ARRANGEMENT OF SECTIONS

NO [ ] OF 2015
A BILL

AN ACT

Entitled
ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING ACT

TABLE OF CONTENTS

ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING ACT

Being an Act which enables the Government of Papua New Guinea to detect and deter money laundering and terrorist financing,

Made by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting with, and in accordance with, the advice of the Minister.

PART 1 – PRELIMINARY

1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS

This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III 3 C (qualified rights) of the Constitution, namely:

(a) Section 42 (liberty of the person)

(b) Section 44 (freedom from arbitrary search and entry)

(c) Section 47 (freedom of assembly and association)

(d) Section 48 (freedom of employment)

(e) Section 49 (right to privacy)

(f) Section 51 (right to freedom of information)

(g) Section 53 (protection from unjust deprivation of property)

is a law that is made for the purpose of complying with Section 38 of the Constitution, that is necessary for the purpose of giving effect to the public interest in public safety, public order and public welfare and is reasonably justifiable in a democratic society having proper respect and regard for the rights and dignity of mankind, taking into account the National Goals and Directive Principles and Basic Social Obligations, and to give effect to certain international obligations of Papua New Guinea and meet relevant Financial Action Task Force Recommendations because of the risk that money laundering and terrorist financing poses to public safety, public order and public welfare as well as to the successful economic and human development of Papua New Guinea and its citizens and to the stability of the State of Papua New Guinea.

2. ACT TO BIND THE STATE

This Act binds the State.

3. APPLICATION OF CRIMINAL CODE ACT

The *Criminal Code Act 1974* applies to all offences under this Act.

4. APPLICATION

This Act applies in Papua New Guinea.

5. INTERPRETATION

The following definitions apply for the purpose of this Act:

"account" includes:

(a) any facility or arrangement by which a financial institution or DNFBP does any of the following:

(i) accepts deposits of assets;

(ii) allows withdrawals or transfers of assets;

(iii) pays, collects or draws on a bearer negotiable instrument on behalf of any other person; or

(iv) supplies a safety deposit box or any other form of safe deposit; and

(b) for the avoidance of doubt, any account which may be closed or inactive, or has a nil balance.

"AML/CTF" means anti-money laundering and counter terrorist financing.

"AML/CTF compliance rule" means a compliance rule approved by the Governor of the Bank of Papua New Guinea under subsection 73(6), as amended from time to time.

"AML/CTF program" means a program established under section 7.

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

"bearer negotiable instrument" means:

(a) a bill of exchange;

(b) a cheque;

(c) a promissory note;

(d) a bearer bond;

(e) a traveller's cheque;

(f) a money order, postal order or similar order; or

(g) a negotiable instrument not covered by any of the above paragraphs.

"**beneficial owner**" means a natural person who:

(a) has ultimate control (directly or indirectly) of a customer; or

(b) ultimately owns (directly or indirectly) the customer;

and in this definition

(c) **"control"** includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies; and

(d) **"owns"** means ownership (either directly or indirectly) of 25% or more of a person or unincorporated entity.

"business relationship" means an on-going business, professional, or commercial relationship between a financial institution or DNFBP and a customer.

"conduct" means an act or omission when used in relation to an offence.

"Court" means the National Court of Papua New Guinea.

"**correspondent banking relationship"** means a relationship that involves the provision of banking business services by one financial institution (the **correspondent)** to another (the **respondent**) where:

(a) the correspondent carries on banking business at or through a permanent place of business in one country;

(b) the respondent carries on banking business at or through a permanent place of business in another country;

(c) the relationship between the correspondent and the respondent relates, in whole or in part, to the provision of banking services between those permanent places of business.

"criminal conduct" has the meaning given by section 508A of the *Criminal Code Act 2005*.

"criminal property" has the meaning given by section 508A of the *Criminal Code Act 2005*.

"currency" means legal tender in physical or non-physical form, or tender that is customarily used and accepted as a medium of exchange, in Papua New Guinea or a foreign country.

"customer" means:

(a) a person or unincorporated entity:

(i) for whom the financial institution or DNFBP carries out a transaction; or

(ii) with whom the financial institution or DNFBP conducts a business relationship;

and includes:

(b) a person or unincorporated entity who attempts to carry out a transaction or business relationship with the financial institution or DNFBP; and

(c) an existing or new customer.

"**Director**" means the Director of FASU.

"domestic electronic funds transfer" means an electronic funds transfer (or a chain of electronic funds transfers) where all of the parties to the transaction are located in Papua New Guinea.

"DNFBP" means a designated non-financial business or profession in Papua New Guinea and includes one or more of the following:

(a) a casino;

(b) a real estate agent;

(c) a dealer in precious metals;

(d) a dealer in precious stones;

(e) a lawyer, notary public, other independent legal professional or an accountant when preparing for, engaging in, or carrying out one or more transactions for a client concerning one or more of the following activities:

(i) buying and selling real estate;

(ii) managing client currency, securities or other assets;

(iii) managing bank, savings or securities accounts;

(iv) organising contributions for the creation, operation or management of bodies corporate;

(v) creating, operating or managing bodies corporate or unincorporated entities; or

(vi) buying and selling businesses; or

(f) a trust or company service provider;

(g) motor vehicle dealers.

"electronic funds transfer"

(a) means 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 currency available to a person (the **receiver,** who may also be the sender) at another financial institution;

and excludes

(b) transfers and settlements between financial institutions if both the sender and the receiver are financial institutions acting on their own behalf; and

(c) credit and debit card transactions if the credit or debit card number accompanies the transaction.

"FASU" means the Financial Analysis and Supervision Unit established under section 61.

"financial group" means a group that consists of a parent company or any other type of body corporate exercising control and coordinating functions over the rest of the group, and includes foreign branches and majority-owned subsidiaries of a financial institution or DNFBP in Papua New Guinea that are part of such a group.

"financial institution" means any person or unincorporated entity that conducts in Papua New Guinea one or more of the following activities for or on behalf of a customer:

(a) acceptance of deposits and other repayable funds from the public, including private banking;

(b) lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;

(c) financial leasing other than with respect to arrangements relating to consumer products;

(d) the transfer of currency or value;

(e) 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;

(f) issuing financial guarantees and commitments;

(g) trading in:

(i) bearer negotiable instruments;

(ii) foreign exchange;

(iii) exchange, interest rate and index instruments;

(iv) transferable securities; or

(v) commodity futures trading;

(h) participation in securities issues and the provision of financial services related to such issues;

(i) individual and collective portfolio management;

(j) safekeeping and administration of physical currency, bearer negotiable instruments or liquid securities on behalf of other persons;

(k) investing, administering or managing assets on behalf of other persons;

(l) underwriting and placement of insurance, including insurance intermediation by agents and brokers; or

(m) currency changing.

"foreign indictable offence" means an offence against the law of another country that, if the relevant act or omission had occurred in Papua New Guinea, would be an indictable offence.

"**foreign counterpart agency**" means an agency of another country that performs similar functions to FASU.

"international electronic funds transfer" means an electronic funds transfer (or a chain of electronic funds transfers) where at least one party to the transaction is located outside Papua New Guinea.

"money laundering" means conduct which constitutes an offence of money laundering under section 508B or section 508C of the *Criminal Code Act 2005*.

"occasional transaction" means a transaction that takes place outside an existing business relationship.

"payable-through account" means an account used directly by a third party customer of a respondent to transact business for that party or on behalf of another person.

"person" means a natural person and a body corporate**.**

"policeman" means a member of the Police Force.

"politically exposed person" means:

(a) 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 or the head of a government, a senior politician, a senior government official, a senior judicial official or a senior military official;

(b) a person who is or has been a senior executive in a foreign country of a state-owned company of that foreign country;

(c) a person who is or has been a senior political party official in a foreign country;

(d) 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;

(e) 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

(f) any person who is a family member or close associate of a person mentioned in paragraphs (a) to (e).

"precious metal" means–

(a) gold, silver, platinum, palladium, iridium, osmium, rhodium or ruthenium; or

(b) an alloy or other substance containing any of the metals referred to in paragraph (a).

"precious stone" means a substance with gem quality market-recognized beauty, rarity and value, and includes diamond, corundum (including rubies and sapphires), beryl (including emeralds and aquamarines), chrysoberyl, spinel, topaz, zircon, tourmaline, garnet, crystalline and cryptocrystalline quartz, olivine peridot, tanzanite, jadeite jade, nephrite jade, spodumene, feldspar, turquoise, lapis lazuli, and opal.

"premises" includes:

(a) a structure, building, vehicle, aircraft or vessel;

(b) a place (whether or not it is enclosed or built upon); and

(c) a part of a premises.

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

"regulatory authority" means an agency or body established in Papua New Guinea by or under a Constitutional Law or an Act whose functions include:

(a) setting, monitoring or enforcing compliance with standards or obligations prescribed by or under that or another Constitutional Law or Act; or

(b) granting a licence, practising certificate, registration or other equivalent permission by or under that or another Constitutional Law or Act.

"risk assessment" means an assessment of the risk of money laundering and terrorist financing undertaken in accordance with section 6.

"Sanctions Secretariat" means the Sanctions Secretariat referred to under section 26 of the *United Nations financial Sanctions Act 2015*.

"shell bank" means:

(a) a corporation that:

(i) is incorporated in a foreign country;

(ii) is authorised to carry on banking business in its country of incorporation;

(iii) does not have a physical presence in its country of incorporation; and

(iv) is not affiliated with another corporation that:

(A) is incorporated in a particular country;

(B) is authorised to carry on banking business in its country of incorporation;

(C) is sufficiently supervised and monitored in carrying on its banking business; and

(D) has a physical presence in its country of incorporation.

(b) For the purposes of subparagraph (a)(iii) and clause (a)(iv)(D), a corporation has a physical presence in a country if-

(i) the corporation carries on banking business at a place in that country; and

(ii) banking operations of the corporation are managed and conducted from that place.

(c) For the purposes of subparagraph (a)(iv), a corporation is affiliated with another corporation if –

(i) the corporation is a subsidiary of the other corporation; or

(ii) both corporations are under common effective control.

"terrorist financing" means conduct which constitutes an offence of terrorist financing under section 508J of the *Criminal Code Act 2005*.

"**third party financial institution or DNFBP**" means:

(a) a financial institution or DNFBP who performs customer due diligence on behalf of another financial institution or DNFBP under Section 18; or

(b) a person or unincorporated entity that carries out financial activities equivalent to those carried out by a financial institution, or conducts a non-financial business or profession equivalent to a non-financial business or profession carried out by a DNFBP, and who:

(i) is monitored and supervised by a foreign counterpart agency or an authority that regulates such persons or unincorporated entities; and

(ii) performs customer due diligence on behalf of another financial institution or DNFBP under Section 18.

"transaction"

(c) means a purchase, sale, loan, pledge, gift, transfer, delivery or other disposition, or the arrangement thereof and includes but is not limited to:

(i) the opening of an account;

(ii) any deposit, withdrawal, exchange, or transfer of assets (in any currency) whether:

(A) in physical currency;

(B) by cheque or other bearer negotiable instrument; or

(C) in non-physical currency;

(iii) the use of a safety deposit box or other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation;

(vi) any payment made in respect of a lottery, bet or other game of chance; or

(vii) establishing or creating a body corporate or unincorporated entity; and

(d) for the avoidance of doubt, a reference to a 'transaction' includes a reference to an attempted transaction.

"trust or company service provider" means a person or unincorporated entity who provides to one or more of the following services to another person or unincorporated entity:

(a) forming, registering or managing a body corporate;

(b) acting as, or arranging for another person to act:

(i) as a director or secretary or other office holder of a company;

(ii) as partner of a partnership; or

(iii) in a similar position in relation to a body corporate;

(c) providing a registered office, business address or accommodation, correspondence or administrative address for any body corporate or unincorporated entity;

(d) acting as, or arranging for another person to act as, a trustee of a trust or other similar unincorporated entity; or

(e) acting as, or arranging for another person to act as, a nominee shareholder for another person.

"**unincorporated entity"** includes any unincorporated group, undertaking, organisation or legal arrangement such as a trust or an unincorporated partnership.

"warrant" means a warrant issued under section 87.

PART 2 – OBLIGATIONS ON FINANCIAL INSTITUTIONS

DIVISION 1 – RISK ASSESSMENTS AND AML/CTF PROGRAMS

6. RISK ASSESSMENT

(1). A financial institution must undertake a risk assessment.

(2). A risk assessment must:

(a) be in writing (which includes it being stored electronically);

(b) identify and assess the risk (including the nature and level of risk) of money laundering and terrorist financing that the financial institution may reasonably expect to face in the course of its business;

(c) and be maintained and updated as required to take into account new and emerging risks.

(3). In identifying and assessing the level of risk for the purpose of paragraph (2)(b), a financial institution must have regard to the following:

(a) the nature, size and complexity of its business;

(b) the products and services it offers;

(c) the methods by which it delivers products and services to its customers;

(d) the types of customers it deals with, including politically exposed persons, residents in high risk countries and customers involved in high risk business activities;

(e) the countries or geographic areas it deals with and whether they are high risk countries or geographic areas;

(f) new and developing technologies and products, and new business practices, used by the financial institution or its customers that might assist the commission of money laundering or terrorist financing;

(g) the entities it deals with; and

(h) any applicable guidance produced by FASU or the regulatory authority that regulates the financial institution.

7. REQUIREMENTS FOR RISK BASED AML/CTF PROGRAM

(1). A financial institution must establish, implement and maintain an AML/CTF program.

(2). An AML/CTF program must be in writing (which includes it being stored electronically).

(3). A financial institution's AML/CTF program must be based on its risk assessment and include effective procedures, policies and controls, approved by senior management, for:

(a) managing and mitigating the risks identified in its risk assessment;

(b) monitoring the risks identified in its risk assessment;

(c) complying with the customer due diligence requirements in Divisions 2 and 3 of this Part including, but not limited to:

(i) ensuring that ongoing customer due diligence is conducted in accordance with Section 17;

(ii) determining when a financial institution may rely on a third party financial institution or DNFBP to conduct customer due diligence in accordance with Section 18;

(iii) determining when simplified customer due diligence might be permitted under Section 21;

(iv) determining when enhanced customer due diligence must be conducted under Section 26; and

(v) determining the conditions under which a financial institution may complete verification of identity after the establishment of a business relationship, in accordance with Sections 25(3) and 28(3); and

(d) complying with the other requirements of this Act including, but not limited to:

(i) appointing an AML/CTF compliance officer in accordance with section 8;

(ii) reporting a suspicious matter under section 41; and

(iii) record keeping obligations under Division 4 of this Part;

(e) vetting an employee to ensure he is fit and proper to engage in AML/CTF related duties; and

(f) providing training to an employee that is engaged in AML/CTF matters.

8. REQUIREMENT TO APPOINT AN AML/CTF COMPLIANCE OFFICER

(1). A financial institution must appoint a person with suitable qualifications and experience as its AML/CTF compliance officer to administer and maintain its AML/CTF program.

(2). An AML/CTF compliance officer must have direct access to senior management of the financial institution.

(3). A person appointed under subsection (1) may be, but is not required to be, an employee of the financial institution.

(4). Notwithstanding subsection (3), a financial institution has the ultimate responsibility for ensuring compliance with its obligations under this Act.

9. REVIEW AND AUDIT OF RISK ASSESSMENT AND AML/CTF PROGRAM

(1). A financial institution must review its risk assessment and AML/CTF program on a regular basis to:

(a) ensure its risk assessment and AML/CTF program remain current; and

(b) identify and address any deficiencies in the effectiveness of its risk assessment and AML/CTF program.

(2). A financial institution must periodically engage an external auditor to provide an independent review of its risk assessment and AML/CTF program and make recommendations for improvements.

10. APPOINTMENT OF AN EXTERNAL AUDITOR TO CONDUCT INDEPENDENT AUDIT

(1). FASU may, by written notice, require a financial institution to appoint an external auditor to conduct an independent audit of the financial institution's risk assessment and AML/CTF program.

(2). In conducting an independent audit under subsection (1), an external auditor must:

(a) assess whether the financial institution's risk assessment and AML/CTF program are current;

(b) identify any deficiencies in the effectiveness of the financial institution's risk assessment and AML/CTF program; and

(c) make recommendations to address any deficiencies identified under paragraph (b) and improve the financial institution's risk assessment and AML/CTF program.

(3). The financial institution must provide FASU with a copy of the external auditor's written report within the period specified in subsection (4)(c).

(4). A written notice under subsection (1) must specify:

(a) the matters to be covered by the audit;

(b) the form of the audit report; and

(c) the period within which the financial institution must provide a copy of the external auditor's report to FASU.

(5). A person is not eligible to be appointed as an external auditor by a financial institution if:

(a) the person is an officer, employee or agent of the financial institution; or

(b) the financial institution is part of a group, and the person is an officer, employee or agent of another member of that group.

11. EXTERNAL AUDITOR MAY HAVE REGARD TO THE RESULTS OF PREVIOUS AUDIT

In conducting an independent audit under section 10, an external auditor may have regard to the results of any previous audit if:

(a) an external audit was completed under that section within the last preceding 2 years; and

(b) the external auditor is satisfied that the previous audit is still relevant.

12. EXTERNAL AUDITORS

(1). FASU may prescribe in writing a list of specified persons or firms who may be appointed as an external auditor for the purpose of section 10(1) .

(2). A financial institution or DNFBP must appoint an external auditor prescribed by FASU under subsection (1), unless FASU has in writing approved the appointment of another auditor.

13. FINANCIAL GROUPS TO IMPLEMENT GROUP-WIDE AML/CTF PROGRAM

(1). A financial group must implement a group-wide AML/CTF program, which should:

(a) be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group; and

(b) cover the requirements in sections 7 to 12;

and include

(c) policies and procedures for sharing information required for the purposes of customer due diligence and AML/CTF risk management;

(d) policies and procedures for branches and majority-owned subsidiaries to provide customer, account, and transaction information to the financial group when necessary; and

(e) adequate safeguards on the confidentiality and use of information exchanged.

(2). For the purpose of this section, a "group-wide AML/TFF program" means a program established by a financial group in accordance with subsection (1).

14. OFFENCE OF FAILURE TO COMPLY WITH RISK ASSESSMENT, AML/CTF PROGRAM AND APPOINTMENT OF EXTERNAL AUDITOR OBLIGATIONS

(1). A person who intentionally engages in conduct that contravenes a requirement of section 6, section 7, section 8 or section 9 is guilty of a crime.

Penalty: If the offender is a natural person – a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate – a fine not exceeding K1,000,000.00.

(2). A person who recklessly engages in conduct that contravenes a requirement of section 6, section 7, section 8 or section 9 is guilty of a crime.

Penalty: If the offender is a natural person – a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate – a fine not exceeding K500,000.00

(3). A person who intentionally fails to comply with a notice under subsection 10(1) is guilty of a crime.

Penalty: If the offender is a natural person – a fine not exceeding K100,000.00.

If the offender is a body corporate a fine not exceeding K200,000.00.

(4). A person who recklessly fails to comply with a notice under subsection 10(1) is guilty of a crime.

Penalty: If the offender is a natural person – a fine not exceeding K50,000.00.

If the offender is a body corporate a fine not exceeding K100,000.00

(5). For the purpose of subsections (1) and (3), intention can be inferred from objective factual circumstances.

DIVISION 2 – DUE DILIGENCE

SUBDIVISION 1 – GENERAL DUE DILIGENCE REQUIREMENTS

15. RELIANCE ON RISK ASSESSMENT AND AML/CTF PROGRAM

When assessing risk (including the nature and level of risk) for the purpose of complying with this Division, a financial institution must assess risk in accordance with its risk assessment, and the procedures, policies and controls approved by senior management for managing and mitigating identified risks, as set out in its AML/CTF program.

16. BASIS FOR VERIFYING IDENTITY

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

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

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

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

17. ONGOING DUE DILIGENCE

(1). A financial institution is under an obligation to conduct ongoing due diligence in respect of all of its business relationships.

(2). When conducting ongoing due diligence, a financial institution must, at a minimum, do the following:

(a) maintain current and up to date information and records relating to its customers and their beneficial owners;

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

(c) ensure that ongoing enhanced due diligence is conducted with respect to politically exposed persons in accordance with paragraphs 29(3)(b) and 29(6)(b); and

(d) ensure that ongoing due diligence is conducted with respect to correspondent banking relationships in accordance with subsection 34(2).

18. RELIANCE ON THIRD PARTY FINANCIAL INSTITUTION OR DNFBP FOR CUSTOMER DUE DILIGENCE

(1). Subject to subsection (4), a financial institution may rely on a third party financial institution or DNFBP to conduct customer due diligence on a person or unincorporated entity referred to subsection 20(1), as required by Subdivision 2 or Subdivision 3 of this Division, if the financial institution:

(a) has no suspicion of money laundering or terrorist financing;

(b) is satisfied that the third party financial institution or DNFBP:

(i) is able to provide without delay copies of information regarding the identity and verification of identity of the person or unincorporated entity referred to in subsection 20(1), information on the nature and purpose of the business relationship, and any other information relating to customer due diligence upon request; and

(ii) is subject to the jurisdiction of a State which is not considered a high risk jurisdiction and where the third party financial institution or DNFBP is subject to AML/CTF requirements at least equivalent to those specified in this Act, and is supervised for compliance with those requirements in a manner at least equivalent to that which is specified in this Act; and

(c) is satisfied that the third party financial institution or DNFBP cannot rely on or claim legal professional privilege, confidentiality or other contractual agreement when responding to a request for information referred to in subparagraph (b)(i).

(2). Subject to subsection (3), where a financial institution relies on a third party financial institution or DNFBP to conduct customer due diligence in accordance with subsection (1), it must obtain the information referred to in subparagraph (1)(b)(i) from the third party financial institution or DNFBP before:

(a) establishing a new business relationship;

(b) carrying out an occasional transaction of an amount in currency equal to or greater than K20,000.00;

(c) making a payment to a beneficiary pursuant to a life insurance policy; or

(d) ordering an electronic funds transfer or an amount in currency equal to or greater than K2,500.00 in the case of an ordering financial institution within the meaning of Section 31(1).

(3). The verification of the identity of the person or unincorporated entity referred to in subsection 20(1) may be completed as soon as reasonably practicable after the establishment of the business relationship where:

(a) the risk of money laundering or terrorist financing is not high and is effectively managed by the financial institution; and

(b) a delay in verification is essential in order not to interrupt the regular conduct of business of the financial institution.

(4). A financial institution has the ultimate responsibility for compliance with this Act.

19. WHERE CUSTOMER DUE DILIGENCE CANNOT BE COMPLETED OR MUST BE CEASED

(1)Where a financial institution is unable to conduct customer due diligence required by Subdivision 2 or Subdivision 3 of this Division, the financial institution:

(a) must not establish a business relationship with the new customer;

(b) must terminate any existing business relationship with the customer;

(c) must not carry out an occasional transaction with or for the customer;

(d) must not, if it is an ordering financial institution within the meaning of subsection 31(1), carry out an electronic funds transfer if it is not transmitted with the information required under subsection 31(5);

(e) must, if it is an intermediary financial institution within the meaning of subsection 32(1) consider whether to carry out, reject or suspend an electronic funds transfer pursuant to subsection 32(3);

(f) must, if it is a beneficiary financial institution within the meaning of section 33(1), consider whether to carry out, reject or suspend an electronic funds transfer pursuant to subsection 33(3);

(g) must consider whether to make a suspicious matter report under subsection 41(4); and

(h) may, under subsection 41(11), communicate to FASU any suspicions it may have prior to making a suspicious matter report.

(2) Where a financial institution forms a suspicion of money laundering or terrorist financing, and the financial institution has reasonable grounds to believe that performing customer due diligence will tip-off the customer, the financial institution:

(a) must cease to conduct customer due diligence;

(b) must comply with paragraphs (1)(a) to (1)(f) and (1)(h); and

(c) must file a suspicious matter report under subsection 41(4).

SUBDIVISION 2 – CUSTOMER DUE DILIGENCE REQUIREMENTS

20. OBLIGATION TO CONDUCT CUSTOMER DUE DILIGENCE

(1). Subject to subsection (2), a financial institution must conduct customer due diligence on:

(a) a customer;

(b) any beneficial owner of a customer;

(c) any person or unincorporated entity acting on behalf of a customer; and

(d) a beneficiary of an insurance policy.

(2). A financial institution that is required to conduct customer due diligence in the circumstances described in this Subdivision is not required to obtain or verify any documents, data or information that it has previously obtained and verified for the purposes of carrying out customer due diligence in accordance with this Division, unless there are reasonable grounds for the financial institution to doubt the adequacy or veracity of the documents, data or information previously obtained.

Simplified Customer Due Diligence

21. CIRCUMSTANCES WHERE SIMPLIFIED CUSTOMER DUE DILIGENCE MAY BE APPLIED

(1). Subject to subsection (2), a financial institution may conduct simplified customer due diligence in accordance with section 22 in the following circumstances:

(a) if standard customer due diligence is not required under Subdivision 2 of this Division;

(b) if enhanced customer due diligence is not required under Subdivision 2 of this Division;

(c) if the financial institution takes the view that the customer is not resident in a high risk country;

(d) if the financial institution does not suspect money laundering or terrorist financing; and

(e) if the financial institution takes the view that the customer is a low risk.

(2). A financial institution must conduct customer due diligence in accordance with the requirements of Subdivision 3 of this Division in relation to an electronic funds transfer in currency equivalent to or above K2,500.00.

22. SIMPLIFIED CUSTOMER DUE DILIGENCE: IDENTITY AND VERIFICATION REQUIREMENTS

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

(2) The information may include:

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

(b) 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;

(c) 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; and

(d) for a person who is not the customer, the person's relationship to the customer.

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

(4) Simplified customer due diligence must be conducted before carrying out a transaction.

Standard Customer Due Diligence

23. CIRCUMSTANCES WHERE STANDARD CUSTOMER DUE DILIGENCE APPLIES

(1) A financial institution must conduct standard customer due diligence in accordance with the requirements of sections 24 and 25 in the following circumstances:

(a) if a new customer wishes to establish a business relationship with a financial institution, including if a new customer wishes to open an account or establish an insurance policy with a financial institution;

(b) if a customer wishes to carry out an occasional transaction of an amount in currency equal to or greater than K20,000.00, whether conducted as a single transaction or by way of several transactions that appear to be linked;

(c) if, in respect of an existing customer and according to the level of risk involved, doubt exists about the veracity or adequacy of previously obtained customer information; or

(d) if, during the establishment, or during the course of, a business relationship, or when conducting an occasional transaction, there is a suspicion of money laundering or terrorist financing involving the customer or the customer's account.

(2) In addition to the requirement to conduct standard customer due diligence in the circumstances described in subsection (1), a financial institution must conduct customer due diligence in accordance with the requirements of Subdivision 3 of this Division in relation to an electronic funds transfer of an amount in currency equal to or greater than K2,500.00.

24. STANDARD CUSTOMER DUE DILIGENCE: IDENTITY REQUIREMENTS

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

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

(b) 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;

(c) 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; and

(d) for a person who is not the customer, the person's relationship to the customer.

(2). A financial institution must also obtain the following information when conducting standard due diligence:

(a) sufficient information to allow it to understand the nature and purpose of the intended business relationship; and

(b) where the customer is a body corporate or unincorporated entity, sufficient information to allow it to understand the nature and business of the customer.

25. STANDARD CUSTOMER DUE DILIGENCE: VERIFICATION OF IDENTITY REQUIREMENTS

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

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

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

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

(2) Subject to subsection (3), a financial institution must verify the identity of a person or unincorporated entity referred to in subsection 20(1) before:

(a) establishing the business relationship;

(b) carrying out an occasional transaction; or

(c) making a payment to a beneficiary pursuant to an insurance policy.

(3) The verification of the identity of a person or unincorporated entity referred to in subsection 20(1) may be completed as soon as reasonably practicable after the establishment of the business relationship where:

(a) the risk of money laundering or terrorist financing is not high and is effectively managed by the financial institution; and

(b) a delay in verification is essential in order not to interrupt the regular conduct of business of the financial institution.

Enhanced Customer Due Diligence

26. CIRCUMSTANCES WHERE ENHANCED CUSTOMER DUE DILIGENCE APPLIES

(1) A financial institution must conduct enhanced customer due diligence in accordance with the requirements of sections 27 and 28 in the following circumstances:

(a) if it takes the view that the customer is a resident in a high risk country;

(b) if it takes the view that the customer is involved in a high risk business activity;

(c) if it takes the view that the customer is a politically exposed person;

(d) if it takes the view that the customer or a beneficiary of an insurance policy is a high risk;

(e) if it takes the view that the risk of money laundering or terrorist financing is high; or

(f) if the customer is not physically present for the purpose of identification.

(2) In addition to the requirement to conduct enhanced customer due diligence in the circumstances described in subsection (1), a financial institution must conduct customer due diligence in accordance with the requirements of Subdivision 3 of this Division in relation to an electronic funds transfer that is equal to or above K2,500.00.

27. ENHANCED CUSTOMER DUE DILIGENCE: IDENTITY REQUIREMENTS

A financial institution must, in relation to a person or unincorporated entity referred to in subsection 20(1), obtain the following information when conducting enhanced due diligence:

(a) the identity information required for standard customer due diligence as set out in section 24;

(b) information relating to the source of the assets or the wealth of the customer; and

(c) 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.

28. ENHANCED CUSTOMER DUE DILIGENCE: VERIFICATION OF IDENTITY REQUIREMENTS

(1). A financial institution must, at a minimum, undertake the following verification requirements of a person or unincorporated entity referred to in subsection 20(1) when conducting enhanced due diligence:

(a) conduct the verification of identity requirements for standard due diligence as set out in section 25;

(b) take reasonable steps to verify information relating to the source of the assets or the wealth of the customer; and

(c) where the beneficiary of an insurance policy is a body corporate or an unincorporated entity, take steps to verify the identify the beneficial owner of the beneficiary.

(2). Subject to subsection (3), a financial institution must verify the identity of a person or unincorporated entity referred to in subsection 20(1) before:

(a) establishing a new business relationship;

(b) carrying out an occasional transaction of an amount in currency equal to or greater than K20,000.00; or

(c) making a payment to a beneficiary pursuant to an insurance policy.

(3). The verification of the identity of a person or unincorporated entity referred to in subsection 20(1), and the identity of a beneficial owner of beneficiaries of insurance policies, may be completed as soon as reasonably practicable after the establishment of the business relationship where:

(a) the risk of money laundering or terrorist financing is not high and is effectively managed by the financial institution; and

(b) a delay in verification is essential in order not to interrupt the normal conduct of business of the financial institution.

29. ENHANCED CUSTOMER DUE DILIGENCE: ADDITIONAL REQUIREMENTS FOR POLITICALLY EXPOSED PERSONS

(1). A financial institution must take all reasonable steps to identify whether a customer or beneficial owner is a politically exposed person.

(2). Where a financial institution takes the view that a customer or beneficial owner is a politically exposed person, it must conduct the additional measures as set out in subsection (3).

(3). If a financial institution takes the view that a customer or beneficial owner with whom it is establishing a business relationship, or has established a business relationship, is a politically exposed person, it must:

(a) obtain the approval of senior management to commence or continue the business relationship with the customer or the beneficial owner; and

(b) conduct ongoing enhanced due diligence of the business relationship.

(4). A financial institution must take all reasonable steps to identify whether a beneficiary of an insurance policy or beneficial owner of the beneficiary is a politically exposed person.

(5). Where a financial institution takes the view that a beneficiary of an insurance policy or beneficial owner of the beneficiary is a politically exposed person, it must conduct the additional measures as set out in subsection (6).

(6). If a financial institution takes the view that a beneficiary of an insurance policy or beneficial owner of the beneficiary, is a politically exposed person and the level of risk is high, it must before making a payment to the beneficiary under the insurance policy:

(a) obtain the approval of senior management to make the payment;

(b) conduct enhanced due diligence of the business relationship relating to the insurance policy; and

(c) consider making a suspicious matter report under subsection 41(4).

SUBDIVISION 3 – CUSTOMER DUE DILIGENCE REQUIREMENTS FOR ELECTRONIC FUNDS TRANSFERS

30. OVERVIEW OF CUSTOMER DUE DILIGENCE REQUIREMENTS FOR ELECTRONIC FUNDS TRANSFERS

(1). A financial institution that is required to conduct customer due diligence in the circumstances described in this Subdivision is not required to verify any documents, data or information that it has previously verified for the purposes of carrying out customer due diligence in accordance with this Division, unless there are reasonable grounds for the financial institution to doubt the adequacy or veracity of the documents, data or information previously obtained.

(2). A financial institution that is required to conduct customer due diligence in the circumstances described in this Subdivision must also:

(a) conduct standard customer due diligence in accordance with the requirements of sections 24 and 25 if any of the circumstances described in section 23 apply and;

(b) conduct enhanced customer due diligence in accordance with the requirements of sections 27, 28 and 29 if any of the circumstances described in section 26 apply;

31. ELECTRONIC FUNDS TRANSFER – IDENTITY AND VERIFICATION OF IDENTITY REQUIREMENTS FOR ORDERING FINANCIAL INSTITUTIONS

(1). This section applies to a financial institution that receives a request from a sender to execute an electronic funds transfer of an amount in currency equal to or greater than K2,500.00 (an ordering financial institution).

(2). In the case of a request to execute an international electronic funds transfer, an ordering financial institution must:

(a) in the case of an international electronic funds transfer or a domestic electronic funds transfer, identify the sender of the electronic funds transfer by obtaining the following identity information:

(i) the sender’s full name;

(ii) the sender's account number or such other identifying information that allows the transaction to be traced back to the sender; and

(iii) any one of the following:

(A) the sender's address;

(B) the sender's customer identification number; or

(C) the sender's place and date of birth.

(b) in the case of an international electronic funds transfer, identify the receiver of the electronic funds transfer by obtaining the following identity information:

(i) the receiver's full name; and

(ii) the receiver's account number or, other identifying information that allows the transaction to be traced back to the receiver.

(3). An ordering financial institution must, based on the level of risk, verify the sender's identity so that it is satisfied that the information obtained under paragraph (2)(a) is correct.

(4). An ordering financial institution must verify the sender's identity before ordering the electronic funds transfer.

(5). An ordering financial institution must transmit with the electronic funds transfer:

(a) identity information about the sender that it has obtained under paragraph (2)(a) and verified under subsection (3); and

(b) in the case of an international electronic funds transfer, identity information about the receiver that it has obtained under paragraph (2)(b).

32. ELECTRONIC FUNDS TRANSFERS – REQUIREMENTS FOR INTERMEDIARY FINANCIAL INSTITUTIONS

(1) This section applies to a financial institution that receives a request to act as an intermediary in a chain of electronic funds transfers of an amount in currency equal to or greater than K2,500.00 (an **intermediary financial institution**).

(2) Subject to subsection (3), an intermediary financial institution must transmit all of the identity information it receives under subsection 31(5) from an ordering financial institution with the electronic funds transfer.

(3) Where an intermediary financial institution does not receive all of the identity information required to accompany an electronic funds transfer under subsection 31(5) it must, based on the level of risk, assess whether to execute, reject or suspend that electronic funds transfer.

33. ELECTRONIC FUNDS TRANSFERS - IDENTITY AND VERIFICATION OF IDENTITY REQUIREMENTS FOR BENEFICIARY FINANCIAL INSTITUTIONS

(1) This section applies to a financial institution that receives a request to receive an electronic funds transfer of an amount in currency equal to or greater than K2,500.00 on behalf of a receiver (**beneficiary financial institution**).

(2) A beneficiary financial institution must, based on the level of risk, verify the receiver's identity so that it is satisfied that the information obtained by the ordering financial institution under paragraph 31(2)(b) is correct.

(3) Where a beneficiary financial institution does not receive all of the information required to accompany an electronic funds transfer from an ordering financial institution under subsection 31(5) or from an intermediary financial institution under subsection 32(2), it must, based on the level of risk, assess whether to execute, reject or suspend that electronic funds transfer.

SUBDIVISION 4 – DUE DILIGENCE REQUIREMENTS FOR CORRESPONDENT BANKING RELATIONSHIPS

34. DUE DILIGENCE FOR CORRESPONDENT BANKING RELATIONSHIPS

(1) Where a financial institution enters or proposes to enter into a correspondent banking relationship it must undertake the following due diligence prior to the commencement of that relationship:

(a) identify and verify the identity of the respondent with which it proposes to conduct a correspondent banking relationship;

(b) take steps to understand the nature of the respondent's business activities;

(c) 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;

(d) assess the respondent's AML/CTF controls to ascertain that those controls are adequate and effective;

(e) obtain approval from senior management before establishing a new correspondent banking relationship;

(f) establish an agreement which sets out the respective responsibilities of each party under the correspondent banking relationship; and

(g) in the case of a payable-through account, ensure that the respondent has verified its own customer's identity, has implemented mechanisms for ongoing due diligence with respect to its customers, and is capable of providing relevant identification information on request.

(2) A financial institution must conduct ongoing due diligence of a respondent financial institution.

35. WHERE DUE DILIGENCE CANNOT BE COMPLETED

Where a financial institution is unable to conduct due diligence required by Section 34, the financial institution must not establish the correspondent banking relationship.

SUBDIVISION 5 – OFFENCES

36. FAILURE TO COMPLY WITH DUE DILIGENCE REQUIREMENTS

(1) A person who intentionally engages in conduct that contravenes a requirement of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2) For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3) A person who recklessly engages in conduct that contravenes a requirement of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500, 000.00.

37. OFFENCE OF OPENING OR OPERATING ANONYMOUS ACCOUNTS AND ACCOUNTS IN FALSE NAMES

(1). A person who intentionally opens or operates an anonymous account or an account in a false name is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2). For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3). A person who recklessly opens or operates an anonymous account or an account in a false name is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500, 000.00.

38. OFFENCE OF ESTABLISHING OR CONTINUING A BUSINESS RELATIONSHIP INVOLVING A SHELL BANK

(1). A person who intentionally:

(a) establishes or takes steps to establish a shell bank in Papua New Guinea;

(b) enters into or continues 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 shell bank; or

(c) allows an occasional transaction to be conducted through it by a shell bank or a correspondent financial institution in a foreign country that permits its accounts to be used by a shell bank

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate- a fine not exceeding K1,000,000.00

(2). For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3). A person who recklessly:

(a) establishes or takes steps to establish a shell bank in Papua New Guinea;

(b) enters into or continues 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 shell bank; or

(c) allows an occasional transaction to be conducted through it by a shell bank or a correspondent financial institution in a foreign country that permits its accounts to be used by a shell bank

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate- a fine not exceeding K500,000.00.

DIVISION 3 – REPORTING OBLIGATIONS

SUBDIVISION 1 – REPORTING OBLIGATIONS AND OFFENCES

39. THRESHOLD REPORTING OBLIGATION

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

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

(3). A financial institution must report to FASU under subsection (1) or subsection (2) as soon as reasonably practicable and in any event within 10 working days from the date of the transaction where it is a single transaction, or from the date of the last transaction, where there are two or more transactions that appear to be linked.

(4). A financial institution must provide a report required under subsection (1) in accordance with any form and procedure specified by FASU.

(5). Compliance with subsection (1) does not affect the obligation of a financial institution to make a suspicious matter report under section 41(4).

(6). A person who intentionally fails to make a report under subsection (1) or subsection (2) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(7). For the purposes of subsection (6), intention can be inferred from objective factual circumstances.

(8). A person who recklessly fails to make a report under subsection (1) or subsection (2) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

40. OBLIGATION TO REPORT ASSETS OF A DESIGNATED PERSON OR ENTITY

(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 designation under section 13(f) of the *United Nations Financial Sanctions Act 2015*.

(2). A financial institution must provide a report required under subsection (1) in accordance with any form and procedure specified by FASU.

(3). For the purpose of this section:

(a) "**asset"** has the meaning given by section 6 of the United Nations Financial Sanctions Act 2015; and

(b) "**designated person or entity"** has the meaning given by section 6 of the United Nations Financial Sanctions Act 2015.

(4). A person who intentionally fails to make a report under subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(5). For the purposes of subsection (4), intention can be inferred from objective factual circumstances.

(6). A person who recklessly fails to make a report under subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

41. SUSPICIOUS MATTER REPORTING OBLIGATIONS

(1). This section applies where a financial institution has reasonable grounds to suspect that information that is known to it may:

(a) be relevant to the detection, investigation or prosecution of a person for money laundering, terrorist financing, an offence under section 15 or section 16 of the *United Nations Financial Sanctions Act 2015* or any other indictable offence;

(b) be relevant to the detection, investigation or prosecution of a person for a foreign indictable offence; or

(c) concern criminal property.

(2). For the avoidance of doubt, subsection (1) applies where a suspicion is formed after this Act comes into operation, but that suspicion may be based on information obtained before this Act came into operation.

(3). Where subsection (1) applies, a financial institution must take reasonable measures to ascertain the following information:

(a) the purpose of the transaction;

(b) the origin of the funds;

(c) where the funds will be sent;

(d) the name and address of the person who will receive the funds; and

(e) any other information that may be relevant to the prosecution or investigation of:

(i) an offence of the kind referred to in paragraph (1)(a);

(ii) any proceedings under this Act; or

(iii) a proceeds of crime law of Papua New Guinea.

(4). Where subsection (1) applies, 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 the suspicion first arose.

(5). A report under subsection (4) must include:

(a) such information referred to in subsection (3) that is known to the financial institution;

(b) any other information required by FASU that is known to the financial institution; and

(c) the basis on which the suspicion has arisen.

(6). A financial institution must provide a report under subsection (4) in accordance with any form and procedure specified by FASU.

(7). A financial institution that has made a report in accordance with subsection (4) must, if requested to do so by FASU, provide to FASU any further information that it has relating to the suspicion.

(8). A person who intentionally fails to make a report under subsection (4) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(9). For the purpose of subsection (8), intention can be inferred from objective factual circumstances.

(10). A person who recklessly fails to make a report under subsection (4) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

(11). Nothing in this section precludes a financial institution from communicating to FASU any suspicions it may have prior to the making of a report under subsection (4).

42. PROVIDING A FALSE OR MISLEADING REPORT OR INFORMATION

(1). A person who furnishes 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 this Division, is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2). For the purposes of subsection (1), knowledge can be inferred from objective factual circumstances.

(3). A person who furnishes 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 this Division, is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

43. OBLIGATION NOT TO DISCLOSE A REPORT ETC.

(1). Where a financial institution has made or may make a report to FASU under subsection 39(1), subsection 39(2), subsection 40(1) or subsection 41(4), the

financial institution must not, unless required to do so under this Act, disclose to anyone else:

(a) the report;

(b) that the report has been or may be made to FASU; or

(c) any other information from which a person could reasonably infer that a report has been or may be made to FASU.

(2). Subsection (1) does not apply to a disclosure made by the financial institution to:

(a) FASU in accordance with this Act;

(b) a policeman for any law enforcement purpose;

(c) an officer or employee or agent of the financial institution for any purpose connected with the performance of that person's AML/CTF duties; or

(d) a lawyer for the purpose of obtaining legal advice or representation in relation to the matter.

(3). Subsection (1) does not apply where a court is satisfied that disclosure is necessary in the interests of justice.

(4). A person who intentionally discloses information in contravention of subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(5). For the purposes of subsection (4), intention can be inferred from objective factual circumstances.

(6). A person who recklessly discloses information in contravention of subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

44. OBLIGATION NOT TO DISCLOSE INFORMATION OR SUSPICION

(1). Where section 41(1) applies, the financial institution must not, unless required to do so under this Act, disclose to anyone else:

(a) that the financial institution has formed a suspicion under section 41(1);

(b) that a suspicion has been or may be communicated to FASU under section 41(11); or

(c) any other information from which a person could reasonably infer any of the matters in subsections (a) or (b) above.

(2). Subsection (1) does not apply to disclosures made by the financial institution to:

(a) FASU in accordance with this Act;

(b) a policeman for any law enforcement purpose;

(c) an officer or employee or agent of the financial institution for any purpose connected with the performance of that person's AML/CTF duties; or

(d) a lawyer for the purpose of obtaining legal advice or representation in relation to the matter.

(3). Subsection (1) does not apply where a court is satisfied that disclosure is necessary in the interests of justice.

(4). A person who intentionally discloses information in contravention of subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(5). For the purposes of subsection (4), intention can be inferred from objective factual circumstances.

(6). A person who recklessly discloses information in contravention of subsection (1) is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

45. PROTECTION OF IDENTITY IN RELATION TO SUSPICIOUS MATTER REPORTS

(1). A person who intentionally discloses 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 section 41 is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00

(2). For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3). A person who recklessly discloses any transaction, report or information that will identify, or is likely to identify, the person who prepared or made a report or provided information under section 41 is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

(4). Subsections (1) and (2) do not apply to disclosures made by the financial institution to:

(a) a policeman for any law enforcement purpose;

(b) an officer or employee or agent of the financial institution for any purpose connected with the performance of that person's AML/CTF duties;

(c) a lawyer for the purpose of obtaining legal advice or representation in relation to the matter; or

(d) FASU in accordance with this Act.

SUBDIVISION 2 – OTHER OFFENCES

46. STRUCTURING OFFENCE

(1). A person who:

(a) conducts two or more transactions by whatever means that are equivalent to K20,000.00 or less; and

(b) 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 section 39

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2). For the purpose of paragraph (1)(b), a Court may have regard to:

(d) the manner and form in which the transactions were conducted, including, but not limited to, any of the following:

(i) the value of the currency involved in each transaction;

(ii) the aggregated value of the currency involved in the transactions;

(iii) the period of time over which the transactions occurred;

(iv) the interval of time between any of the transactions; and

(v) the locations at which the transactions were initiated or conducted; and

(e) any explanation made by the person as to the manner or form in which the transactions were conducted.

DIVISION 4 – RECORD KEEPING BY FINANCIAL INSTITUTIONS

47. OBLIGATION TO KEEP TRANSACTION RECORDS

(1). In relation to every transaction conducted by or through a financial institution, the financial institution must keep such records as are reasonably necessary to enable that transaction to be readily reconstructed at any time.

(2). Without limiting subsection (1), records must contain the following information:

(a) the nature of the transaction;

(b) the date of the transaction;

(c) the amount of the transaction and the type of currency;

(d) the parties to the transaction;

(e) the type and identifying number of any account with the financial institution involved in the transaction;

(f) if the transaction involves a bearer negotiable instrument:

(i) the name of the drawer of that instrument;

(ii) the name of the institution on which it was drawn;

(iii) the name of the payee (if any);

(iv) the amount and date of the instrument;

(v) the number (if any) of the instrument; and

(vi) details of any endorsements appearing on the instrument;

(g) the name and address of the financial institution and name of the officer, employee or agent of the financial institution who handled the transaction, if that officer, employee or agent:

(i) has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and

(ii) has formed a suspicion under subsection 41(1).

(3). A financial institution must retain the records it has kept, in accordance with this section, for:

(a) at least 7 years after the completion of that transaction; or

(b) any longer period that FASU may prescribe by regulations.

48. OBLIGATION TO KEEP IDENTITY AND VERIFICATION RECORDS

(1). In respect of each case in which a financial institution is required to identify and verify the identity of a person or unincorporated entity under Division 2 of this Part, a financial institution must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that identification and verification to be readily available at any time.

(2). Without limiting subsection (1), those records may comprise:

(a) a copy of the evidence so used; or

(b) if it is not practicable to retain that evidence, any information as is reasonably necessary to enable that evidence to be obtained.

(3). A financial institution must retain the identity and verification records for 7 years:

(a) after the end of the business relationship;

(b) after carrying out an occasional transaction in an amount equal to or above K20,000, whether conducted as a single transaction or by way of several transactions that appear to be linked;

(c) after payment to a beneficiary pursuant to an insurance policy;

(d) after entering into a correspondent banking relationship with another financial institution;

(e) after carrying out an electronic funds transfer of an amount equal to or above K2,500.00; or

(f) after conducting due diligence in any other circumstance as set out in Division 2 of this Part

as the case may be appropriate.

49. GENERAL OBLIGATION TO KEEP OTHER RECORDS

(1). A financial institution must also keep the following records:

(a) records that relate to a risk assessment, AML/CFT program and audit undertaken in accordance with Division 1 of this Part;

(b) records that are relevant to the establishment of the business relationship with the customer; and

(c) other customer records, including but not limited to, account files and business correspondence relating to, and obtained during the course of, a business relationship that are reasonably necessary to establish the nature and purpose of, and activities relating to that business relationship with the customer.

(2). A financial institution must retain the records kept by it for at least 7 years after the end of the business relationship.

50. INTERACTION WITH OTHER LEGISLATION

Nothing in this Division affects the obligation of a financial institution to retain records in accordance with the requirements of any other applicable legislation.

51. FAILURE TO COMPLY WITH RECORD KEEPING REQUIREMENTS

(1) A person who intentionally engages in conduct that contravenes a requirement of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2) For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3) A person who recklessly engages in conduct that contravenes a requirement of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

PART 3 – OBLIGATIONS ON DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

52. OBLIGATIONS ON DNFBPS

(1) Subject to subsection (2), a DNFBP is required to comply with the obligations set out in Part 2, as if the references in that Part to a financial institution were a reference to a DNFBP, in the following circumstances:

(a) a casino – when a customer engages in a transaction equal to or above K10,000.00;

(b) a real estate agent – when it is involved in a transaction for a client concerning the buying and selling of real estate;

(c) a dealer in precious metals – when it engages in a transaction with a customer in currency equal to or above K40,000.00;

(d) a dealer in precious stones – when it engages in a transaction with a customer in currency equal to or above K40,000.00;

(e) a lawyer, notary public, other independent legal professional or an accountant when preparing for, engaging in, or carrying out one or more transactions for a client concerning any of the following activities:

(i) buying and selling real estate;

(ii) managing client money, securities or other funds;

(iii) managing bank, savings or securities accounts;

(iv) organising contributions for the creation, operation or management of bodies corporate;

(v) creating, operating or managing bodies corporate or unincorporated entities; or

(vi) buying and selling businesses; and

(f) a trust or company service provider.

(2) A DNFBP is not required to comply with the due diligence requirements set out in:

(a) Sections 30 to 33 on electronic funds transfers; and

(b) Sections 34 and 35 on correspondent banking relationships.

53. OFFENCES

Where a DNFBP is required to comply with an obligation under Part 2, and the DNFBP fails to comply with that obligation, any offence and penalty provision relating to the obligation that is applicable to a financial institution is also applicable to a DNFBP.

PART 4 – ADDITIONAL OBLIGATIONS APPLYING TO FINANCIAL INSTITUTIONS AND DNFBPS

54. FOREIGN BRANCHES AND MAJORITY-OWNED FOREIGN SUBSIDIARIES TO COMPLY WITH PARTS 2 AND 3

(1). A financial institution 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 2.

(2). If the law of a foreign country does not permit the application of the equivalent measures in subsection (1) the financial institution must, as soon as is reasonably practicable:

(a) inform FASU accordingly; and

(b) take such additional measures as are permitted to implement the requirements of Part 2.

(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 3.

(4). If the law of a foreign country does not permit the application of the equivalent measures in subsection (3), the DNFBP must, as soon as is reasonably practicable:

(a) inform FASU accordingly; and

(b) take such additional measures as are permitted to implement the requirements of Part 3.

55. FAILURE TO COMPLY WITH REQUIREMENTS RELATING TO FOREIGN BRANCHES AND MAJORITY-OWNED FOREIGN SUBSIDIARIES

(1) A person who intentionally engages in conduct that contravenes a requirement of section 54 is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(2) For the purposes of subsection (1), intention can be inferred from objective factual circumstances.

(3) A person who recklessly engages in conduct that contravenes a requirement of section 54 is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

56. PROTECTION FROM LIABILITY FOR ACTS DONE IN GOOD FAITH

(1) No financial institution, member of its governing body, or officer, employee or agent of the financial institution, and no person who has been a member of its governing body or who has been an officer, employee or agent of the financial institution shall be subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done in good faith in the discharge of their obligations under this Act.

(2) No DNFBP, member of its governing body, or officer, employee or agent of the DNFBP, and no person who has been a member of its governing body or who has been an officer, employee or agent of the DNFBP shall be subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done in good faith in the discharge of their obligations under this Act.

(3) For the avoidance of doubt, nothing in subsection (1) or (2) precludes the prosecution of a person for money laundering, terrorist financing or offences arising under other laws.

57. REQUIREMENT TO REGISTER WITH FASU

(1). A financial institution and a DNFBP must register with FASU for the purpose of this Act.

(2). FASU may specify the form, content and procedure for such registration.

58. FAILURE TO REGISTER WITH FASU

A person who fails to register with FASU under section 57 is guilty of a crime.

Penalty: If the offender is a natural person – a fine not exceeding K25,000.00.

If the offender is a body corporate – a fine not exceeding K50,000.00.

PART 5 – BENEFICIAL OWNERSHIP INFORMATION AND FIT AND PROPER CONTROLS

59. OBLIGATIONS ON FINANCIAL INSTITUTIONS AND DNFBPS TO DISCLOSE BENEFICIAL OWNERSHIP INFORMATION

(1). A financial institution or DNFBP must provide information on the beneficial ownership and control, and the source of funds used to pay the capital, of the

financial institution or DNFBP to its regulatory authority prior to applying for a licence, practising certificate, registration or other equivalent permission.

(2). Where a financial institution or DNFBP has obtained a licence, practising certificate, registration or other equivalent permission from its regulatory authority prior to this Act coming into operation, it must, provide information on the beneficial ownership and control, and the source of funds used to pay the capital of, the financial institution or DNFBP to its regulatory authority as soon as reasonably practicable upon this Act coming into operation.

(3). A financial institution or a DNFBP must inform its regulatory authority of any changes to the information provided under subsection (1) or subsection (2) as soon as reasonably practicable.

(4). A person who intentionally engages in conduct that contravenes a requirement of this section is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K500,000.00 or imprisonment for a term not exceeding 5 years or both; or

If the offender is a body corporate - a fine not exceeding K1,000,000.00.

(5). For the purpose of subsection (4), intention can be inferred from objective factual circumstances.

(6). A person who recklessly engages in conduct that contravenes a requirement of this section is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

60. OBLIGATIONS ON REGULATORY AUTHORITIES AND FASU REGARDING BENEFICIAL OWNERSHIP INFORMATION AND FIT AND PROPER CONTROLS

(1). A regulatory authority must ensure that:

(a) it verifies and maintains up to date records of the beneficial ownership and control, and the source of funds used to pay the capital, of the financial institutions or DNFBPs it regulates; and

(b) it makes beneficial ownership and control information of the financial institutions or DNBPs it regulates available to FASU when requested and on a timely basis.

(2). FASU or a regulatory authority must ensure that Directors, Chief Executives, Senior Managers or persons in other equivalent positions in the regulated financial institution or DNFBP and beneficial owners of the regulated financial institution or DNFBP meet fit and proper criteria on an initial and ongoing basis.

(3). For the purpose of subsection (2), fit and proper criteria are those criteria set out by FASU, or the regulatory authority of the financial institution or DNFBP it regulates, in AML/CTF compliance rules, guidelines, forms or other directions as may be appropriate.

PART 6 – SUPERVISION AND ENFORCEMENT

DIVISION 1 – FINANCIAL ANALYSIS AND SUPERVISION UNIT (FASU)

SUBDIVISION 1 – ESTABLISHMENT OF FASU

61. ESTABLISHMENT OF FASU

(1). FASU is established within the Bank of Papua New Guinea.

(2). FASU shall be an operationally independent unit with the functions and powers specified under this Act.

(3). FASU can institute proceedings on behalf of the Bank of Papua New Guinea for the purpose of this Act.

(4). FASU shall be comprised of a Director and officers.

62. STATUS OF THE DIRECTOR

The Director is an officer of the Bank of Papua New Guinea in accordance with the *Central Banking Act* 2000.

63. APPOINTMENT OF THE DIRECTOR

(1). The appointment of the Director must be by written instrument made by the Governor of the Bank of Papua New Guinea, who may, in making the appointment, consult with the following:

(a) the Commissioner of the Police; and

(b) the Departmental Head of the department responsible for national justice administration.

(2). Prior to making an appointment under subsection (1) the Governor of the Bank of Papua New Guinea may also consult with a relevant regulatory authority or government department or agency of Papua New Guinea.

(3). A person is qualified for appointment as the Director of FASU if he:

(a) has relevant and sufficient qualifications, skills and experience to deal with matters of the kind that may be dealt with by FASU;

(b) is of the highest integrity and good reputation; and

(c) has the capacity to maintain the independence of the position of Director.

(4). Any contract or agreement regarding the terms and conditions of the Director's appointment must be consistent with the Director's functions under this Act.

64. TERM OF APPOINTMENT

(1). The Director may be appointed for an initial term that does not exceed five years.

(2). The Director may be reappointed for a second term that does not exceed five years.

(3). After the second term of appointment, a new appointment process must be undertaken for the position of Director.

(4). A person who has previously held the position of Director may apply for that position under the appointment process referred to in subsection (3).

65. DISMISSAL OF THE DIRECTOR

The Director may be dismissed by the Governor of the Bank of Papua New Guinea, who may consult with the following:

(a) the Commissioner of the Police; and

(b) the Departmental Head of the department responsible for national justice administration,

if the Director:

(c) has been found guilty of any criminal offence under the law of Papua New Guinea or a foreign law, whether before, on or after the commencement of this Act;

(d) has breached a term or condition of his or her appointment;

(e) acts in a manner that is grossly prejudicial to the performance of the duties of the office;

(f) is an undischarged bankrupt or insolvent; or

(g) is of unsound mind within the meaning of any law relating to the protection of the person and property of persons of unsound mind.

66. VACANCY OF THE DIRECTOR'S POSITION

(1) The Governor of the Bank of Papua New Guinea must appoint a senior officer of FASU as the Acting Director where:

(a) the Director resigns in writing prior to the expiry of his term of appointment; or

(b) the Director's position becomes vacant for any other reason.

(2) The Director must designate a senior officer of FASU as the Acting Director where the Director takes a temporary leave of absence for any purpose.

(3) An Acting Director can exercise all the powers and functions, and carry out the duties, of the Director under this Act.

(4) The Governor of the Bank of Papua New Guinea must appoint a person as the Director in accordance with sections 63 and 64 as soon as practicable after the Director resigns or his position becomes vacant.

67. OFFICERS OF FASU

(1). Officers of FASU are officers of the Bank of Papua New Guinea in accordance with the *Central Banking Act 2000*.

(2). Notwithstanding subsection (1), officers of FASU are at all times solely under the operational direction and control of the Director in the performance of their duties as officers of FASU.

(3). The Director is responsible for recruiting officers of FASU and may consult with the Governor of the Bank of Papua New Guinea or his delegate and any other appropriate persons with respect to their recruitment.

68. FUNCTIONS AND POWERS OF FASU TO VEST IN THE DIRECTOR

The functions and powers of FASU under this Act are vested in the Director.

69. DUTIES OF THE DIRECTOR

(1). The Director is responsible for implementing the functions and powers of FASU under this Act.

(2). In the exercise of the functions and powers of FASU under this Act, the Director is operationally independent.

70. DELEGATION OF AUTHORITY

(1) The Director may delegate in writing an officer of FASU to exercise any or all of his powers and functions under this Act, other than:

(a) the power of delegation conferred by this section;

(b) the recruitment of officers of FASU under section 67(3); and

(c) a decision to exercise an enforcement power under Division 4 of this Part.

(2) For the avoidance of doubt, the Director may delegate the exercise of particular enforcement powers under Division 4 of this Part to an officer of FASU, provided that the Director does not delegate the decision to exercise such powers.

71. PROTECTION FROM LIABILITY FOR ACTS DONE IN GOOD FAITH

The Bank of Papua New Guinea, FASU, the Director, an officer, employee or agent of FASU, or a person who has been the Director, or who has been an officer, employee or agent of FASU shall not be subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done in good faith in performance of their functions, duties and powers under this Act.

SUBDIVISION 2 – FUNCTIONS OF FASU

72. THE FUNCTIONS OF FASU

(1) The functions of FASU under this Act are to:

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

(b) monitor and enforce compliance with this Act; and

(c) receive reports and information provided to it under Part 2 of the *Proceeds of Crime Act 2005* and disseminate such reports and information in accordance with the *Proceeds of Crime Act 2005* and this Act.

(2) In carrying out its functions under subsection (1), FASU may:

(a) receive, request, collect, analyse and disseminate reports or other relevant information concerning suspected money laundering and associated predicate offences, terrorist financing and proceeds of crime;

(b) develop risk assessments and typology reports in relation to, and raise awareness of, money laundering and terrorist financing and obligations on financial institutions and DNFBPs under this Act;

(c) co-operate with domestic agencies and regulatory authorities and foreign counterpart agencies as provided for under this Act to:

(i) monitor and assess the risk of money laundering and terrorist financing; and

(ii) ensure the effective implementation of this Act.

(d) supervise financial institutions and DNFBPs for the purpose of this Act, including enforcing compliance with this Act;

(e) co-ordinate with other regulatory authorities for the purpose of supervising financial institutions and DNFBPs in enforcing compliance with the obligations under this Act; and

(f) produce AML/CTF compliance rules to assist financial institutions and DNFBPs to comply with their obligations under this Act.

73. FASU MAY PREPARE AML/CTF COMPLIANCE RULES

(1). FASU may prepare an AML/CTF compliance rule.

(2). An AML/CTF compliance rule must be in writing (which includes it being stored electronically).

(3). The purpose of an AML/CTF compliance rule is to provide a statement of practice, guidance or clarification that assists a financial institution or DNFBP to comply with its obligations under this Act.

(4). In preparing an AML/CTF compliance rule, FASU may consult with a relevant regulatory authority or government department, agency or authority of Papua New Guinea, having regard to the subject matter of the proposed AML/CTF compliance rule.

(5). FASU may, in writing, amend or revoke an AML/CTF compliance rule.

(6). The Governor of the Bank of Papua New Guinea must approve in writing an AML/CTF compliance rule, an amendment to a rule and the revocation of a rule.

(7). An AML/CTF compliance rule, or an amendment to or revocation of an AML/CTF compliance rule, comes into operation on the date that it is approved by the Governor of the Bank of Papua New Guinea.

(8). Nothing in subsection (7) precludes an AML/CTF compliance rule, or an amendment to or revocation of an AML/CTF compliance rule, from coming into operation at a date which is specified in the AML/CTF compliance rule.

(9). An AML/CTF compliance rule continues in operation until it is revoked.

(10). FASU:

(a) must publish an AML/CTF compliance rule, and any amendment or revocation of an AML/CTF compliance rule; and

(b) may circulate to all financial institutions and DNFBPs in such other manner as it thinks fit an AML/CTF compliance rule, and any amendment or revocation of an AML/CTF compliance rule

as soon as possible after it is approved by the Governor of the Bank of Papua New Guinea.

74. LEGAL EFFECT OF AN AML/CTF COMPLIANCE RULE

(1). In deciding whether a person has committed an offence under Part 2 or Part 3 of this Act, the court must consider an AML/CTF compliance rule which was in operation at the time of the relevant conduct.

(2). A financial institution or DNFBP complies with an obligation imposed on it under Part 2 or Part 3 of this Act by complying with the provisions of an AML/CTF compliance rule that state a means of satisfying the obligation.

(3). Notwithstanding subsection (2), a financial institution or DNFBP may use means that are different to those specified in an AML/CTF compliance rule to satisfy an obligation under Part 2 or Part 3 of this Act.

75. FASU TO PRODUCE ANNUAL REPORT

(1). FASU must produce and submit an annual report by 30 March of each year to the Board of the Bank of Papua New Guinea.

(2). An annual report must include:

(a) a summary of the activities of FASU;

(b) a summary of reports received by FASU; and

(c) an analysis of current money laundering and terrorist financing trends.

(3). FASU must, as soon as is reasonably practicable after the Board of the Bank of Papua New Guinea has considered the annual report:

(a) provide a copy of the report to the Departmental Head of the department responsible for national justice administration; and

(b) make a copy of the report publicly available.

(4). The publically available report under paragraph (3)(b) must not contain information that refers to or otherwise enables the identification of any particular person.

76. FASU TO MAINTAIN REGISTER OF FINANCIAL INSTITUTIONS AND DNFBPS

FASU must establish and maintain an updated register which includes:

(a) the name of every financial institution and DNFBP which has obligations under this Act;

(b) the address of the principal place of business at which every financial institution or DNFBP carries on its business; and

(c) such other information as may be considered necessary by FASU to identify a financial institution or DNFBP and monitor its compliance with this Act.

77. FASU TO MAINTAIN A DATABASE

FASU must maintain an up to date database containing reports received in accordance with this Act and other relevant information, statistics and records relating to money laundering and terrorist financing.

78. FASU TO DESTROY SUSPICIOUS MATTER REPORTS

FASU must destroy, or make arrangements for the destruction of, any suspicious matter reports received by FASU under section 41(4) or section 52 on the expiry of:

(a) 10 years after the date of receipt of the report if there has been no further activity or information relating to the report of the persons named in the report; or

(b) 10 years from the date of the last activity relating to the person or to the report.

DIVISION 2 – INFORMATION GATHERING AND MONITORING POWERS

79. POWER TO RECEIVE REPORTS AND INFORMATION

For the purpose of carrying out its functions as set out in section 72, FASU may:

(a) receive, request and collect reports and information under subsections 39(1) and (2), 40(1), 41(4), (7) and (11), section 52 and this Part;

(b) receive reports and information under subsections 14(4) and (7), 16(3), 17(3) and 19(4) of the *Proceeds of Crime Act* 2005; and

(c) analyse and disseminate such reports or information received under paragraph (a) in accordance with Division 3 of this Part.

80. POWER TO REQUEST INFORMATION FROM OTHER BODIES

(1) FASU may request, in relation to any report or information it has received under this Act, any information it deems necessary to carry out is functions from:

(a) a regulatory authority;

(b) a law enforcement agency; or

(c) any other government department, agency or authority of Papua New Guinea.

(2) FASU may enter into an arrangement or memoranda of understanding with a regulatory authority, law enforcement agency or any other government department, agency or authority of Papua New Guinea with respect to information sharing and usage.

(3) Any arrangement or memorandum of understanding entered into under subsection (2) must be made in accordance with the requirements of Division 3 of this Part.

81. POWER TO REQUEST INFORMATION AND RECORDS FROM A FINANCIAL INSTITUTION OR DNFBP

(1). For the purpose of monitoring and enforcing compliance with this Act, FASU may request in writing that a financial institution or a DNFBP provide information or produce records in its possession or subject to its control.

(2). FASU may specify the manner in which, and a reasonable period within which, information or records are to be provided.

(3). A request made under subsection (1) may include a continuing obligation to keep FASU informed as circumstances change or on such regular basis as FASU may specify.

(4). Where a request is made for the production of records FASU may:

(a) keep copies of or extracts from any records so produced; and

(b) request any person producing a record to give an explanation of it in writing.

82. DETERMINING IF A PERSON IS A FINANCIAL INSTITUTION OR A DNFBP

(1) For the purpose of monitoring and enforcing compliance with this Act, FASU may, if it believes on reasonable grounds that a person or unincorporated entity is a financial institution or DNFBP that has obligations under this Act, by notice in writing require that person or unincorporated entity to provide any information, or produce any records, relevant to determining whether that person or unincorporated entity is a financial institution or DNFBP within the meaning of this Act.

(2) FASU may specify the manner in which, and a reasonable period within which, information or records are to be provided.

(3) Where a request is made for the production of documents FASU may:

(a) keep copies of or extracts from any record so produced; and

(b) request any person producing a record to give an explanation of it in writing.

83. COMPLYING WITH A REQUEST FOR DOCUMENTS OR INFORMATION

(1) A person required under section 81 or section 82 to disclose any information or produce any record must comply with a request made under section 81 or section 82, regardless of any grounds of confidentiality based on any other Acts or contractual obligations.

(2) For the avoidance of doubt, this section does not affect any privileges under the underlying Law or any Constitutional Law.

84. FAILURE TO COMPLY WITH A REQUEST FOR DOCUMENTS OR INFORMATION

(1) A person who:

(a) refuses to comply with a request for information or records under section 81 or section 82;

(b) produces any record, or gives any information, knowing it is false in any material way, in response to a request for information or records under section 81 or section 82; or

(c) with intent to evade the provisions of section 81 or section 82 destroys, mutilates, defaces, conceals or removes any record

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

(2) For the purpose of subsection (1), intention and knowledge can be inferred from objective factual circumstances.

(3) A person who:

(a) fails within the time and in the manner specified to comply with a request for information or records made under section 81 or section 82; or

(b) produces any record, or gives any information, reckless as to whether it is false in any material way in response to such a request;

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 1 year or both; or

If the offender is a body corporate - a fine not exceeding K200,000.00.

(4) A person does not commit a crime under subsection (1) or (2) if the person:

(a) has a reasonable excuse for their failure to comply with a request under this subdivision; or

(b) relies on a privilege referred to in section 83(2).

85. FASU MAY CONDUCT AN ON-SITE INSPECTION

(1) FASU may conduct an on-site inspection of the premises of, or used by, a financial institution or DNFBP, for the purpose of determining whether the financial institution or DNFBP has complied with, or is complying with, its obligations under this Act.

(2) FASU may request the assistance of a regulatory authority, policeman or other person in conducting an on-site inspection under subsection (1).

(3) Before conducting an on-site inspection under subsection (1):

(a) FASU must provide written notice of the proposed entry prior to or at the time;

(b) the officer of FASU appointed to monitor compliance must identify himself; and

(c) the officer of a regulatory authority, policeman or other person assisting FASU under subsection (2) must identify himself.

(4) For the avoidance of doubt, written notice of the proposed entry may be provided at the time FASU seeks to enter the premises of or used by a financial institution or DNFBP.

86. CONDUCT OF AN ON-SITE INSPECTION

(1) When conducting an on-site inspection under section 85(1) FASU, and any regulatory authority, policeman or other person assisting FASU, may:

(a) inspect the premises to obtain any information, or records or items that are kept at, or accessible from, the premises, that relates to a financial institution's or DNFBP's obligations under this Act; and

(b) take copies, or make videos or audio recordings, of any record, activity or matter that relates to a financial institution's or DNFBP's obligations under this Act.

(2) FASU may request that the occupier of the premises provides FASU, and any regulatory authority, policeman or other person assisting FASU, with such assistance as is reasonably required to conduct an on-site inspection including, but not limited to, the following:

(a) facilitating access to electronic equipment;

(b) unlocking doors, cabinets, drawers and other items;

(c) producing records and items; and

(d) responding to questions about records and items.

(3) FASU must, within a reasonable period after the on-site inspection, restore the premises or cause the premises to be restored as nearly as possible to the same state of cleanliness and neatness that existed immediately before the commencement of the inspection.

(4) For the avoidance of doubt, this section does not affect any privileges under the underlying Law or any Constitutional Law.

87. INSPECTION OF PREMISES PURSUANT TO A WARRANT

(1) A policeman may apply to a court under section 6 of the *Search Act 1977* for a warrant to search the premises of, or used by, a financial institution or DNFBP.

(2) An application for a warrant must be made in accordance with the requirements of Division 2 of Part III of the *Search Act* 1977 and subsection (3) of this section.

(3) An application for a warrant under subsection (1) must also:

(a) specify that there are reasonable grounds for suspecting that there is, on the premises of, or used by, the financial institution or DNFBP:

(i) any record or item in respect of which any offence under this Act has been or is believed on reasonable grounds to have been committed;

(ii) any record or item in respect of which there are reasonable grounds for believing that the record or item is likely to afford evidence of the commission of any offence under this Act; or

(iii) any record or item in respect of which there are reasonable grounds for believing the record or item is intended to be used to commit any such offence under this Act;

(b) specify whether it is sought that an officer of FASU is a named person for the purpose of section 7(a) of the *Search Act 1977;* and

(c) specify whether it is sought that an officer a regulatory authority or any other person is a named person for the purpose of section 7(a) of the *Search Act 1977*.

(4) If it is impracticable for the application to be made in person for reasons of urgency, the application may be made by fax, email or such other means of communication approved by the court.

(5) The application may be heard *ex parte* and may be heard in closed court or in chambers.

(6) The court may issue a warrant if it is satisfied that the requirements of section 6 of the *Search Act 1977* and subsection (3) of this section have been met.

(7) For the purpose of this section, "court" has the meaning given in section 1(1) of the *Search Act 1977*.

(8) For the avoidance of doubt, Part III of the *Search Act 1977* applies to the execution of a warrant issued under this section.

88. REQUIREMENTS REGARDING ENTRY PURSUANT TO A WARRANT

(1) Before conducting a search pursuant to a warrant:

(a) a policeman and any other person named in the warrant must identify themselves to the occupier of the premises, or a person representing the occupier of the premises; and

(b) a policeman must make a copy of the warrant available to the occupier of the premises or a person representing the occupier of the premises.

(2) The occupier of the premises or a person representing the occupier of the premise may observe the execution of the warrant.

89. POWERS THAT CAN BE EXERCISED UNDER THE WARRANT

(1) A warrant authorises a policeman and any other person named in the warrant to exercise the powers under Division 3 of Part III of the *Search Act 1977* in addition to the powers set out in subsection (2).

(2) A policeman and any other person named in the warrant may exercise the following powers when conducting a search pursuant to a warrant:

(a) enter the premises;

(b) search the premises for any records or items that:

(i) are kept at, or accessible from, the premises; and

(ii) relate to a financial institution's or DNFBP's obligations under this Act.

(c) in relation to the records and items referred to in paragraph (b):

(i) search for, and operate, any electronic equipment (including any data storage device) used by a financial institution or a DNFBP for keeping those records or items;

(ii) unlock any doors, cabinets, drawers or other storage facilities that may contain records or items;

(iii) take copies of, or extracts from, those records;

(iv) bring onto the premises such equipment as is reasonably necessary to examine, detect, transport or process records or items that may be found during the exercise of the monitoring powers; and

(v) take any steps which may appear to be necessary for preserving, or preventing interference with, those records or items; and

(d) take photographs or make videos or audio recordings on the premises of any record, item, activity or matter that relates to a financial institution's or DNFBP's obligations under this Act; and

(e) in relation to entry pursuant to a warrant use reasonable force to break into or open:

(i) the premises to which the warrant relates; or

(ii) part of, or anything on, the premises.

(3) In addition to the powers in subsection (1), a policeman can seize a record or item for the purposes of investigation or prosecution of an offence under this Act.

(4) If a record or item is seized under subsection (2), a policeman:

(a) may take possession of, and may make copies of, the record or item, or take extracts from the record;

(b) may retain possession of the record or item for such period as is necessary for the purposes of the investigation to which the record or item relates; and

(c) must provide a copy of that record or item to FASU.

(5) While retaining the record or item, a policeman must allow a person who would otherwise be entitled to inspect the record or item to do so at the times that the person would ordinarily be able to do so.

(6) While retaining the record or item, a policeman must allow a person who would otherwise be entitled to inspect the record or item to do so at the times that the person would ordinarily be able to do so.

(7) If the retention of the record or item by the policeman is not, or ceases to be, reasonably necessary for the purposes of the investigation or a prosecution to which the record or item relates, the policeman must cause it to be delivered to the person who appears to the policeman to be entitled to possession of the record or item.

(8) A policeman must make a record of all documents or things seized under a warrant.

(9) A record or document seized by a policeman under a warrant under this Act is admissible in evidence against a person in criminal proceedings for:

(a) an offence under this Act;

(b) an offence of money laundering or terrorist financing under the Criminal Code; and

(c) an offence under the *United Nations Financial Sanctions Act 2015.*

90. ASSISTANCE IN EXERCISING MONITORING POWERS

A policeman and any other person authorised to execute the warrant may require an occupier of premises to provide such assistance as is reasonably required to execute the warrant including, but not limited to:

(a) facilitating access to electronic equipment; and

(b) unlocking doors, cabinets, drawers and other items.

91. RESTORE PREMISES

The persons authorised to execute the warrant must, within a reasonable period after the conclusion of a search of premises restore the premises or cause the premises to be restored as nearly as possible to the same state of cleanliness and neatness that existed immediately before the commencement of the search.

92. OFFENCE OF OBSTRUCTING THE EXECUTION OF A WARRANT AND TAMPERING WITH OR DESTROYING RECORDS

(1) A person who intentionally prevents, hinders or obstructs the execution of a warrant, including by tampering with or destroying a record is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

(2) For the purpose of subsection (1), intention can be inferred from objective factual circumstances.

93. POWERS TO ASK QUESTIONS AND SEEK PRODUCTION OF RECORDS

(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 to:

(a) answer any questions and produce any records which may be relevant to monitoring compliance or detecting non-compliance with this Act; and

(b) where such records are produced, require the person producing them to provide an explanation of such records.

(2) A statement made by a person in compliance with subsection (1) may be used in evidence against him.

(3) A person requested to disclose any information or produce any record under subsection (1) must comply with a request, regardless of any grounds of confidentiality based on any other Acts or contractual obligations.

(4) For the avoidance of doubt, this section does not affect any privileges under the underlying Law or any Constitutional Law.

(5) A person who:

(a) refuses to comply with a request under subsection (1) to disclose any for information or produce any records

(b) produces any record, or gives any information, knowing it is false in any material way, in response to a request for information or records under subsection (1);

(c) with intent to evade subsection (3) destroys, mutilates, defaces, conceals or removes any record

is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K250,000.00 or imprisonment for a term not exceeding 3 years or both; or

If the offender is a body corporate - a fine not exceeding K500,000.00.

(6) A person who produces any record, or gives any information, reckless as to whether it is false in any material way in response to such a request is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 1 year or both; or

If the offender is a body corporate - a fine not exceeding K200,000.00.

(7) A person does not commit a crime under subsection (1) or subsection (2) if the person:

(a) has a reasonable excuse for their failure to comply with a request under this subdivision; or

(b) relies on a privilege referred to in subsection (4).

DIVISION 3 – USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

94. CONFIDENTIAL INFORMATION

For the purpose of this Division, "**confidential information**" is information supplied to or obtained by FASU in the exercise of its functions and powers under this Act, but does not include:

(a) information which is factually the same as the confidential information and which is already in the public domain; or

(b) information which is presented so that it does not refer to, or otherwise enable the identification of, any particular person.

95. OFFENCE OF DISCLOSING CONFIDENTIAL INFORMATION

(1) An officer of FASU must not disclose confidential information except as permitted under this Division.

(2) A person who intentionally discloses confidential information in contravention of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 1 year or both.

(3) For the purpose of subsection (2), intention can be inferred from objective factual circumstances.

(4) A person who recklessly discloses confidential information in contravention of this Division is guilty of a crime.

Penalty: If the offender is a natural person - a fine not exceeding K50,000.00.

96. CIRCUMSTANCES IN WHICH CONFIDENTIAL INFORMATION MAY BE DISCLOSED

(1) An officer of FASU may disclose confidential information to any regulatory authority or government department, agency or authority for the purpose of:

(a) exercising any of its functions or powers under this Act;

(b) the detection, investigation or prosecution of money laundering, terrorist financing, an offence under section 15 or section 16 of the *United Nations Financial Sanctions Act 2015* or any other indictable offence;

(c) investigations or the taking of action under the *Proceeds of Crime Act* 2005; or

(d) assisting a regulatory authority or government department, agency or authority to exercise its functions or powers.

(2) An officer of FASU may disclose confidential information to a foreign counterpart agency in accordance with section 97.

(3) FASU must immediately provide to the Sanctions Secretariat a copy of a report received under:

(a) subsection 40(1) or section 52; or

(b) subsection 41(4) or section 52, in relation to a suspicion under subsection 41(1)(a) of an offence under section 15 or section 16 of the *United Nations Financial Sanctions Act 2015*.

(4) No person shall be compelled to disclose, in any civil or criminal proceeding, any confidential information relating to:

(a) a suspicious matter report provided under subsection 41(4) or section 52, including information that will identify, or is likely to identify, the person who prepared or made a suspicious matter report; or

(b) information relating to a suspicion provided under subsection 41(7) or (11) or section 52 in relation to communicating a suspicion,

unless the Court is satisfied that the disclosure of the information is necessary in the interests of justice.

97. SHARING CONFIDENTIAL INFORMATION WITH A FOREIGN COUNTERPART AGENCY

(1) FASU may enter into an agreement or arrangement to share confidential information with a foreign counterpart agency, subject to the restrictions on sharing confidential information under section 98.

(2) On the request of a foreign counterpart agency, FASU may:

(a) search its own records;

(b) search other records to which FASU has direct or indirect access, including law enforcement records, public records, administrative records and commercially available records; and

(c) provide information obtained from its search to the foreign counterpart agency subject to the restrictions on sharing confidential information under section 98.

98. RESTRICTIONS ON SHARING CONFIDENTIAL INFORMATION WITH A FOREIGN COUNTERPART AGENCY

(1) FASU may share confidential information with a foreign counterpart agency for the purposes of:

(a) detecting, investigating or prosecuting a foreign indictable offence;

(b) enforcing or taking action under a proceeds of crime law in the foreign counterpart agency's jurisdiction; or

(c) supervising and enforcing compliance with an AML/CTF regulation and supervision law in the foreign counterpart agency's jurisdiction.

(2) FASU may disclose information under subsection (1) only when FASU has obtained written agreement from the foreign counterpart agency that:

(a) the information can only be used for the purpose for which the information was sought; and

(b) the information will not be further disclosed without the consent of FASU.

DIVISION 4 – ENFORCEMENT

99. POSSIBLE ENFORCEMENT MEASURES

(1) FASU may do one or more of the following where it has reasonable grounds to believe that a financial institution or DNFBP has failed to comply with an obligation under this Act:

(a) issue a formal warning under section 100;

(b) issue an infringement notice under section 101;

(c) accept an enforceable undertaking under section 102 and seek an order from a court for breach of that undertaking under section 103;

(d) seek a performance injunction from the Court under section 104

(e) seek a restraining injunction from the Court under section 105; or

(f) publish a notice of non-compliance under section 106.

(2) For the avoidance of doubt, this Act does not affect a power of a regulatory authority to issue, revoke, impose conditions upon or amend the conditions of a licence, practising certificate, registration or other equivalent permission granted to a financial institution or DNFBP by that regulatory authority or to exercise any of its other powers or functions.

100. FORMAL WARNING

(1) FASU may issue a formal warning to a financial institution or DNFBP where FASU has reasonable grounds to believe that the financial institution or DNFBP has engaged in conduct that has contravened a requirement of this Act.

(2) A formal warning may specify any remedial action that FASU believes the financial institution should take.

(3) FASU may publish a formal warning issued to the financial institution or DNFBP.

101. INFRINGEMENT NOTICE

(1) FASU may serve an infringement notice in writing to a financial institution or DNFBP where FASU has formed the view based on reasonable grounds to believe that the financial institution or DNFBP has engaged in, or may engage in, conduct which constitutes an offence under this Act.

(2) If FASU intends to issue an infringement notice, it must do so as soon as possible after it has become aware that the financial institution or DNFBP has engaged in, or may engage in, conduct which constitutes an offence under this Act.

(3) The infringement notice must require the financial institution or DNFBP to pay a penalty prescribed in the notice within 30 days of the date the notice was served.

(4) A prescribed penalty must not exceed:

(a) K1,000.00 for an individual; or

(b) K5,000.00 for a body corporate.

(5) FASU may publish an infringement notice issued to the financial institution or DNFBP.

(6) A financial institution or DNFBP on whom an infringement notice has been served under Subsection (1) and payment of which remains outstanding after the completion of the 30 day period, shall pay, in addition to the penalty, interest at the rate of 8% of the amount of unpaid penalty for each 5 day period or part thereof, beginning on the day after the notice was served on the financial institution or DNFBP and ending on the day the penalty has been paid in full.

(7) Where FASU serves an infringement notice under Subsection (1), a prosecution in respect of that offence may only be commenced if the penalty remains unpaid 30 days after payment was due, and the Court may take account of any unpaid penalty and interest accrued when imposing a penalty in respect of such action.

102. ENFORCEABLE UNDERTAKING

(1) FASU may request a written undertaking from a financial institution or DNFBP in connection with compliance with this Act.

(2) Without limiting subsection (1), a written undertaking may relate to an activity of a financial institution or DNFBP or to an officer, employee, agent, or a group of officers, employees or agents of the financial institution or DNFBP.

(3) A financial institution or DNFBP may give FASU a written undertaking in connection with compliance with this Act.

(4) For the avoidance of doubt, the terms of an undertaking must be lawful and in compliance with this Act.

103. ENFORCEMENT OF UNDERTAKING

(1) Where FASU considers that a financial institution or DNFBP has breached one or more of the terms of an undertaking it provided under section 102, FASU may apply to the Court for an order under subsection (2).

(2) If the Court is satisfied that:

(a) the financial institution or DNFBP has breached one or more of the terms of its undertaking; and

(b) the undertaking was relevant to the financial institution's or DNFBP's obligations under this Act

the Court may make an order directing the financial institution or DNFBP to comply with any of the terms of the undertaking.

104. PERFORMANCE INJUNCTIONS

(1) FASU may apply to the Court for an injunction requiring a person to do an act or thing in order to comply with this Act.

(2) Further to an application under subsection (1), the Court may grant an injunction requiring a person to do an act or thing under this Act if it is satisfied that:

(a) a person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do an act or thing; and

(b) the refusal or failure was, is or would be a contravention of this Act;

(3) An injunction granted by the Court under subsection (2) may relate to an officer, employee or agent, or a group of officers, employees or agents of the financial institution or DNFBP.

(4) An application made under subsection (1) may be made *ex parte* and the Court may grant an injunction under subsection (2) on an interim basis without the defendant being heard when the Court considers it appropriate to do so.

105. RESTRAINING INJUNCTIONS AND INTERIM RESTRAINING INJUNCTIONS

(1) FASU may apply to the Court for an injunction restraining a person from engaging in conduct in contravention of this Act.

(2) Further to an application under subsection (1), the Court may grant an injunction restraining a person from engaging in conduct in contravention of this Act if it is satisfied that:

(a) a person has engaged, is engaging or is proposing to engage, in any conduct; and

(b) the conduct was, is or would be a contravention of this Act.

(3) An injunction under subsection (2) may relate to an officer, employee or agent, or a group of officers, employees or agents of the financial institution or DNFBP.

(4) An application made under subsection (1) may be made *ex parte* and the Court may grant an inunction under subsection (2) on an interim basis without the defendant being heard when the Court considers it appropriate to do so.

106. NOTICE OF NON-COMPLIANCE

(1) Where the Court has granted an injunction under section 104 or section 105, FASU may publish a notice which sets out the details of the financial institution's or DNFBP's non-compliance, and any remedial action ordered by the Court.

(2) Where a financial institution or DNFBP has failed to comply with an injunction granted by the Court section 104 or section 105, FASU may publish a notice of that non-compliance and any other remedial action as ordered by the Court.

PART 7 – MISCELLANEOUS

107. CONDUCT BY DIRECTOR, SERVANT OR AGENT

(1) For the purpose of this Act, the state of mind of a person may be established in accordance with this section.

(2) Conduct engaged in for a body corporate is taken, for this Act, to have been engaged in by the body corporate if it was engaged in:

(a) by a director, servant or agent of the body corporate within the scope of his or her actual or apparent authority; or

(b) by another person, if:

(i) it was done at the direction or with the consent or agreement (whether express or implied) of a director, servant or agent of the body corporate; and

(ii) giving the direction, consent or agreement was within the scope of the actual or apparent authority of the director, servant or agent.

(3) To establish the relevant state of mind for conduct engaged in, or taken under subsection (2) to have been engaged in, by a body corporate, it is sufficient to show that a director, servant or agent of the body corporate who engaged in the conduct within the scope of his or her actual or apparent authority had that state of mind.

(4) Conduct engaged in for a person (other than a body corporate) is taken, for this Act, to have been engaged in by the person if it was engaged in by:

(a) a servant or agent of the person within the scope of the servant or agent's actual or apparent authority; or

(b) by another person at the direction or with the consent or agreement (whether express or implied) of a servant or agent of the first-mentioned person, if the giving of the direction, consent or agreement is within the scope of the actual or apparent authority of the servant or agent.

(5) To establish the relevant state of mind for conduct taken, under subsection (4), to have been engaged in by a person (other than a body corporate), it is sufficient to show that a servant or agent of the person who engaged in the conduct within the scope of his or her actual or apparent authority had that state of mind.

(6) A reference in this section to the state of mind of a person includes the person's knowledge, intention, opinion, belief or purpose, and the person's reasons for that intention, opinion, belief or purpose.

108. POWER TO MAKE REGULATIONS

The Head of State, acting on advice, may make regulations not inconsistent with this Act prescribing all matters which are by this Act required or permitted to be prescribed or necessary or convenient to be prescribed for giving effect to this Act.

109. CONSEQUENTIAL AMENDMENTS

(1) The definitions of "cash dealer" and "FIU" in subsection 3(1) of the *Proceeds of Crime Act 2005* are repealed.

(2) Sections 13 to 30, 36 and 37 of the *Proceeds of Crime Act 2005* are repealed.

110. TRANSITIONAL AND SAVING PROVISIONS

(1). Despite the repeal of the definitions of "cash dealer" and "FIU" in subsection 3(1), and the repeal of sections 13 to 30, 36 and 37, of the *Proceeds of Crime Act 2005* by this Act, these sections continue to apply after the commencement of this Act in relation to:

(a) an offence committed before the commencement of this Act; or

(b) proceedings for an offence alleged to have been committed before the commencement of this Act; or

(c) any matter connected with, or arising out of such proceedings

as if the repeal had not been made.

(2). Despite the repeal of the definition of "minimum retention period" in section 19, and the repeal of section 28, of the *Proceeds of Crime Act 2005* by this Act, a

financial institution and DNFBP who was required to retain records under those sections must continue to retain those records in accordance with section 28 for the minimum retention period specified in section 19 the *Proceeds of Crime Act*.

(3). Upon the coming into operation of this Act, any reports provided to the Financial Intelligence Unit under sections 13, 14, 23 and 24 of the *Proceeds of Crime Act 2005* will come under the possession and control of FASU.