver of the electronic funds transfer by obtaining:
    - the receiver's full name; and

- the receiver's account number or other identifying information that allows the transaction to be traced back to the receiver;

- verify the sender's identity before carrying out the electronic funds transfer;
- transmit with the electronic funds transfer the identity information about the sender you have obtained and verified; and
- in the case of an international electronic funds transfer, transmit with the electronic funds transfer the identify information about the receiver you have obtained.

!	**As an ordering financial institution, you must not carry out an electronic funds transfer if it is not transmitted with the required identify information (Section 19(1) (d)).**

If you receive a request to act as an **intermediary financial institution** in a chain of electronic funds transfers of K2,500 or more, in any currency, you must transmit *all* of the identity information that you receive from the ordering financial institution with the electronic funds transfer.

!	**As an intermediary financial institution, if you do not receive all of the identify information required to accompany an electronic funds transfer, you must, based on the nature and level of risk, assess whether to carry out, reject or suspend that electronic funds transfer (Section 19(1)(e)).**

If you receive a request from another financial institution to receive an electronic funds transfer of K2,500 or more, in any currency, on behalf of a receiver, you are classified as a **beneficiary financial institution** under the Act. When you receive such a request you must:

- verify the receiver's identity, so that you are satisfied that the information obtained by the ordering financial institution is correct; and
- ensure you receive all of the necessary identity information required to accompany an electronic funds transfer from an ordering financial institution or from an intermediary financial institution.

!	**As a beneficiary financial institution, if you do not receive all of the information required to accompany an electronic funds transfer, you must, based on the nature and level of risk, assess whether to carry out, reject or suspend that electronic funds transfer (Section 19(1)(f)).**

Due diligence on correspondent banking relationships and prohibitions against shell banks

> *i*
>
> The Act sets out the due diligence obligations in relation to correspondent banking relationships in Sections 34 and 35.
>
> The prohibition against establishing or continuing a business relationship with a shell bank is set out in Section 38.

Another situation where enhanced due diligence must be conducted is that involving correspondent banking relationships, as these are considered to involve higher risks of money laundering and terrorist financing. A correspondent banking relationship involves the provision of banking business services by one financial institution (**correspondent**) to another (**respondent**) where:

- the correspondent carries on banking business at or through a permanent place of business in one country;
- the respondent carries on banking business at or through a permanent place of business in another country; and
- the relationship between the correspondent and respondent relates, in whole or in part, to the provision of banking services between those permanent places of business.

You must undertake the following due diligence *prior* to entering into a correspondent banking relationship with another financial institution:

- identify and verify the identity of the respondent financial institution;
- take steps to understand the nature of the respondent's business activities;
- determine from publicly available information the reputation of the respondent, including whether the respondent has been subject to a money laundering or terrorist financing investigation or regulatory action;
- assess the respondent's AML/CTF controls to ascertain that those controls are adequate and effective;
- obtain approval from senior management before establishing a new correspondent banking relationship;
- establish an agreement which sets out the respective responsibilities of each party under the correspondent banking relationship; and
- in the case of a payable-through account, ensure that the respondent has verified its own customer's identity, has implemented mechanisms for ongoing CDD with respect to its customers and is capable of providing relevant identification information on request.

You must conduct ongoing due diligence of a respondent financial institution.

!	**If you cannot conduct the required due diligence, you must not establish a correspondent business relationship (Section 35).**

You are also prohibited from entering into, or continuing, a correspondent banking relationship with a shell bank. A shell bank is defined under the Act as a corporation that:

- is incorporated in a foreign country;
- is authorised to carry on banking business in its country of incorporation;
- does not have a physical presence in its country of incorporation; and
- is not affiliated with another corporation that:
  - is incorporated in a particular country;
  - is authorised to carry on banking business in its country of incorporation;
  - is sufficiently supervised and monitored in carrying on its banking business; and
  - has a physical presence in its country of incorporation.

!	**Failure to comply with the due diligence requirements in relation to correspondent banking relationships, or establishing or continuing a business relationship involving a shell bank, is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Sections 36 and 38).**

9 Reporting obligations

The Act sets out the reporting obligations in Part II, Division 3 (Sections 39 to 46).

Specifically:

- Subdivision 1 – Reporting obligations and offences (Sections 39 to 45); and
- Subdivision 2 – Other offences (Section 46).

If your customer, or someone acting on their behalf, conducts certain transactions or acts suspiciously, you must report these to FASU within a specified timeframe.

You are also required to report assets you hold of persons or entities who are designated under the *United Nations Financial Sanctions Act* 2015 within a specified timeframe.

Refer to the:

Threshold Transaction Report (TTR) ***Appendix C***

International Electronic Funds Transfer Report (IEFTR) ***Appendix D***

Assets of Designated Persons or Entities (ADPER) ***Appendix E***

Suspicious Matter Report (SMR) ***Appendix F***

When submitting any of the report to FASU, you should email to iReports@bankpng.gov.pg with an encrypted password.

Alternatively, either the hard copies or soft copies stored in flash drives or CDs can be hand delivered to FASU in a sealed envelope bearing the appropriate security markings and addressed to the Director of FASU.

Certain activities or transactions may be more likely to be the result of money laundering or terrorist financing, or certain information may give rise to an actual suspicion of money laundering or terrorist financing. You must report these circumstances to FASU. Because there may be limited opportunity to obtain information after the occurrence of an event, or to prevent the commission of a money laundering or terrorist financing offence, you must make the relevant report within the strict timeframes set out in the Act.

You must report the following matters:

- You must report **any transaction** involving a large sum of **cash** or cash equivalent in the form of a bearer negotiable instrument that is **K20,000** or more, even if it is not suspicious. A transaction may be carried out as a single transaction, or two or more transactions that appear to be linked. The link between the two transactions can be identified in various ways. For example, an individual may carry out a number of transactions from the one account on the same day, or a number of customers may carry out transactions from the same account on the same day;

- You must submit a Threshold Transaction Report (TTR) to FASU as soon as reasonably practicable, and no later than 10 working days from the date of the transaction(s). Refer to ***Appendix C*** for a copy of the TTR;

- You must report **any international electronic funds** transfer that is **K20,000** or more, even if it is not a suspicious transfer. You must submit an International Electronic Funds Transfer Report (IEFTR) to FASU as soon as reasonably practicable, and no later than 10 working days from the date of the transfer. Refer to ***Appendix D*** for a copy of the IEFTR;

- You must report any **assets of a designated person or entity** which you hold as soon as reasonably practicable, and no later than 10 working days from receiving notification of a designation under the *United Nations Financial Sanctions Act* 2015. You must submit an Asset of a Designated Person or Entity Report (ADPER) to FASU. You can contact FASU for information on the list of designated persons or entities. Refer to ***Appendix E*** for a copy of the ADPER; and

- You must report a **suspicious matter** if you have reasonable grounds to suspect that information known to you may be relevant to the detection, investigation or prosecution of a person for:

  - money laundering or terrorist financing;
  - dealing with an asset that is owned, controlled or held, directly or indirectly, by or on behalf of, or at the direction of, a designated person or entity. This is prohibited under Section 14 of the *United Nations Financial Sanctions Act* 2015;
  - making assets available to a designated person or entity. which is prohibited under Section 15 of the *United Nations Financial Sanctions Act* 2015;
  - any other indictable offence; or
  - a foreign indictable offence.

  You must also report information that concerns criminal property.

  You must submit a Suspicious Matter Report (SMR) to FASU within 5 working days from the date the suspicion first arose. You can also communicate your suspicions to FASU prior to making a report. Refer to ***Appendix F*** for a copy of the SMR.

Refer to ***Appendix G*** for examples of common indicators and circumstances that may raise a suspicion. A suspicion can be based on information obtained before the Act was introduced in 2015.

Once an SMR is submitted, or a suspicion is disclosed or reported to FASU, you must not disclose this to anyone else, except if the disclosure is to:

- a policeman for any law enforcement purpose;
- an officer or employee or agent of your institution, for any purpose connected with the performance of that person's AML/CTF duties; or
- a lawyer for the purpose of obtaining legal advice or a representation in relation to the matter.

!

Failure to comply with the reporting obligations is a crime punishable by up to 5 years imprisonment and fines of K500,000 for an individual and K1,000,000 for a body corporate (Sections 39 to 41).

Providing false or misleading information in a report is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 42).

Disclosing a report, information or suspicion is a crime punishable by up to 5 years imprisonment and fines of K500,000 for an individual and K1,000,000 for a body corporate (Sections 43 and 44).

10 Record keeping

i The Act sets out the record keeping obligations in Part II, Division 4 (Sections 47 to 51).

Record keeping obligations are important to ensure that in prosecutions involving money laundering and terrorist financing, evidence of a particular transaction or business can readily be made available. Such records are also important to demonstrate that you are complying with your obligations, and FASU has the power to seek production of records under the Act for supervision and enforcement purposes.

You must keep the following records:

- records to enable every **transaction** to be readily reconstructed at any time;
- records to enable the nature of the evidence used to **identity** a person or unincorporated entity; and
- records to enable the nature of the evidence used to **verify the identity** of a person or unincorporated entity.

You must keep these records for at least seven years after the completion of a transaction or business relationship.

You must also keep other records relating to risk assessments, AML/CTF programs and audits, including customer records such as account files or business correspondences relating to the establishment and duration of the business relationship with the customer. You must retain these records for at least seven years.

You must retain customer records, such as account files or business correspondence obtained during the establishment and throughout the course of the business relationship, for at least seven years after the end of the business relationship.

! **Failure to comply with the record-keeping obligations is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 51).**

11 Foreign branches and majority-owned subsidiaries

i The Act sets out the obligations in relation to foreign branches and majority-owned subsidiaries in Part IV (Section 54 and 55).

You must ensure all of your foreign branches and majority-owned foreign subsidiaries located outside PNG apply measures broadly equivalent to those set under the Act, to the extent permitted by the law of the foreign country. Where foreign measures applied are not equivalent to those set under the Act, **you must inform FASU**. You must take additional measures as are permitted by the laws of the foreign country to apply measures broadly equivalent to those set under the Act.

! **Failure to comply with the requirements applicable to foreign branches and majority-owned subsidiaries is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 55).**

12 Registration with FASU

i

The Act sets out the registration obligations in Part IV (Sections 57 and 58) and FASU's information gathering powers in Part VI, Division 2 (Sections 82 to 84).

Refer to the **Registration of Financial Institutions and Designated Non-Financial Business or Profession Form** ***Appendix H***

You must register the fact you are a financial institution with FASU in accordance with the 'Registration of Financial Institutions and Designated Non-Financial Business or Profession' form.

If you do not register, and FASU has reasonable grounds to believe you are a financial institution, FASU can make a written request to you to provide any information, or produce any records, relevant to determining whether you are a financial institution. You must comply with this request.

!

Failure to register as a financial institution with FASU is a crime punishable by fines of K25,000 for an individual and K50,000 for a body corporate (Section 58).

Failure to comply with a request for documents or information to demonstrate you are a financial institution is a crime punishable by fines of K250,000 for an individual and K500,000 for a body corporate (Section 84).

13 Beneficial ownership and fit and proper controls

i The Act sets out the obligations on beneficial ownership and fit and proper criteria in Part V (Sections 59 and 60).

To safeguard against criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution, Section 59 requires beneficial ownership information to be collected and shared with regulatory authorities and FASU. This includes information on the control and source of funds used to pay the capital of the financial institution.

You must provide information on the beneficial ownership and control, and the source of funds used to pay the capital, of your financial institution, to your regulatory authority. You must do this prior to applying for a licence, practising certificate, registration or other equivalent permission. Alternatively, if you already held such a licence etc. when the Act came into operation on 4 February 2016, you should have provided this information as soon as reasonably practicable after this date. If you have not done so, you must provide this information immediately.

You must inform your regulatory authority of any changes to the information on the beneficial ownership and control, and the source of funds used to pay the capital, of your financial institution. You must do this within one month from the date of change.

You should be aware that your regulatory authority is mandated under the Act to ensure that:

- it verifies and maintains up-to-date records of information provided to it on the beneficial ownership and control, and the source of funds used to pay the capital, of your financial institution, and
- it makes this information available to FASU when requested.

In addition, you should be aware that your regulatory authority and FASU are mandated under the Act to ensure that directors, chief executives, senior managers or persons in other equivalent positions in your financial institution, and beneficial owners of your financial institution, meet fit and proper criteria on an initial and on-going basis. Fit and proper criteria are those criteria set out by FASU, or the regulatory authority, in AML/CTF compliance rules, guidelines, forms or other directions as may be appropriate. In most instances, your regulatory authority will issue fit and proper criteria and ensure compliance with those criteria. FASU will issue the fit and proper criteria where your regulatory authority has not issued such criteria.

! **Failure to comply with the beneficial ownership obligations is a crime punishable by up to 5 years imprisonment and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 59).**

14 Providing information and records to FASU

i The Act sets out FASU's information gathering and monitoring powers in Part VI, Division 2 (Sections 71 to 93). You must comply with a request by FASU to provide information or records.

To ensure the effectiveness of the AML/CTF regime, FASU has a broad range of information gathering and monitoring powers.

FASU may request information and records from you to monitor and enforce compliance with the Act (Sections 81 and 82). FASU can conduct an on-site inspection of your premises and take copies of necessary records and ask you questions about records and items located on the premises (Section 86). These powers are to enable FASU to review your compliance with the obligations in the Act. Failure to comply with a legally-based request to provide information or produce records to FASU is an offence (Sections 83 and 84).

In certain cases, it may be necessary for FASU to request the RPNGC to apply for a search warrant of your premises. FASU may be named on the warrant as a person assisting the police in the execution of the warrant. A broad range of powers can be exercised under that warrant, including taking copies of documents, asking questions and seeking production of records. You must comply with a request to disclose any information or produce any record relevant to your compliance with the Act. In addition, it is an offence to obstruct an officer executing a warrant.

i For further detail on the execution of a warrant, see sections 89 to 91 and refer to:

Guidance on Supervision and Enforcement Powers of the Financial Analysis and Supervision Unit under the *Anti-Money Laundering and Terrorist Financing Act 2015* (No. 3 of 2018).

! **Failure to comply with a request by FASU to provide information and records under Section 81 or 82 is a crime punishable by up to 3 years imprisonment, and fines of K250,000 for an individual and K500,000 for a body corporate (Section 84).**

Obstructing the execution of a warrant and tampering with or destroying is a crime punishable by up to 3 years imprisonment, and fines of K250,000 for an individual and K500,000 for a body corporate (Section 92).

Failure to comply with a request by FASU to provide information and records pursuant to a warrant is a crime punishable by up to 3 years imprisonment, and fines of K250,000 for an individual and K500,000 for a body corporate (Section 93).

15 Offences and penalties

PNG's AML/CTF regime will be far more effective if you voluntarily comply with your obligations under the Act. This will assist in detecting, deterring and preventing money laundering and terrorist financing. This will contribute to strengthening the financial stability of PNG and combating AML/CTF related crimes and predicate offences.

FASU has a broad range of powers to monitor and enforce your compliance with the Act. These are designed to be facilitative in the first instance. However, failure to comply with your obligations under the Act will attract heavy penalties.

i	For further detail on FASU's powers, refer to: Guidance on Supervision and Enforcement Powers of the Financial Analysis and Supervision Unit under the *Anti-Money Laundering and Terrorist Financing Act 2015* (No. 3 of 2018).

Appendix I set out a complete list of offences and their associated penalties under the Act

16 References and contacts

Financial Analysis and Supervision Unit (FASU)

www.bankpng.gov.pg

General queries can be directed to: fasu@bankpng.gov.pg or +675 322 7147

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/wp-content/uploads/2014/08/1-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/wp-content/uploads/2016/03/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/wp-content/uploads/2016/03/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/wp-content/uploads/2014/08/No-23-of-2015-Proceeds-of-Crime-Amendment-Act-20153.pdf

PNG's *United Nations Financial Sanctions Act* 2015: https://www.bankpng.gov.pg/wp-content/uploads/2016/03/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

Appendix A: Sample risk assessment

	Low Risk	Medium Risk	High Risk
Customers	Simple customer types, mostly individuals	Mixture of customers types, with some complex companies and trusts	All customer types represented, including large numbers of highly complex companies, trusts and politically exposed person. (see FATF defined PEP list)
	Minimal involvement of agents acting for customers	Moderate involvement of agents acting for customers	Significant involvement of agents acting for customers
	Small customer base	Medium-sized customer base	Very large customer base
Use of cash	Facilitation of product/service rarely involves cash, or involves cash in small amounts	Facilitation of product/service often involves cash, or involves cash in moderate amounts	Facilitation of product/service usually involves cash, or involves cash in very large amounts
Source of funds and wealth	Source of funds/wealth can be readily established	Some difficulty in establishing the source of funds/wealth	Source of funds/wealth difficult to establish

Products and Services	Product/service does not allow a customer to remain anonymous (ownership is transparent)	Product/service allows a customer to retain some anonymity (ownership can be concealed)	Product/service allows a customer to remain anonymous (ownership is non-transparent)
	Small volume of transactions	Moderate volume of transactions	Large volume of transactions
	Movement of funds cannot occur easily and/or quickly	Movement of funds can occur relatively easily and/or quickly	Movement of funds can occur relatively easily and/or quickly
	Transfer of ownership of product cannot occur easily and/or quickly	Transfer of ownership of product can occur relatively easily and/ or quickly	Transfer of ownership of product is easy and/or quick
Delivery channel	Regular face-to-face contact, with minimal online/telephone services	Mix of face-to-face and online/ telephone services	Predominantly online/ telephone services, with minimal face-to-face contact
Foreign Jurisdiction	Very few or no overseas-based customers	Some overseas-based customers	Many overseas-based customers
	Low no transnational/organised crime rate in that jurisdiction	Moderate trans-national/organised crime in that jurisdiction	High or very high trans-national/organised crime in that jurisdiction
	Transactions rarely or never involve foreign jurisdictions	Transactions sometimes involve foreign jurisdictions, or a high-risk jurisdiction	Transactions often involve foreign jurisdictions, or high-risk jurisdictions

Operational vulnerabilities	There are very few operational factors that make the sector susceptible to criminal activity	There are some operational factors that make the sector susceptible to criminal activity	There are many operational factors that make the sector susceptible to criminal activity
AML/CTF Controls and systems	Sector is subject to all or most AML/CTF obligations	Sector is subject to partial AML/CTF obligations	Sector is not subject to AML/CTF obligations
	At a sector level, significant systems and controls have been implemented to mitigate against criminal threats	At a sector level, moderate systems and controls have been implemented to mitigate against criminal threats.	At a sector level, limited systems and controls have been implemented to mitigate against criminal threats.
Appropriate action from reporting institution	Simplified customer due diligence is sufficient.	Standard identification is required.	Enhanced due diligence required including identification and verification of source of wealth or funds along with standard identification.
	Exceptional identification cards or documents can be used to identify the customer in cases of financial exclusion	Required identification cards or documents must be used to identify the customer in cases of financial exclusion	Enhanced due diligence is required to identify customer as well as maintaining an on-going due diligence and monitoring on the customer.
	Not necessary to seek approval from Senior Management or Board before engaging in a business relationship with customer.	Must seek approval from Senior Management or Board before engaging in a business relationship with customer.	Highly necessary to seek approval from Senior Management or Board before engaging in, or terminating a business relationship with customer.

Appendix B: Sample AML/CTF program

Pursuant to the Act a financial institution must have and comply with an AML/CTF program.

The financial institution is required to design and maintain its AML/CTF program. The AML/CTF program formally documents the company's policies and procedures and applies to all representatives and customers of financial institution.

The purpose of the AML/CTF program is to identify, mitigate, and manage the risk that the financial institution may reasonably face (inadvertently or otherwise) by facilitating money laundering or terrorist financing through the provision of its designated services and set out the applicable customer identification and verification procedures for customers of the financial institution.

The AML/CTF Program is risk based and seeks to identify, mitigate and manage the possible ML/TF risks posed to the document the controls and systems to address the ML/TF risks. Any weakness in the AML/CTF Program may impact adversely on the management of the ML/TF risks identified.

In particular, the AML/CTF Program documents the risks associated with the types of customers, types of designated services, delivery methods, and foreign jurisdiction risk. Furthermore, the AML/CTF Program describes the employee due diligence procedures, employee risk awareness and a training program, procedures for independent review and FASU feedback.

ML/TF schemes can be difficult to identify and criminals can be ingenious in formulating different schemes to facilitate their money laundering or terrorist financing agendas. Accordingly, in order for the AML/CTF Program to be effective so that it accomplish its purpose of identifying, mitigating, and managing ML/TF risk, it requires regular review and if necessary amendment.

Furthermore, the AML/CTF Program allows for any significant changes in ML/TF risks, including changes to risks resulting from:

- the introduction of a designated service to the market
- the introduction of new methods of delivery of a designated service; or
- the introduction of any new or developing technology to be used for the provision of designated services.

Where such changes are proposed and they result in a change in the ML/TF risks, the financial institution will implement controls to mitigate and manage the ML/TF risks, prior to adopting new designated services, delivery methods or technologies.

The AML/CTF Program, and any addendums to it, is subject to Board oversight and approval.

Customer Identification Process

Customer identification and verification procedures (commonly referred to as “Know your Customer” or “KYC” procedures) are also risk based, having regard to the ML/TF risk relevant to the provision of the services offered by the financial institution.

Well-designed procedures will mitigate and manage the potential ML/TF risks faced by the financial institution and ensure that the company is reasonably satisfied as to the true identity of its customers.

Employee Due Diligence

The financial institution is required to implement comprehensive supervision procedures, ensuring that the identity and past history of prospective employees is verified. The company should also recognise the potential risk of staff turnover and implement procedures so that new staff members (or existing staff members promoted to greater levels of AML/CTF responsibility) are trained, monitored and subject to transactional limits. Comprehensive training in the company’s policies and procedures must be completed at various stages of employment.

AML/CTF Risk Awareness Training Programs

Employees will undergo training in AML/CTF laws and internal policy and procedures.

Employee training should be carried out under the supervision of the AML/CTF Compliance Officer and senior management. Training must occur upon commencement of employment with financial institution and thereafter ongoing training will occur periodically (at least annually).

The training program will takes into consideration the size of the company, its customer base, products and services offered and resources and will include the following:

- the AML/CTF Policy
- the AML/CTF Program

- the obligations of financial institution under the Act and Rules
- the types of ML/TF risk the financial institution might face and the possible consequences of such risks
- how to identify signs of ML/TF that arise during the course of the employee duties
- escalation procedures i.e. what to do once a ML/TF risk is identified;
- what the employee's role is in the firm's compliance efforts and how to perform them i.e. the processes and procedures relevant to each person's role
- the record keeping and record retention policy; and
- the disciplinary consequences (including civil and criminal penalties) for non-compliance with the Act and supporting Rules.

AML/CTF Compliance Officer

The AML/CTF Compliance Officer is should state his or her name and the position that he/she holds within the reporting agency.

The AML/CTF Compliance Officer's duties include ensuring that financial institution complies with its AML/CTF obligations and monitoring compliance, receiving and investigating reports of suspicious matters/activities, overseeing communication and training employees, ensuring that proper AML/CTF records are kept and reporting suspicious activity.

On-going Customer Due Diligence and Transaction Monitoring

The financial institution should establish procedures for on-going customer due diligence and implement a transaction monitoring program. It also must have procedures for identifying and reporting threshold transactions and suspicious matters as required by the AML/CTF records are kept and reporting suspicious activity.

- Customers are monitored on an on-going basis in order to identify any suspicious activity.
- Representatives review transactions, including trading and electronic fund transfers, in the context of other account activity to determine if a transaction is suspicious.
- The AML/CTF Compliance Officer is responsible for monitoring

adherence to the Act and documenting when and how this monitoring is conducted, and will report suspicious activities to the appropriate authorities.

- Exception reports will be utilised to identify possible ML/TF risks and include monitoring transaction size, location, type, number and nature of the activity.
- Employee guidelines, with examples of suspicious money laundering activity and lists of high-risk customers whose accounts may warrant further scrutiny, will be prepared.
- The AML/CTF Compliance Officer will conduct an appropriate investigation before reporting a suspicious matter.

Suspicious Matter Reporting

Staff training and awareness programs will educate representatives as to the potential indicators for forming a suspicion that a prospective or existing customer is seeking to use services offered by the company for money laundering purposes or terrorist financing, thereby triggering reporting obligations.

Suspicion is formed if a representative considers that an existing or prospective customer is attempting to use services offered by the financial institution for ML/TF purposes and **any one** of the following conditions is met:

- the representative suspects on reasonable grounds that the customer is not the person they claim to be;
- the representative suspects on reasonable grounds that the customers agent is not the person they claim to be;
- the representative suspects on reasonable grounds that information collected by the financial institution concerning the provision (or prospective provision) of services;
- the representative suspects on reasonable grounds that the provision, or prospective provision, of the services is preparatory to the commission of an offence of financing of terrorism;
- the representative suspects on reasonable grounds that information collected by financial institution concerning the provision, or prospective provision of services may be relevant to the investigation of, or prosecution of a person or entity for an offence of financing of terrorism;
- the representative suspects on reasonable grounds that the provision, or

prospective provision, of the service is preparatory to the commission of an offence of money laundering; or

- the representative suspects on reasonable grounds that information collected by financial institution concerning the provision, or prospective provision, of the service may be relevant to the investigation of, or prosecution of a person or entity for an offense of money laundering.

Threshold transaction reports

The financial institution will be committed to design and implement a robust system to detect threshold transactions covering all specified requirements.

Representatives with reporting responsibilities must be trained to prepare, lodge and retain records for threshold transaction reporting.

Independent review of the AML/CTF Program

A review of the AML/CTF Program will be undertaken annually.

The review will be undertaken either internally by a person separate from the company's AML/CTF Compliance Officer or the AML/CTF Compliance Office or by an external service provider that will be retained to conduct the review.

The purpose of the review will be to:

- assess the effectiveness of the AML/CTF Program having specific regard to the ML/TF risk faced by the financial institution;
- assess whether AML/CTF Program complies with the Act;
- assess whether AML/CTF Program has been effectively implemented; and
- assess whether the financial institution has complied with the AML/CTF Program.

The result of the review, including any report prepared, will be provided to the Board and senior management.

Record Keeping

The financial institution will retain all records relevant to its AML/CTF Program and policies including;

- the AML/CTF Program and all reviews and addendums to the same;

- this AML/CTF Policy and all reviews and addendums to the same;
- transactional records;
- customer identification and verification records;
- audits and compliance reviews;
- suspicious matter reporting;
- reports relating to transactions which exceed threshold limits set out in the law;
- senior management approvals;
- customer account/relationship records;
- annual compliance reports and other management reports;
- training and compliance monitoring reports; and
- information relating to the effectiveness of training.

Where the financial institution (or its agent or intermediary) carries out a customer identification and verification procedure with respect to a prospective customer to whom financial institution proposes to provide a designated service, it must make (and retain) a record of:

- the procedure (i.e. the checklist);
- information obtained in the course of carrying out the procedure (i.e. supporting documentation to verify the identification of the customer); and
- such other information (if any) about the procedure as is.

Records in respect of customer identification and verification are to be retained for 7 years after account closure. Records in respect of financial transactions are to be retained for 7 years after the date of the transaction.

The AML/CTF Program and addendums, together with any documentation relevant to the reason for amendment, are also to be retained for 7 years after the adoption of the AML/CTF Program and/or amendments cease to be in force.

Systems to re-assess risk

The financial institutions will review all areas of their business to identify potential ML/TF risks that may not be covered in the procedures described above.

The additional areas of ML/TF risks are in respect of new products, services, distribution channels and developing technologies. Additional procedures will be designed and will be implemented to identify, mitigate and manage potential ML/TF risk.

FASU Feedback

FASU is the AML/CTF regulator and Financial Intelligence Unit (FIU) for Papua New Guinea. FASU's role is to monitor compliance with the legislation.

FASU may provide Reporting Entities (such as a financial institution) with feedback in respect of their performance on the management of ML/TF risk. FASU also has the power to compel Reporting Entities to produce certain information.

The receipt of any notice, direction or recommendation from FASU will be immediately referred to the AML/CTF Compliance Officer. Notices from FASU may include, but not limited to the following requirements:

- to compel production of information or documents;
- to enter premises under a monitoring warrant;
- to require an external audit or AML/CTF risk assessment;
- to provide remedial direction; and
- to accept enforceable undertakings.

The AML/CTF Compliance Officer, in conjunction with other representatives, will take all necessary steps to comply with any, notices, orders, and warrants, or implement any directions issued by FASU.

In particular, the financial institution will have due regard to any feedback provided by FASU in regards to the financial institution's performance in managing its ML/TF risks. Such feedback will be incorporated into on-going monitoring programs and the AML/CTF Program will be amended (where appropriate).

The financial institution will be responsible for the implementation of any specific recommendations made by FASU to the financial institution in respect of its ML/TF risk management performance.

The financial institution will monitor FASU information sources, circulars, and guidance notes, in respect of domestic and international issues which may affect the business. This includes financial sanctions and updates to lists of terrorist groups.

Privacy

Customer information will be collected and retained in accordance with obligations under the AML CTF Act, Section 44.

Secrecy and access

The financial institution must not disclose that it has reported, or is required to report, information to FASU (suspicious matter) or formed a suspicion (pursuant to Section 94 of the Act) about the transaction or matter.

Offences

The Act makes it an offence to:

- produce false or misleading information;
- produce a false or misleading document;
- forge a document for use in an applicable customer identification procedure;
- provide or receive a designated service using a false customer name or customer anonymity;
- structure a transaction to avoid a reporting obligation under the Act'; or
- "tip off' a person with respect to a suspicious matter that is required to be reported to AUSTRAC.

Enforcement and Penalties

The Act provides for pecuniary penalties for contraventions of various provisions of the Act.

Appendix C: Threshold Transaction Report

STRICTLY CONFIDENTIAL WHEN COMPLETED

PAPUA NEW GUINEA
FINANCIAL ANALYSIS & SUPERVISION UNIT (FASU)
THRESHOLD TRANSACTION REPORT (TTR)
K20,000 OR MORE

Threshold Transaction Reporting is required under Section 39 (1) of the *Anti Money Laundering & Counter Terorrist Financing Act (AML/CTF) 2015*

For the purpose of TTR reporting, transactions to be reported include physical currency or any form of a bearer negotiable instrument such as a bill of exchange, cheque (including bank cheque and travellers cheque), promissory note, bearer bond, postal and money order equal to or greater than K20,000, whether carried out as a single transaction or two or more transactions that appear to be linked.

Section 39 (3) of the AML/CTF Act 2015 requires a Financial Institution to report to FASU a TTR as soon as reasonably practicable or 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.

Failure to report or reporting false or misleading information may result in a fine of up to K500,000 or 5 years imprisonment or both, or a fine of up to K1,000,000 for a body corporate

Contact FASU's anti-money laundering and counter terrorist financing (AML/CTF) officers if you are unsure about how to correctly fill out this form. Please complete in **INK** and **CAPITAL LETTERS**.

PART A - IDENTITY OF PERSON(S) CONDUCTING THE THRESHOLD TRANSACTION

1. Full Name (Title, Given Names and Surname)

2. Other Name (If known by any other name please specify)

3. Date of Birth

/ /
D D M M Y Y Y Y

4. Citizen of PNG? (tick a box)

☐ Yes ☐ No

5. NON PNG CITIZEN - PNG Contact Address

6. Phone Number

7. Residential Address (can not be a PO Address)

Street:
Surburb:
City:
Province:
Country:
Phone:

9. Occupation, Business or Principal Activity

10. TIN

11. How was the Identity of this Person Confirmed?

(1) ID Type:
ID Number:
Issuer:
Country of Issue:

(2) ID Type:
ID Number:
Issuer:
Country of Issue:

Other type of Identification (please speficy below)

8. Postal Address (If different to residential address)

PO Box:
Post Office:
City:
Province:
Country:
Post Code:

12. Is a Photocopy of ID Document/s Attached?

☐ Yes ☐ No

13. Is this Person a Signatory to an Account(s) Affected by this Transaction?

☐ Yes ☐ No

If more than one person involved please provide same details contained in Sections 1 - 13 for each person, where appropriate, and attach.

PART B - DETAILS OF PERSON/ORGANISATION ON WHOSE BEHALF THE TRANSACTION WAS CONDUCTED (If applicable)

14. Full Name of Person / Organisation

15. Other Name (If known by any other name please specify)

16. Date of Birth B (For individual)

__ __ / __ __ / __ __ __ __

D D M M Y Y Y Y

17. Citizen of PNG? (If Individual) (tick box)

☐ Yes ☐ No

18. NON PNG CITIZEN - PNG Contact Address

19. Phone Number

20. Residential/Business Address (can not be a PO Address)

Street:
Surburb:
City:
Province:
Country:
Phone:

21. Postal Address

PO Box:
Post Office:
City:
Province:
Country:
Post Code:

22. Occupation, Business or Principal Activity

23. Business Structure (If not individual)

☐ Sole Trader ☐ Association
☐ Partnership ☐ Charity
☐ Trust ☐ Church
☐ Company ☐ Other
☐ Government Body

Specify if other:

24. TIN or Company/Business Registration Number

25. Details of Account

(1) Account Title / Name:

(2) Financial Institution:
Institution:
Branch:
Agency:

(3) Account Number:

(4) Type of Account:

PART C - DETAILS OF TRANSACTION

26. Date of Transaction

__ __ / __ __ / __ __ __ __

D D M M Y Y Y Y

27.Type of Transaction

☐ Cash Received ☐ Cash Paid Out

28.Transaction Description (Eg. Payment for Services)

29. Types of Cash or BNI (If a Foreign Currency is Involved, Convert the Amount to PNG Kina)

PGK

Please Specify the Cash Types Involved in This Transaction

Type of Cash/BNI	Amount (PGK)
Cash (Notes & Coins)	.
Bill of Exchange	.
Cheque	.
Promissory Note	.
Bearer Bond	.
Money/Postal Order	.
Bank Draft	.

30. If a Foreign Currency Was Involved in this Transaction. Specify:

Currency Code *(e.g. AUD)*	Foreign Currency Amount *(e.g. AUD 100,000)*
	.
	.
	.
	.
	.
	.

31. If Another Financial Institution was Involved in this Transaction, Please Specify:

Name of Financial Institution:

Branch / Office / Agency:

Country:

32. Was Account(s) of OTHER Persons / Organisations Affected by this Transaction?

☐ Yes ☐ No

Details of Account(s):

(1) Account Title / Name:

Financial Institution:

Branch / Office / Agency:

Account Number:

(2) Account Title / Name:

Financial Institution:

Branch / Office / Agency:

Account Number:

33. Is Additional Information Attached to this Report? (Transaction History, Signature Card, Insurance Policy, Share Certificate, Land Title)

☐ Yes ☐ No

Please Specify:

PART D - DETAILS OF RECIPIENT PERSON/ORGANISATION

34. Full Name of Person / Organisation

35. Business Address (Physical and PO Box)

PO Box:

Country:

Phone:

36. Residential Address (Cannot be a PO Box)

Country:

Phone:

37. Occupation, Business or Principal Activity

38. Was an Account(s) Affected for the Recipient Person / Organisation?

☐ Yes ☐ No

Details of Account(s):

(1) Account Title / Name:

Financial Institution: Branch / Office / Agency:

Account Number:

(2) Account Title / Name:

Financial Institution: Branch / Office / Agency:

Account Number:

PART E - REPORTING FINANCIAL INSTITUTION

39. Type of Financial Institution (e.g. Bank, FX Dealer, Lending Company, Insurance Company, Legal Practitioner, Accountant)

40. Full Name of Financial Institution

41. Name of Branch / Office / Agency where the Transaction occurred

42. Business Address of Financial Institution (Physical and PO Box)

PO Box:

Country:

Phone:

PART F - FINANCIAL INSTITUTION STATEMENT

43. Details of Authorised Person

Given Names and Surname:

Position:

Phone:

E-Mail:

45. Financial Institutions Internal Reference Number (if applicable)

44. Signature This Statement is Made Pursuant to the Requirement of the Threshold Reporting Obligation Under Section 39(1) of the AML/CTF Act 2015

Signature of Authorised AML/CTF Officer:

Sign Here ______________________________

Date: __ __ / __ __ / __ __ __ __
D D M M Y Y Y Y

FINANCIAL ANALYSIS & SUPERVISION UNIT USE ONLY

FASU USE ONLY	
Report Number:	
Authorisation:	
Comments:	

FINANCIAL ANALYSIS & SUPERVISION UNIT - CONTACTS

Send Completed Forms To:	Staff should send completed TTR forms via internal mail to the bank or financial institution's central officer responsible for AML/CTF in Port Moresby. The central AML/CTF officer will then arrange delivery by hand to the FASU, or collection by the FASU. **Note**: Completed TTR forms should not be sent to the FASU via email or facsimile
For Assistance Please Contact:	Director, FASU Phone: 322 7200 Email: fasu@bankpng.gov.pg Website: www.bankpng.gov.pg

Appendix D: International Electronic Fund Transfer Report (IEFTR)

STRICTLY CONFIDENTIAL WHEN COMPLETED

PAPUA NEW GUINEA
FINANCIAL ANALYSIS & SUPERVISION UNIT (FASU)
INTERNATIONAL ELECTRONIC FUND TRANSFER REPORT (IEFTR)
K20,000 OR MORE

International Electronic Fund Transfer Reporting is required under Section 39 (2) of the Anti Money Laundering & Counter Terorrist Financing Act (AML/CTF) 2015

For the purpose of IEFT reporting, transactions to be reported are international electronic funds transfers in currency equal to or greater than K20,000, whether carried out as a single transaction or two or more transactions that appear to be linked.

Section 39(3) of the AML/CTF Act 2015 requires a Financial Institution to report to FASU a IEFTR as soon as reasonably practicable or within 10 working days from the date of the transaction where there is a single transaction, or from the date of the last transaction, where there are two or more transactions that appear to be linked.

Failure to report or reporting false or misleading information may result in a fine of up to K500,000 or 5 years imprisonment or both for a natural person, or a fine of up to K1,000,000 for a body corporate.

Contact your FASU anti-money laundering and counter terrorist financing (AML/CTF) officer if you are unsure about how to correctly fill out this form on 3227 200 or fasu@bankpng.gov.pg. Please complete in **INK** and **CAPITAL LETTERS**.

PART A - DETAILS OF TRANSACTION

1. Total Amount of Transaction

PGK ☐☐☐☐☐☐☐☐☐☐☐☐☐☐ . ☐☐

2. Date of Transmission/Receipt

☐☐ / ☐☐ / ☐☐☐☐
D D M M Y Y Y Y

3. Date Funds Available

☐☐ / ☐☐ / ☐☐☐☐
D D M M Y Y Y Y

4. Direction of Transmission

☐ Into PNG ☐ Out of PNG

5. Transaction Reference Number

6. Sending Institutions Details

BIC: (Where Applicable)

Name of Bank or Money Transmission Service Provider:

City / Town:

Country:

7. Receiving Institutions Details

BIC: (Where Applicable)

Name of Bank or Money Transmission Service Provider:

City / Town:

Country:

8. Please Specify the Foreign Currency Involved:

Currency Code (e.g. AUD)	Transaction Amount (e.g. 100,000)

PART B - DETAILS OF ORDERING CUSTOMER TRANSFERING THE MONEY

9. Full name of person/Organisation

10. Other name (If known by any other name please specify)

11. Date of Birth

/ /

D D M M Y Y Y Y

12. Residential Address (can not be a PO Address)

Country:

Phone:

13. Postal Address (If different to residential address)

Country:

Post Code:

14. Phone Number

15. Email

16. Occupation, Business or Principal Activity

17. Details of Account(s)

(1) Account Title / Name:

(2) Financial Institution:

Institution:

Branch:

Agency:

(3) Account Number:

(4) Type of Account:

18. Business Structure (If not individual)

- ☐ Sole Trader
- ☐ Partnership
- ☐ Trust
- ☐ Company
- ☐ Government Body
- ☐ Association
- ☐ Charity
- ☐ Church
- ☐ Other

If Other, Specify:

19. How was the identity of the ordering customer verified?

(1) ID Type:

ID Number:

Issuer:

Country of Issue:

(2) ID Type:

ID Number:

Issuer:

Country of Issue:

PART C - DETAILS OF BENEFICIARY CUSTOMER/ORGANISATION

20. Beneficiary Customer Account Details

Account Title / Name:

Account Number:

Account Type:

Branch / Office / Agency:

Financial Institution:

21. Full Name of Person Identified to Receive Payment

22. Other Name (If known by any other name please specify)

23. Date of Birth

/ /

D D M M Y Y Y Y

24. Residential Address (can not be a PO Address)

Country:

Phone:

25. Postal Address (If different to residential address)

Country:

Post Code:

26. Phone Number

27. Email

28. Occupation, Business or Principal Activity

29. Beneficiary Customer Details

Name:

Position within the Organisation:

Business or Principal Activity:

30. How was the identity of the ordering customer verified?

(1) ID Type:

ID Number:

Issuer:

Country of Issue:

(2) ID Type:

ID Number:

Issuer:

Country of Issue:

PART D - ADDITIONAL PAYMENT DETAILS

31. Details of Payment ***Swift Format Only***

32. Sender to Receiver Information ***Swift Format Only***

33. Additional Information (Include Intermediary Bank Details, Related Reference Number, Ordering and Beneficiary Institutions) **Swift Format Only**

34. Receiver's Correspondent ***Swift Format Only***

BIC:

or Name of Financial Institution:

City:

Country:

35. Sender's Correspondent ***Swift Format Only***

BIC:

or Name of Financial Institution:

City:

Country:

PART E - DETAILS OF REPORTING FINANCIAL INSTITUTION

36. Type of Financial Institution

☐ Bank

☐ Money Transmission Service Provider

37. Name of Financial Institution

38. Name of Branch / Office / Agency Where Transaction was Conducted

39. Business Address

Country:

Phone:

PART F - FINANCIAL INSTITUTION STATEMENT

40. Details of Authorised Person (Given Name and Surname)

Position:

Phone:

E-Mail:

42. Financial Institutions Internal Reference Number (if applicable)

41. Signature This Statement is Made Pursuant to the Requirement of Threshold Reporting Obligation Under Section 39 (2) of the *AML/CTF Act 2015.*

Signature of Authorised AML/CTF Officer:

Sign Here ______________________

Date: __ __ / __ __ / __ __ __ __
D D **M M** **Y Y Y Y**

FINANCIAL ANALYSIS & SUPERVISION USE ONLY

FASU USE ONLY	
Report Number:	
Authorisation:	
Comments:	

FINANCIAL ANALYSIS & SUPERVISION UNIT - CONTACTS

Send Completed Forms To:	Staff should send completed IEFTR forms via internal mail to the bank or financial institution's central officer responsible for AML/CTF in Port Moresby. The central AML/CTF officer will then arrange delivery by hand to the FASU, or collection by the FASU. **Note**: Completed IEFTR forms should not be sent to the FASU via email or facsimile
For Assistance Please Contact:	Director, FASU Phone: 322 7200 Email: fasu@bankpng.gov.pg Website: www.bankpng.gov.pg

Appendix E: Reporting Form: Assets of Designated Person or Entity (ADPER)

STRICTLY CONFIDENTIAL WHEN COMPLETED

Financial Analysis and Supervision Unit
(PNG's Financial Intelligence Unit)

Assets of a Designated Person or Entity Report (ADPER)

Reporting assets of a designated person or entity, is required under Section 40 of the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015. (AML/CTF Act)

Where a Financial Institution or Designated Non-Financial Business or Profession (DNFBP) receives notification(s) of a designation under Section 12(*e*)(*i*) of the *United Nations Financial Sanctions Act* 2015, the FI or DNFBP must report any assets belonging to the designated person or entity that it has custody of.

Section 40(1) of the AML/CTF Act requires the Financial Institution or DNFBP to report to FASU assets of a designated person or entity as soon as 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 *United Nations Financial Sanctions Act* 2015.

Failure to report or reporting false or misleading information may result in a fine of up to K500,000 or 5 years imprisonment or both for a natural person, or a fine of up to K1,000,000 for a body corporate.

Please complete in **INK** and **CAPITAL LETTERS**

PART A - DETAILS OF FINANCIAL INSTITUTION OR DNFBP

1) **Name of Financial Institution or DNFBP.**

____

____

2) **Name of Branch / Office / Agency Where asset(s) is held.**

____

____

3) **Business Address .**

Level: ______________________

Building: ______________________

Street: ______________________

City/Town: ______________________

Province: ______________________

Country: ______________________

Telephone: ______________________

4) **Postal Address.**

Post Office Box No: ______________________

Town/City: ______________________

Province: ______________________

Telephone: ______________________

Email: ______________________

PART B – NOTIFICATION OF DESIGNATED PERSON OR ENTITY

5) **Source(s) from which the Financial Institution or DNFBP named in PART A has identified the designated person or entity:**

☐ The Gazette of the Government of Papua New Guinea announced/notified by Prime Minister

☐ The United Nations Security Council or the United Nationas Security Council Committee

☐ Other source(s) (specify):

____

____

____

6) **Date notification was issued by relevant authority (ies):**

_____ / _____ / _________

7) **Full name of the designated person or entity published**

____

____

PART C - DETAILS OF ASSET CUSTODY ARRANGEMENT

8) **Full name of designated person or entity to whom the Financial Institution or DNFBP named in Part A has custody over its assets (e.g.. by direct or indirect ownership or control)**

9) **Type of business relationship the person named in (8) has with the Financial Institution or DNFBP named in Part A**

10) **Location where arrangement was legalised**

11) **Date the custody arrangement was legalised**

12) **Period of asset to be in custody**

From:

To:

PART D - DETAILS OF IDENTIFIED ASSET OWNED BY DESIGNATED PERSON OR ENTITY

13) **Type of asset. E.g. a house, motor vehicle, trust account, proxy/agent**

14) **Details of Asset**

Name:

Street:

Suburb:

City:

Province:

Country:

Home/Vehicle Owner:

Registration no:

Bank account name:

Bank account no:

Other details:

Asset value @ reporting date: PGK

PART E - FINANCIAL INSTITUTION STATEMENT

15) **This Statement is made pursuant to Section 40 of the AML/CTF Act 2015.**

☐ I declare the information given herein is true and correct to the best of my knowledge and belief

16) **Details of Authorised Person**

Given Names and Surname:

Position / Title:

Phone:

E-Mail:

Signature of Authorised Person:

Sign Here **X**

Date: ____ / ____ / ________

17)

(if applicable)

FINANCIAL ANALYSIS & SUPERVISION UNIT USE ONLY

Report Number:	
Authorisation:	
Comments:	

FINANCIAL ANALYSIS & SUPERVISION UNIT - CONTACTS

SEND COMPLETED FORMS TO:	Staff should send completed ADPER forms via internal mail to the bank or financial institution's central officer responsible for AML/CTF in Port Moresby. The central AML/CTF officer will then arrange delivery by hand to the FASU, or collection by the FASU.
	Note: Completed ADPER forms should not be sent to the FASU via email or facsimile
FOR ASSISTANCE PLEASE CONTACT:	Director, FASU Phone: 322 7200 Email: fasu@bankpng.gov.pg

Appendix F: Suspicious Matter Report (SMR)

STRICTLY CONFIDENTIAL WHEN COMPLETED

PAPUA NEW GUINEA
FINANCIAL ANALYSIS & SUPERVISION UNIT (FASU)
SUSPICIOUS MATTER REPORT (SMR)

Reporting suspicious matters is required under Section 41 of the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (AML/CTF Act).

For the purpose of SMR, suspicious matters need to be reported where the Financial Institution the Designated Non-Financial Business or Profession (DNFBP) 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; or

b. Be relevant to the detection, investigation or prosection of a person for a foreign indictable offence; or

c. Concern criminal property.

Section 41 (4) of the AML/CTF Act requires a Financial Institution and DNFBP to report to FASU a SMR as soon as reasonably practicable or within 5 working days from the date the suspicion first arose.

Failure to report or reporting false or misleading information may result in a fine of up to K500,000 or 5 years imprisonment or both for a natural person, or a fine of up to K1,000,000 for a body corporate.

Contact FASU's anti-money laundering and counter terrorist financing (AML/CTF) officers if you are unsure about how to correctly fill out this form. Please complete as many sections as possible in **INK** and **CAPITAL LETTERS**. **You don't need to complete every box - extra information can be provided later if requested.**

PART A - DESCRIPTION OF SUSPICIOUS MATTER

1. Grounds for Suspicion (Tick all appropriate boxes):

- ☐ Customer is evasive or nervous when asked about accounts or business activities
- ☐ Customer provided false or suspicious name or account details, or seems concerned about account secrecy
- ☐ Sudden, unexplained change in banking habits (eg large cash deposits)
- ☐ Customer has several accounts for no good reason, or splits large deposits among several accounts
- ☐ Large or unusual movement of funds to or from another country (eg transactions that have passed through several countries, or using multiple accounts to collect funds that are then transferred to foreign beneficiaries)
- ☐ Unusual cheque transactions (eg. depositing large business or government cheques into personal accounts, or unusual request for special clearance)
- ☐ Any other activity you think is suspicious, for example matters relating to terrorist financing or other proceed of crime(s) – please describe in the space provided below

2. Describe Why You Thought the Transaction Was Suspicious (if there is not enough space here, complete the description on a separate page and attach to this document)

PART B - TRANSACTION DETAILS

3. Transaction Completed (Tick a box)

☐ Yes ☐ No

Reference Number (If Yes)

4. Type of Transaction (eg deposit, withdrawal)

5. Date of Transaction

/ /

D D M M Y Y Y Y

6. Total Amount of Transaction (in Kina)

7. If Foreign Currency State Amount (eg USD 20,000)

8. Type of Instrument Involved (eg cheque, cash)

9. Ordering Customer (Optional)

10. Payee/Favouree/Beneficiary (Optional)

11. Account Name

12. Account Type

13. Account Number

14. Bank Name

15. Branch

16. Source of Funds (If known)

PART C - IDENTITY OF PERSON CONDUCTING TRANSACTION

17. Full Name (Given Names and Surname)

First Name

Middle Name

Last Name

17. A Sex

Male ☐

Female ☐

18. Other Name (If known by any other name, please specify)

19. Date of Birth (if known)

/ /

D D M M Y Y Y Y

24. Work or Business Address

25. Phone Number (include area code)

26. Email Address (If known)

27. Was the Identity of this Person/Corporation Verified? (tick a box)

☐ Yes ☐ No

28. If Identity Verified, Specify Type of ID

20. Country of Birth (if known)

21. PNG Citizen? (tick a box)

☐ Yes ☐ No ☐ Unknown

Country of Citizenship*(if No)*

22. Residential Address or Location in PNG (Include what information you have and PO Box)

23. Occupation, Business or Principal Activity

29. Identity Document Issued By (If applicable)

30. Identity Number

31. Is a Copy of the ID Attached? (tick a box)

☐ Yes ☐ No

31A. Tax Identification Number (TIN) (If Known)

31B. Relationaship to Person in Part D

PART D - DETAILS OF PERSON/CORPORATION ON WHOSE BEHALF THE TRANSACTION WAS CONDUCTED (Answer if applicable)

32. Full Name (Given Names and Surname)

First Name

Middle Name

Last Name

32. A Sex (if individual)

Male ☐

Female ☐

33. Other Name (If known by any other name, please specify)

34. Date of Birth (if known)

__ __ / __ __ / __ __ __ __

D D M M Y Y Y Y

35. Country of Birth (if known)

36. PNG Citizen? (tick a box)

☐ Yes ☐ No ☐ Unknown

Country of Citizenship*(if No)*

37. Residential Address or location in PNG (Include what information you have and PO Box)

38. Occupation, Business or Principal Activity

39. Work or Business Address

40. Phone Number (include area code)

40A. Tax Identification Number (TIN)

40B. Company Registration Number

PART E - DETAILS OF RECIPIENT PERSON/CORPORATION

41. Full Name (Given Names and Surname)

First Name

Middle Name

Last Name

41. A **Sex** (if individual)

Male ☐

Female ☐

42. Other Name (If known by any other name, please specify)

43. PNG Citizen? (tick a box)

☐ Yes ☐ No ☐ Unknown

Country of Citizenship *(if No)*

44. Residential Address or location in PNG (Include what information you have and PO Box)

45. Occupation, Business or Principal Activity

46. Work or Business Address

47. Phone Number (include area code)

48. Email Address

49. Account Name

50. Bank

51. Account Number

52. Branch

53. Reason for Transaction (If known, eg payment for imports)

PART F - DETAILS OF REPORTING ENTITY

54. Name of Financial Institution/Cash Dealer

55. Office or Branch Location

56. Name of Authorised AML/CTF Officer

57. Title

58. Phone Number

59. Email Address

FINANCIAL INSTITUTION STATEMENT

60. Signature This statement is made pursuant to the requirement to report suspicious matters under the laws of PNG on the grounds detailed in Section 41 of the *AML/CTF Act 2015.*

Signature of Authorised AML/CTF Officer:

Name ______________________

Sign Here ______________________

Date: __ __ / __ __ / __ __ __ __
D D M M Y Y Y Y

FINANCIAL ANALYSIS & SUPERVISION UNIT USE ONLY

FASU USE ONLY	
Report Number:	
Authorisation:	
Comments:	

FINANCIAL ANALYSIS & SUPERVISION UNIT - CONTACTS

Send Completed Forms To:	Completed SMR forms should be emailed to iReports@bankpng.gov.pg with an encrypted password. Alternatively, either hard or soft copies stored in Flashdrives or CDs can be hand delivered to FASU in a sealed enveloped bearing the appropriate security markings and addressed to the director of FASU
For Assistance Please Contact:	Director, FASU Phone: 322 7200 Email: fasu@bankpng.gov.pg Website: www.bankpng.gov.pg

Appendix G Common indicators or circumstances that may raise suspicion

1.1 General red flags pointing to money laundering

✓ Customer admits or makes statements about involvement in criminal activities.

✓ Customer attempts to develop close rapport/relationship with staff

✓ Customer offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.

✓ Customer repeatedly uses an address but frequently changes the names involved.

✓ Customer uses aliases and a variety of similar but different addresses

✓ Customer does not want correspondence sent to home address.

✓ Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account

✓ Customer is accompanied and watched.

✓ Customer insists that a transaction be done quickly

✓ Customer shows uncommon curiosity about internal systems, controls and policies.

✓ Customer has only vague knowledge of the amount of a deposit.

✓ Customer presents confusing details about the transaction.

✓ Customer over justifies or explains the transaction.

✓ Customer is secretive and reluctant to meet in person.

✓ Customer is nervous, not in keeping with the transaction.

✓ Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.

1.2 Conduct of transactions domestically

✓ You are aware that a customer is the subject of a money laundering or terrorist financing investigation.

✓ Customer is involved in activity that is inconsistent with what would be expected from declared business

✓ Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.

✓ Customer frequently exchanges small bills for large ones

✓ Customer uses notes in denominations that are unusual for the customer, when the norm in that business is much smaller or much larger denominations.

✓ Customer consistently makes cash transactions that are just under or significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.

✓ Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.

✓ Customer deposits musty or extremely dirty bills.

✓ Customer frequently purchases travellers cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the customer.

✓ Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.

✓ Stated occupation of the customer is not in keeping with the level or type of activity, or maintains a huge account balance (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

✓ Customer makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account).

✓ Customer runs large credit card balances.

✓ Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.

✓ Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount.

✓ Customer frequently exchanges currencies.

✓ Third parties make cash payments or deposit cheques to a customer's credit card.

✓ Customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

✓ Customer acquires significant assets and liquidates them quickly with no explanation.

✓ Customer acquires significant assets and encumbers them with security interests that don't make economic sense.

1.3 Knowledge of reporting or record keeping requirements
✓ Customer attempts to convince employee not to complete any documentation required for the transaction. ✓ Customer makes inquiries that would indicate a desire to avoid reporting. ✓ Customer has unusual knowledge of the law in relation to suspicious matter reporting. ✓ Customer seems very conversant/knowledgeable with money laundering or terrorist financing issues. ✓ Customer is quick to volunteer that funds are clean or not being laundered.
1.4 Identification documents
✓ Customer provides doubtful or vague identification information. ✓ Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate. ✓ Customer refuses to produce personal identification documents. ✓ Customer only submits copies of personal identification documents. ✓ Customer wants to establish identity using something other than his or her personal identification documents. ✓ Customer inordinately delays presenting corporate documents. ✓ All identification presented is foreign or cannot be checked for some reason. ✓ All identification documents presented appear new or have recent issue dates.
1.5 Nature and usage of bank accounts
✓ Opening accounts when the customer's address is outside the local service area. ✓ Opening accounts with names very close to other established business entities. ✓ Attempting to open or operating accounts under a false name. ✓ Account with a large number of small cash deposits and a small number of large cash withdrawals. ✓ Funds are being deposited into several accounts, consolidated into one and transferred outside the country.

✓ Customer frequently uses many deposit locations outside of the home branch location or multiple deposits are made to a customer's account by third parties.

✓ Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.

✓ Activity far exceeds activity projected at the time of opening of the account.

✓ Account that was reactivated from inactive or dormant status suddenly sees significant activity or suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.

✓ Unexplained transfers between the customer's products and accounts.

✓ Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

✓ Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are located in high risk areas.

✓ Customer appears to have accounts with several financial institutions in one area for no apparent reason or establishes a series of new relationships with different financial intuitions.

1.6 Transacting between high risk areas

✓ Customer and other parties to the transaction have no apparent ties to Papua New Guinea.

✓ Transaction crosses many international lines.

✓ Use of a credit card issued by a foreign bank that does not operate in Papua New Guinea, by a customer that does not live and work in the country of issue.

✓ Transactions involving countries deemed by the Financial Action Task Force as requiring enhanced surveillance.

✓ Foreign currency exchanges or deposits that are associated with subsequent wire transfers to high risk areas.

✓ Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.

✓ Transaction involves a country known for highly secretive banking and corporate law.

✓ Transaction involves a country known or suspected to facilitate money laundering activities.

1.7 Transactions related to offshore business activity

✓ Accumulation of large balances, inconsistent with the known turnover of the customers' business, and subsequent transfers to overseas account(s).

✓ Frequent requests for traveller's cheques, foreign currency drafts or other negotiable instruments.

✓ Loans secured by obligations from offshore banks.

✓ Loans to or from offshore companies. Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.

✓ Transactions involving an offshore shell bank whose name may be very similar to the name of a major legitimate institution.

✓ An unexplained electronic fund transfers by customer on an in-and-out basis.

Customer uses letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the customer's business.

✓ Use of a credit card issued by an offshore bank.

1.8 Corporate and business transactions

Some businesses may be susceptible to the mixing of illicit funds with legitimate income. This is a very common method of money laundering. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity.

✓ Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc.

✓ Accounts have a large volume of deposits in bank drafts, cashiers cheques, money orders or electronic funds transfers, which is inconsistent with the customers' business.

✓ Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.

✓ Business does not want to provide complete information regarding its activities.

✓ Financial statements of the business differ noticeably from those of similar businesses.

✓ Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them.

✓ Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations.

✓ Customer maintains a number of trustee or customer accounts that are not consistent with that type of business or not in keeping with normal industry practices.

✓ Customer operates a retail business providing cheque-cashing services but does not make large draws of cash against cheques deposited.

✓ Customer pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments.

✓ Customer purchases cashiers cheques and money orders with large amounts of cash.

✓ Customer deposits large amounts of currency wrapped in currency straps.

✓ Customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.

✓ Customer consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.

✓ Customer makes a single and substantial cash deposit composed of many large bills.

✓ Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business.

✓ There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred.

✓ Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business.

✓ Asset acquisition is accompanied by security arrangements that are not consistent with normal practice.

✓ Unexplained transactions are repeated between personal and commercial accounts.

✓ Account has close connections with other business accounts without any apparent reason for the connection.

✓ Activity suggests that transactions may offend securities regulations or the business prospectus is not within the requirements.

✓ A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from areas considered to be of high risk.

✓ Customer transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash and vice versa

✓ Customer makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.

✓ Customer receives electronic funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the client.

✓ Client instructs you to transfer funds abroad and to expect an equal incoming transfer.

✓ Client shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.

✓ Client transfers funds to another country without changing the form of currency.

✓ Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals.

✓ Customer sends frequent wire transfers to foreign countries or entities, but business does not seem to have connection to destination country or entity and vice versa.

✓ Wire transfers are received from entities having no apparent business connection with customer.

✓ Size of electronic transfers is out-of-keeping with normal business transactions for that customer.

✓ Wire transfers do not have information about the beneficial owner or originator when the inclusion of this information would be expected.

✓ Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).

✓ Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.

✓ Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics or that are known for highly secretive banking and corporate law practices.

✓ Customer makes electronic funds transfers to free trade zones that are not in line with the customers' business or from countries known to have ML or TF problems.

✓ Customer suddenly repays a problem loan unexpectedly.

✓ Customer's employment documentation lacks important details that would make it difficult for you to contact or locate the employer.

✓ Customer has loans to or from offshore companies that are outside the ordinary course of business of the customer.

✓ Customer offers you large dollar deposits or some other form of incentive in return for favourable treatment on loan request.

✓ Customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.

✓ Loan transactions are entered into in situations where the customer has significant assets and the loan transaction does not make economic sense.

✓ Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.

✓ Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the customer.

1.9 Foreign exchange dealers and money services businesses

If you are involved in the money services business, including foreign exchange dealers, money remitters, issuers of traveller's cheques and post offices, consider the following indicators.

✓ Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.

✓ Customer wants to pay transaction fees that exceed the posted fees.

✓ Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.

✓ Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.

✓ Customer wants a cheque issued in the same currency to replace the one being cashed.

✓ Customer wants cash converted to a cheque and you are not normally involved in issuing cheques.

✓ Customer wants to exchange cash for numerous postal money orders in small amounts for numerous other parties.

✓ Customer enters into transactions with counter parties in locations that are unusual for the customer.

✓ Customer instructs that funds are to be picked up by a third party on behalf of the payee.

✓ Customer makes large purchases of travellers cheques not consistent with known travel plans.

✓ Customer requests numerous cheques in small amounts and various names, which total the amount of the exchange.

✓ Customer requests that a cheque or money order be made out to the bearer.

✓ Customer requests that a large amount of foreign currency be exchanged to another foreign currency.

Appendix H: Registration of a Financial Institution or DNFBP

STRICTLY CONFIDENTIAL WHEN COMPLETED

PAPUA NEW GUINEA
FINANCIAL ANALYSIS AND SUPERVISION UNIT (FASU)
REGISTRATION OF FINANCIAL INSTITUTION AND DESIGNATED NON-FINANCIAL BUSINESS OR PROFESSION

A Financial Institution (FI) and a Designated Non-financial Business or Profession (DNFBP) is required to register with FASU under Section 57 (1) of the Anti-Money Laundering and Counter Terrorist Financing Act 2015

Failure to register with FASU may result in a fine of up to K25,000 for a natural person or a fine of up to K50,000 for a body corporate.

Contact FASU's anti-money laundering and counter terrorist financing (AML/CTF) officers on phone 322 7200 or email fasu@bankpng.gov.pg if you are unsure about how to correctly fill out this form. Please complete in **INK** and **CAPITAL LETTERS**.

PART A - REASON FOR REGISTRATION

1. Are You A
- ☐ Financial Institution
- ☐ Designated Non-financial Business or Profession

2. Reason for Registration (tick a box).
- ☐ Initial Registration
- ☐ Renewal
- ☐ Correction on previous registration
- ☐ Re-registration

3. If Filing For A Correction, Indicate FASU Registration No.

4. If Re-registering, Briefly Explain Why

PART B - DETAILS OF FI OR DNFBP

5. Name of FI or DNFBP

6. Nature of Business

7. Company/Business Registration No.

8. GST Registration No. (if applicable)

9. Business Address (Physical and PO Address)

PO Box:
Phone:
Email:
Website:
Business address of branches (if applicable)

10. Estimated Annual Income (in Kina)

PART C - DETAILS OF OWNER OR DIRECTOR(S) OR PARTNER(S)

11. Full Name

12. Residential Address

Phone:

13. Country of Citizenship

14. Work Permit No. (if applicable)

19. Full Name

20. Residential Address

Phone:

21. Country of Citizenship

22. Work Permit No. (if applicable)

15. Full Name

16. Residential Address

Phone:

17. Country of Citizenship

18. Work Permit No. (if applicable)

23. Full Name

24. Residential Address

Phone:

25. Country of Citizenship

26. Work Permit No. (if applicable)

If more than four (4) Directors or Partners please provide above details as an attachment with this Form

PART D - DETAILS OF AML/CTF COMPLIANCE OFFICER(S)

27. Full Name

28. Residential Address

Phone:

29. Country of Citizenship

30. Work Permit No. (if applicable)

31. Full Name

32. Residential Address

Phone:

33. Country of Citizenship

34. Work Permit No. (if applicable)

If more than two (2) Compliance Officers please provide above details as an attachment with this Form

PART E - DETAILS OF BENEFICIAL OWNER(S)

35. Full Name

36. Residential Address

Phone:

37. Country of Citizenship

38. Full Name

39. Residential Address

Phone:

40. Country of Citizenship

If more than two (2) Beneficial Owners please provide above details as an attachment with this Form

PART F - SIGNATURE OF AUTHORIZED PERSON

I am authorized to file this form on behalf of myself/the company/business. I confirm that the information contained above is true, correct and complete.

Given Names and Surname

Position/Title:

Phone:

Email:

Signature:

Sign Here **X**

Date: / /

D D M M Y Y Y Y

PNG FINANCIAL ANALYSIS & SUPERVISION UNIT (FASU) USE ONLY

FASU USE ONLY	
Registration Number:	
Authorisation:	
Comments:	

Appendix I: Offences and penalties under the Act 2015

Ref.	Offence	Section number	Penalty	Explanation
Part II. Obligations on financial institutions				
a.	Failure to comply with risk assessment, AML/CTF program, appointment of AML/CTF compliance officer and appointment of external auditor obligation	14 (1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under Division 1 of Part II, a Financial Institution must: Conduct a risk assessment under s6; Establish, implement and maintain an AML/CTF program under s7; Appoint an AML/CTF compliance officer to administer and maintain its AML/CTF program under s8, and Review and audit its risk assessment and AML/CTF program, including by an external auditor, under s9. It is an offence under s14 (1) for a person to intentionally fail to comply with these requirements. It is an offence under s14 (2) for a person to recklessly fail to comply with these requirements.
		14 (2)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
		14 (3)	*Natural Person*- a fine not	Under s10, FASU may by written notice require a Financial

			exceeding K100,000.00 *Body Corporate* – a fine not exceeding K200,000.00	Institution to appoint an external auditor to conduct an independent audit of its AM/CTF program. It is an offence under s14 (3) for a person to intentionally fail to comply with FASU's written notice. It is an offence under s14 (4) for a person to recklessly fail to comply with FASU's written notice.
		14 (4)	*Natural Person*- a fine not exceeding K50,000.00 *Body Corporate* – a fine not exceeding K100,000.00	
b.	Failure to comply with due diligence requirements	36(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under Division 2 of Part II, a Financial Institution must comply with a number of due diligence requirements, namely: General due diligence requirements in Subdivision 1; Simplified, standard and enhanced customer due diligence requirements in Subdivision 2; Customer due diligence requirements for electronic funds transfer in Subdivision 3, and Due diligence requirement for correspondent banking relationships in Subdivision 4. It is an offence under s36 (1) for a person to intentionally fail to comply with these due diligence requirements. It is an offence under s36 (30 for a person to recklessly fail to
		36(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	

				comply with these due diligence requirements.
c.	Opening or operating anonymous accounts and accounts in false names	37(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	It is an offence under s37 (1) for a person to intentionally open or operate an anonymous account or an account in a false name. It is an offence under s37 (3) for a person to recklessly open or operate an anonymous account or an account in a false name.
		37(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
d.	Establishing or continuing a business relationship involving a shell bank	38(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	It is an offence under s38 (1) for a person to intentionally : Establish or take steps to establish a shell bank in Papua New Guinea; Enter into or continue a business relationship with a shell bank or a correspondent financial institution in a foreign country that permits its accounts to be used by a s hell bank; or Allow an occasional transaction to be conducted through it by a shell bank or a financial institution in a foreign country that
		38(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both	

			Body Corporate – a fine not exceeding K500,000.00	permits its accounts to be used by a shell bank. It is an offence under s38 (3) for a person to recklessly do any of the above.
e.	Failure to comply with threshold reporting obligations	39(6)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under s39 (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. The transaction may be carried out a single transaction or two or more transactions that appear to be linked. Under s39(2) a financial institution must report to FASU an international electronic funds transfer of an amount in currency equal to or greater that K20,000.00. The transaction maybe carried out as single transaction or two or more transactions that appear to be linked. It is an offence under s39 (6) for a person to intentionally fail to make a report under s39 (1) or (2). It is an offence under s39 (8) for a person to recklessly fail to make a report under s39 (1) or (2).
		39(8)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
f.	Failure to report assets of a designated person or entity	40(4)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both	Under s40(1) a financial institution must 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

			Body Corporate – a fine not exceeding K1,000,000.00	designation under s13(f) of the *United Nations Financial Sanctions Act 2015*. It is an offence under s40 (4) for a person to intentionally fail to make a report. It is an offence under s40 (6) for a person to recklessly fail to make a report.
		40(6)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
g.	Failure to comply with suspicious matter reporting obligations	41(8)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under s41(4) read with s4(1), a financial institution must make a suspicious matter report to FASU as soon as is reasonably practicable, and in any event within 5 working days, from the date it has reasonable grounds to suspect that information known to it may: be relevant to the detection, investigation or prosecution of a person for money laundering, terrorist financing, an offence under s15 or 16 of the *United Nations Financial Sanctions Act 2015* or any other indictable offence; be relevant to the detection, investigation or prosecution or a person for a foreign indictable offence; or Concern criminal property. It is an offence under s41 (8) for a person to intentionally fail to make a suspicious matter report under s41 (4). It is an offence under s41 (10) for a person to recklessly fail to
		41(10)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	

				make a suspicious matter report under s41 (4).
h.	Providing false or misleading report or information	42(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	It is an offence under s42(1) for a person to furnish information which he knows to be false or misleading in any material way for the purpose of, or in connection with, making any report or providing any information required by Division 3 of Part II. It is an offence under s42(3) for a person to furnish information reckless as to whether it is false or misleading in any material way for the purpose of, or in connection with, making any report or providing any information required by Division 3 of Part II.
		42(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
i.	Obligation not to disclose a report etc.	43(4)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Section 43(1) requires that where a financial institution has made or makes a report to FASU under ss39(10, 39(2), 40(1) or 41(4), it must not disclose to anyone else: the report; that a report has been or maybe made to FASU; or any other information from which a person could reasonably infer that a report has been or maybe made to FASU. This is subject to certain exceptions listed in s43 (2) and (3).
		43(6)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not	

			exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	The above also does not apply if a financial institution is required to disclose information under the act. It is an offence under s43 (4) for a person to intentionally disclose information in contravention of s43 (1). It is an offence under s43 (6) for a person to recklessly disclose information in contravention of s43 (1).
j.	Obligation not to disclose information or suspicion	44(4)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Section 44(1) requires that where a financial institution forms a suspicion under s41(1), it must not disclose to anyone else (unless otherwise required under the Act): that it has formed the suspicion under s44(1); that a suspicion has been or may be communicated to FASU under s41(11); or any other information from which a person could reasonably infer any of the above. This is subject to certain exceptions listed in s44 (2) and (3). It is an offence under s44 (4) for a person to intentionally disclose information in contravention of s44 (1). It is an offence under s44 (6) for a person to recklessly disclose information in contravention of s44 (1).
		44(6)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
k.	Disclosure or identify in relation to	45(1)	*Natural Person*- a fine not exceeding K500,000.00 or	It is an offence under s45 (1) for a person to intentionally disclose any transaction, communication, report or

	suspicious matter reports or information		imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	information that will identify, or is likely to identify, the person who prepared or made a report or provided information under s41. It is an offence under s45 (3) for a person to recklessly disclose any transaction, communication, report or information that will identify, or is likely to identify, the person who prepared or made a report or provided information under s41.
		45(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
l.	Structuring Offence	46(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under s46(1) a person commits a crime if he: conducts two or more transactions by whatever means that are equivalent to K20,000.00 or more, and conducts the transactions for the dominant purpose of ensuring, or attempting to ensure, that no report in relation to the transactions would need to be made under s39.
m.	Failure to comply with record keeping requirements	51(1)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not	Under Division 4 of Part II, a financial institution must comply with certain record keeping requirements. These include: Keeping transaction records under s47;

			exceeding K1,000,000.00	Keeping identity and verification records under s48, and
		51(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	Keeping other records under s49 such as those relating to: a risk assessment, AML/CTF program and audit; records relevant to establishing a business relationship with a customer, and customer records such as account files and business correspondence. A financial institution is required to retain these records for a certain period of time, as set out in the Act. It is an offence under s51 (1) for a person to intentionally fail to comply with these record keeping requirements. It is an offence under s51 (3) for a person to recklessly fail to comply with these record keeping requirements.
Part III. Obligations on designated non-financial businesses and professions				
n.	Offences	53	When a DNFBP is required to comply with an obligation under Part II and fails to do so, any penalty provision applicable to a financial institution is also applicable to a DNFBP.	Further to s52, a DNFBP is required to comply with the obligations set out in Part II, as if the reference in that Part to a financial institution were a reference to a DNFBP. This is subject to two qualifications: The obligation only applies to a DNFBP in the circumstances listed in s52(1)(a)-(f), and A DNFBP is not required to comply with the due diligence requirements regarding electronic funds transfers and correspondent banking relationships.

				Further to s53, where a DNFBP is required to comply with an obligation under Part II, and the DNFBP fails to do so, any offence provision relating to the obligation that is applicable to a financial institution is also applicable to a DNFBP.
Part IV. Additional obligations applying to financial institutions and designated non-financial businesses and professions				
o	Failure to comply with requirements relating to foreign branches and majority-owned foreign subsidiaries	55(1)	*Natural Person*- a fine not exceeding K5000,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Under s54(1) and ((2) a financial institution must ensure that its foreign branches and majority owned foreign subsidiaries located outside Papua New Guinea apply to the extent permitted by the law of that foreign country, measures broadly equivalent to those set out in Part II. If it does not, a financial institution must inform FASU and take additional measures to implement those requirements. Under s54(3)a DNFBP of Papua New Guinea must ensure that its foreign branches and majority- owned foreign subsidiaries located outside Papua New Guinea apply to the extent permitted by the law of that foreign country, measures broadly equivalent to those set out in Part III. If it does not, a DNFBP must inform FASU and take additional measures to implement those requirements. It is an offence under s55(1) for a person to intentionally engage in conduct that contravenes the requirement of s54 It is an offence under s55(3) for a person to recklessly engage in conduct that contravenes the requirement of s54
		55(3)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	
p	Failure to register	58	*Natural Person*- a fine not	Under s57 a financial institution and DNFBP must register with FASU for the purpose of this Act. A person who fails to

	with FASU		exceeding K25,000.00 *Body Corporate* – a fine not exceeding K50,000.00	register with FASU is guilty of a crime under s58
Part V. Beneficial ownership information and fit and proper controls				
q	Failure of financial institutions and DNFBPs to disclose beneficial ownership information	59(4)	*Natural Person*- a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both *Body Corporate* – a fine not exceeding K1,000,000.00	Section 59(1) and (2) requires a financial institution and DNFBP to provide information to its regulatory authority on the beneficial ownership and control, and the sources of funds used to pay the capital of, the financial institution of DNFBP. This may occur either before or after the financial institution or DNFBP applies for licence, practising certificate, registration or other equivalent permission or (where the licence etc. has already been granted) upon the Act coming into operation. It is an offence under s59 (4) for a person to intentionally fail to provide this information.
		59(6)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	It is an offence under s59(6) for a person to recklessly fail to provide this information
r.	Failure to comply with a request for documents or	84(1)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not	Under its new information gathering and monitoring powers, FASU can request information and records from a financial institution or DNFBPs to monitor and enforce compliance

	information		exceeding 3 years or both *Body Corporate* – a fine not exceeding K500,000.00	with the Act (s81) or to determine if a person is a financial institution or DNFBP (S82). Further to s83, a person requested to disclose any information or produce any record must comply with that request. It is an offence under s84 (1) for a person to: Refuse to comply with a request for information or record under s81 or s82; Produce any record, or give any information, knowing it is false in any material way in response to a request under s81 or s82; With intent to evade the provisions of s81 or s82, destroys mutilates, deface, conceal or remove any record. 3It is an offence under s84 (1) for a person to: Fail to comply with a request for information or record under s81 or s82 within the specified time and manner; Produce any record, or give any information, reckless as to whether it is false in any material way in response to a request under s81 or s82;
		84(3)	*Natural Person*- a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 1 year or both *Body Corporate* – a fine not 2exceeding K200,000.00	
s.	Obstructing the execution of a warrant and tampering with or destroying records	92(1)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both	Further to Section 87 – 90, a policeman may apply for a search warrant of the premises of or used by a financial institution or DNFBP under the *Search Act 1977* in order to monitor compliance. FASU may be named as a person

			Body Corporate – a fine not 2exceeding K500,000.00	assisting the policeman in the execution of the warrant. A broad range of powers can be exercised under that warrant including taking copies of documents, asking questions and seeking production of records. It is an offence under s92 (1) for a person to intentionally prevent, hinder or obstruct the execution of a warrant, including by tampering with or destroying records.
t.	Failure to respond to questions and produce records.	93(5)	*Natural Person*- a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both *Body Corporate* – a fine not 2exceeding K500,000.00	Further to s93 (1), where an officer of FASU enters the premises of a financial institution or DNFBP pursuant to a warrant, that officer may ask the occupier questions, seek production of records and ask for an explanation of those records. A person requested to disclose any information or produce any record must comply with that request under s93 (3). It is an offense under s93 (5) for a person to: Refuse to comply with a request under s93 (1) to disclose information or produce records; Produce any record or information knowing it to be false in any material way in response to request under s93(1); or With intent to evade s93 (3), destroys, mutilates, defaces, conceals or removes any record.
		93(6)	*Natural Person*- a fine not exceeding K100, 000.00 or imprisonment for a term not exceeding 1 year or both.	

				It is an offence under s93 (6) for a person to produce any record or give any information recklessly as to whether it is false in any material way.
u.	Offence of disclosing confidential information	95 (2)	*Natural Person*- a fine not exceeding K100, 000.00 or imprisonment for a term not exceeding 1 year or both.	Further to s94, information which is supplied to or obtained by FASU under the Act is considered confidential' information. This excludes information which is factually the same as the confidential information and is already in the public domain, or which is presented so that it does not enable the identification of the particular person. An officer of FASU may not disclose confidential information, unless certain circumstances apply. It is an under s95 (2) for a person to intentionally disclose confidential information in contravention of Division 3 of Part VI. It is an offence under s95 (4) for a person to recklessly disclose confidential information in contravention of Division 3 of Part VI
		95 (4)	*Natural Person*- a fine not exceeding K50,000.00	