CENTRAL BANK of BELIZE

ANTI-MONEY LAUNDERING
COMBATING THE FINANCING OF TERRORISM
AND
COUNTER-PROLIFERATION FINANCING
(AML/CFT/CPF) GUIDELINES
FOR
CENTRAL BANK - REGULATED INSTITUTIONS

CENTRAL BANK OF BELIZE
GABOUREL LANE
BELIZE CITY
BELIZE

DECEMBER 2023

ANTI -MONEY LAUNDERING COMBATING THE FINANCING OF TERRORISM AND COUNTER-PROLIFERATION FINANCING (AML/CFT/CPF) GUIDELINES FOR CENTRAL BANK-REGULATED INSTITUTIONS

DECEMBER 2023

TABLE OF CONTENTS

INTRODUCTION

Within the financial sector, systems must continuously be strengthened to deter illicit activities and their related offences. More emphasis must be applied to detecting attempts to launder money and finance terrorism. Given that these activities go beyond borders, Belize has joined many other countries in the world in recognizing the importance of strengthening capacity to discourage illicit activities in this jurisdiction, being mindful of international standards and best practices.

The Central Bank of Belize (Central Bank) is issuing the Anti-Money Laundering, Combating the Financing of Terrorism and Counter-Proliferation Financing Guidelines (AML/CFT/CPF Guidelines) in its capacity as Supervisory Authority for entities as captured in the Third Schedule of the Money Laundering and Terrorism (Prevention) Act (MLTPA), and in accordance with Section 21(2)(b) of the MLTPA., The Central Bank is hereby providing guidance to banks, financial institutions, credit unions, moneylenders including pawnbrokers, payment service providers including remittance service providers and e-wallets, and payment service operators that fall under its regulatory umbrella, with a view to strengthening the compliance functions of the relevant institutions.

These Guidelines replace the previously issued AML/CFT Guidelines, 2010.

SCOPE

These Guidelines are sector specific and must be viewed in collaboration with the MLTPA and accompanying Regulations. These Guidelines set the expectations of the Central Bank for the minimum standards of anti-money laundering/combating the financing of terrorism/counter-proliferation financing (AML/CFT/CPF) practices by all financial institutions. Toward this end, financial institutions should integrate AML/CFT/CPF measures as an integral part of their risk management strategies. Notably, these Guidelines form a key component of the framework used to evaluate how financial institutions implement their AML/CFT/CPF policies.

These Guidelines draw on the principles contained in the Financial Action Task Force[1] (FATF) Recommendations. It encapsulates concepts from various papers on related topics as set out by the Basel Committee on Banking Supervision, as well as incorporates local AML/CFT/CPF legislation.

APPLICATION

Banks, financial institutions credit unions, moneylenders (including pawnbrokers), payment service providers (including remittance services and E-wallets), and payment system operators should apply adequate resources to mitigate the risks involved in transacting the proceeds of illicit activities. All banks and financial institutions licensed under the Domestic Banks and Financial Institutions Act (DBFIA), International Banking Act (IBA), credit unions registered under the Credit Unions Act (CUA), moneylenders licensed under the Moneylenders Act (MLA) and payment service providers, and payment system operators, licensed under the National Payment System Act (NPSA) are obligated to comply with these Guidelines, which contain both advisory and obligatory requirements. Advisory matters are expressed using the term “may”. This allows financial institutions to implement alternative but just as effective measures in some circumstances. On the

[1] FATF is an inter-governmental body which sets standards, develops and promotes policies to combat ML/TF/PF.

other hand, institutions are not to divert from mandatory requirements which are expressed using the term "should".

These Guidelines apply to all financial institutions in Belize that are licensed under the DBFIA, IBA, MLA, and NPSA and registered under the CUA. These institutions are referred to as "financial institutions" throughout these Guidelines. Financial institutions should ensure that, at a minimum, these Guidelines are also implemented in their branches and subsidiaries abroad, where applicable. Where standards in the host country are considered more rigorous, then institutions should abide by the higher standards. In the case of subsidiaries abroad, a financial institution should inform the Central Bank if the local applicable laws and regulations prohibit implementation. General references to ML should be interpreted to include ML terrorist financing (TF) and/or proliferation financing (PF).

INTERPRETATION

1. Any term used in these Guidelines that is not defined herein carries the meaning as per the relevant legislation. Unless otherwise stated, the following terms appearing in these Guidelines should be applied to mean:

Bearer Shares	-	Negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.
Close Associate	-	Any individual who is widely and publicly known to maintain an unusually close relationship with a politically exposed person (PEP) and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of a PEP. For the purpose of deciding whether a person is a known close associate of a PEP, a financial institution need only have regard to any information which is in its possession, or which is publicly known.
Competent Authority	-	A public authority with designated responsibilities for combating money laundering or terrorist financing or proliferation financing ML/TF/PF, including the Financial Intelligence Unit (FIU) and supervisors the Attorney General or any authority responsible for international cooperation.
Customer Due Diligence	-	The care a reasonable person should take before entering into an agreement or transaction with another party. It includes not only establishing the identity of customers, but also monitoring account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account.
Facility	-	Any account or arrangement which is provided by a financial institution to a facility holder which may be used by the facility holder to conduct two or more transactions. It specifically includes provision for safe custody, including safety deposit boxes.
Facility Holder	-	A person in whose name the facility is established and includes any person to whom that facility is assigned or who is authorized to conduct transactions through that facility.
Financial Institution	-	Entities in Belize that are licensed under the DBFIA and IBA, MLA, credit unions registered under the CUA and payment service providers and payment system providers licensed under the National Payment Systems Act. (**See Appendix 1**)

Immediate Family	-	The parents, grandparents, siblings, spouse, children, grandchildren, and in-laws of the person who has been designated.
Intermediary	-	A financial institution, such as a bank, that acts as a conduit between suppliers of funds (depositors) and users of funds (borrowers).
Occasional Transaction	-	Any one-off transaction including, but not limited to, cash that is conducted by a person without an account or facility at the financial institution.
Payable-through Accounts	-	Correspondent accounts that are used directly by third parties to transact business on their own behalf.
Person	-	A natural person or a legal person and includes, among others, a corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture, or other unincorporated organization or group, capable of acquiring rights or entering into obligations.
Politically Exposed Persons	-	Individuals in Belize or in a foreign country entrusted with public functions, their family members, or close associates.
Reporting Entity	-	A person whose regular occupation/business is the carrying on of any activity listed in the First Schedule of the MLTPA or any other activity defined by the Minister.
Remittance Services Providers	-	Money remittance companies; check cashers; issuers, sellers and redeemers of money orders and travelers cheques; currency exchange houses and stored value product companies. These businesses accept cash, cheques, other monetary instruments, or stored value in one location and payment of a corresponding sum in cash or other form to a beneficiary is made in another location by means of a communication, message, transfer or through a clearing network to which the money transfer business belongs. This excludes the sale of postal money orders by the Post Office. Remittances may be domestic or international.
Remittance Agent	-	A person carrying on money transfer services on behalf of a money transfer service provider.
Senior Political Figure	-	A senior figure in the executive, legislative, administrative, military, or judicial branches of a government, political party, or a senior executive of a government-owned corporation. It includes any corporate entity, partnership or

		trust relationship that has been established by, or for the benefit of a senior political figure.
Settlors	-	Persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.
Shell Bank	-	A bank incorporated in a jurisdiction in which it has no physical presence, and which is unaffiliated with a regulated financial group.
Source of Funds	-	Description of the origin and the means of transfer for monies that are accepted for the account opening and/or subsequent transfers to the account.
Source of Wealth	-	The means through which a customer acquires his wealth (e.g., through a business or an inheritance).
Supervisors	-	The designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat ML/TF.
Third Party	-	An individual or other entity who is not a direct party to a contract, agreement, or transaction but who somehow has an interest in or is affected by it.

ACRONYMS AND ABBREVIATIONS

AML	-	Anti-Money Laundering
AML/CFT	-	Anti-Money Laundering/Combating the Financing of Terrorism
AML/CFT/CPF	-	Anti-Money Laundering/Combating the Financing of Terrorism and Combating Proliferation Financing
AML/CFT/CPF Guidelines	-	Anti-Money Laundering, Combating the Financing of Terrorism and Counter-Proliferation Financing Guidelines
DBFIA	-	Domestic Banks and Financial Institutions Act
CDD	-	Customer Due Diligence
Central Bank	-	Central Bank of Belize
CUA	-	Credit Unions Act
EDD	-	Enhanced Due Diligence
FATF	-	Financial Action Task Force
FIU	-	Financial Intelligence Unit
IBA	-	International Banking Act
KYC	-	Know Your Customer
KYE	-	Know Your Employee
ML	-	Money Laundering
MLA	-	Moneylenders Act
ML/TF/PF	-	Money Laundering, Terrorist Financing and Proliferation Financing
MLRO	-	Money Laundering Reporting Officer
MLTPA	-	Money Laundering and Terrorism (Prevention) Act
NAMLC	-	National Anti-Money Laundering Committee
NPM	-	New Payment Method

NPO	-	Non-Profit-Organization
NPSA	-	National Payment Systems Act
NRA	-	National Risk Assessment
OFAC	-	Office of Foreign Assets Control
PEP	-	Politically Exposed Person
RBA	-	Risk Based Approach
RSP	-	Remittance Service Provider
SDD	-	Simplified Due Diligence
SOF	-	Source of Funds
STR	-	Suspicious Transaction Report
SWIFT	-	Society for Worldwide Interbank Financial Telecommunication
TF	-	Terrorist Financing
UBO	-	Ultimate Beneficial Owner
UK	-	United Kingdom
UN	-	United Nations
UNSCRs	-	UN Security Council
UTR	-	Unusual Transaction Report

SECTION I - BACKGROUND

1.1 Money Laundering Defined

2. Money laundering (ML) is the process of disguising the source and ownership of money or assets derived from criminal activity to make it appear to have originated from a legitimate source. If undertaken successfully, it allows criminals to maintain control over illicit funds and, ultimately, to provide a legitimate cover for their source of income.

3. A person guilty of ML is punishable, upon conviction, with a fine and/or imprisonment **(see Appendix 4)**.

1.2 Stages of Money Laundering

4. ML may be accomplished through different methods, ranging from purchasing and reselling of luxury assets (such as cars, yachts, artwork or precious metals and stones), to passing money through a complex international web of legitimate businesses and "shell" companies. The criminal's objective in laundering illicit proceeds is to conceal the origin and the ownership of the funds, change the form of the money to recycle it into the economy, and control the movement of the funds to avoid detection.

5. Regardless of the methods utilized, certain points of vulnerability have been identified in the laundering process, which the money launderer finds difficult to avoid. Accordingly, entry of cash into the financial system, cross-border flows of cash and transfers within and from the financial system are activities more predisposed to being recognized through vigilance on the part of the financial institution.

6. The launderer's effort to transform "dirty" money into "clean" money involves the following three stages which may occur separately, simultaneously, or overlap:

i. **Placement** is the physical introduction of cash derived from criminal activity into the financial system.

The objective of this is to convert funds from cash to a financial instrument, such as a bank account or insurance product, in an effort to place the proceeds of crime into the financial system. Techniques such as purchasing and reselling high value goods for payment by cheque or bank transfer, structuring deposits to evade reporting requirements or co-mingling deposits of legal and illegal activities are some of the ways used to accomplish this.

ii. **Layering** is the separation of illicit proceeds from their source by moving them around the financial system, often in complex layers of transactions to create confusion, complicate the audit trail and sever links with the original crime.

Methods used to accomplish this include converting cash into monetary instruments, investing in real estate and other legitimate businesses, transferring deposited funds from one account to another or transferring funds abroad using shell companies.

iii. **Integration** is the attempt to attach legitimacy to illicit wealth by re-entry of the funds into the economy. If placement and layering is successful, the criminally derived proceeds appear as legitimate funds or assets.

At this stage, it is difficult to differentiate legitimate and illegitimate wealth.

1.3 Terrorism or Terrorist Act Defined

7. Terrorism is, *inter alia*, any act, in or outside Belize, which is intended to intimidate the public or coerce a government or international organization to comply with the demands of terrorists and which is intended to cause death or serious bodily harm to a person, serious risk to public health or safety, damage to property or interference with or disruption of essential services or systems, or to advance or achieve a political, ideological or religious cause.

8. A person guilty of terrorism is punishable, upon conviction, with a fine and/or imprisonment **(see Appendix 4)**.

1.4 Financing of Terrorism

9. A notable difference between ML and TF is that while ML seeks to legitimize money from illegal sources, TF may come from both legal and illegal sources. Furthermore, terrorist financing transactions may appear normal, as the sums used to finance such causes are not always large and the associated transactions are not necessarily complex.

10. TF may be derived from criminal activities such as kidnapping, extortion, fraud, or drug trafficking. On the other hand, it may also be derived from legitimate sources such as membership dues, sale of publications or income from legitimate business operations owned by terrorist organizations.

11. The methods used by terrorist organizations (e.g., cash smuggling, structuring, wire transfers, purchase of monetary instruments, and use of debit and credit cards) to move, collect, hide, or make funds available are like those utilized by criminal organizations, especially when funds are from illegitimate sources. Regardless of the source, terrorist organizations usually seek to obscure or disguise the links between the organization and the funds.

12. The financing of terrorism is listed as a serious offence under the Second Schedule of the MLTPA. Under the MLTPA, the Director of FIU has powers to direct those accounts held on behalf of terrorists or terrorist organizations to be frozen. Applications may also be made by the FIU or the Director of Public Prosecutions to the Supreme Court for the forfeiture of terrorist property.

1.5 Proliferation Financing Defined

13. Proliferation financing (PF) is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials. This includes both technologies and dual use goods dual use goods used for non-legitimate purposes.

1.6 Vulnerability of Banks and Financial Institutions to Money Laundering

14. Efforts to combat ML should focus on those points in the process where the launderer's activities are more easily recognized. In the case of banks and other deposit-taking financial institutions, these efforts should be concentrated on the deposit-taking procedures, that is, the placement stage. In those cases where cash is not involved, staff should be aware of the more sophisticated schemes that may be utilized by launderers to place their dirty money. A financial institution should consider the ML risks posed by the products and services they offer, as well as prospective products and services to be offered, particularly where face-to-face contact with a customer is not required. AML procedures

should be devised bearing such risks in mind.

15. The most common form of ML that financial institutions will encounter involve the accumulation of cash transactions which will be deposited in the financial system or used to acquire assets. Electronic funds/(wire) transfer systems increase vulnerability since cash deposits can be switched rapidly between accounts in different names or different jurisdictions.

16. Because of the large range of services provided by financial institutions, they may be used in the layering and integration stages as well. For instance, mortgage and other loan accounts may be used to create complex layers of transactions.

1.7 Tipping-Off

17. It is an offence under the MLTPA for a person who knows or suspects that an investigation into ML was, is, or will be conducted, to divulge such information if in doing so, the investigation is likely to be prejudiced. Tipping-off is punishable by fines and/or imprisonment upon conviction **(see Appendix 4)**.

18. Initial inquiries to verify the identity of a customer and ascertain the source of funds or other relevant information to understand the nature of a transaction do not constitute tipping-off. However, where a financial institution suspects that a transaction relates to ML/TF and it is believed that performing customer due diligence (CDD) measures may tip-off the customer or potential customer to that suspicion, that reporting entity shall not perform the CDD measures.

19. Where a financial institution is unable to perform CDD, file the necessary disclosure with the FIU.

20. Where it is known or suspected that a suspicious transaction report (STR) has been filed with the FIU, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.

1.8 International Initiatives

21. Standard setters, such as the Basel Committee on Banking Supervision and FATF, set out a comprehensive and consistent framework of measures which countries should implement to combat ML/TF, as well as the financing of proliferation of weapons of mass destruction (PF). This internationally accepted framework includes the FATF Recommendations, supported by subsequently issued guidance covering a range of topics including:

i. Guidance on Correspondent Banking;

ii. Guidance on Proliferation Financing Risk Assessment and Mitigation;

iii. Guidance on Digital ID;

iv. Terrorist Financing Risk Assessment Guidance;

v. AML/CFT Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence;

vi. AML/CFT Guidance - Private Sector Information Sharing;

vii. Guidance on Transparency and Beneficial Ownership;

viii. Risk-Based Approach for the Banking Sector;

ix. AML/CFT Guidance: Politically Exposed Persons (Recommendations 12 and 22);

x. Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments, and Internet-Based Payment Services;

xi. Revised Guidance on AML/CFT and Financial Inclusion; and

xii. FATF Guidance on Proliferation Financing Risk Assessment and Mitigation.

1.9 Legislative and Regulatory Framework

22. Belize's commitment to fight the harmful effects of money laundering, terrorist financing, proliferation financing (ML/TF/PF) and their related offences is manifested in the following legislations and agreements aimed at suppressing crimes:

i. Prevention of Corruption Act Chapter 105, Revised Edition 2011

ii. Prevention of Corruption in Public Life Act, 2000 CAP 12;

iii. Financial Intelligence Unit Act Chapter 138:02, Revised Edition 2020

iv. Convention on the Suppression of the Financing of Terrorism ratified in 2003;

v. Caribbean Treaty on Mutual Legal Assistance in Serious Criminal Matters Act, 2005 (No. 47 of 2005);

vi. Mutual Legal Assistance in Criminal Matters (Belize/USA) Act 2005 (No. 10 of 2005);

vii. Security Council Resolution 1617 (2005) (Enforcement) Order, 2006 (S.I. No. 32 of 2006);

viii. Money Laundering and Terrorism (Prevention) (National Anti-Money Laundering Committee) Regulations, 2014; and

ix. Money Laundering and Terrorism (Prevention) Act CAP 104, Revised Edition 2023.

1.10 Penalties for Non-Compliance

Various penalties can be imposed on a financial institution, bodies of persons, as well as individuals, for non-compliance with requirements of the AML/CFT/CPF legal framework. Penalties range from a written warning to imprisonment for ten years to life. Penalties also include possible seizure of property or sanctions imposed by the supervisory authority including suspension, restriction, or revocation of license.

Administrative penalties in an amount not exceeding BZ$500,000 may also be applied. A financial institution should therefore be vigilant and aspire to operate within the confines of the laws.

1.11 Enforceability of this Guideline

23. Section 21 of the MLTPA, empowers the Central Bank to issue guidelines to assist banks, financial institutions, credit unions, moneylenders including pawnbrokers, payment service providers (remittance service providers and e-wallets) and payment system providers to comply with the MLTPA or any other written law relating to AML/CFT/CPF.

24. Pursuant to section 22 of the MLTPA, the Central Bank can issue compliance directions to ensure adherence with this Guideline. It also allows the Central Bank to issue compliance directions to an agent, or its controllers or officers for breaching any written law, including AML/CFT/CPF laws.

25. Failure to comply with this guideline may result in an administrative penalty issued in accordance with section 22 of the MLTPA.

1.12 The Role of the National Anti-Money Laundering Committee

26. Section 77B of the MLTPA provides for the National Anti-Money Laundering Committee (NAMLC) to be established. NAMLC meets as often as may be necessary and advises the Minister of Finance on:

i. Detecting and preventing of ML/TF/PF;

ii. Developing a national plan of action to include recommendations on effective mechanisms to enable supervisory and law enforcement authorities to coordinate in Belize;

iii. Participating in international efforts against ML/TF/PF; and

iv. Developing policies to combat ML/TF/PF.

27. The members of the National Anti-Money Laundering Committee are:

i. the Director of the FIU, who shall be the Chairman;

ii. the Solicitor General or his representative;

iii. the Financial Secretary or his representative;

iv. the Chief Executive Officer of the Ministry responsible for the Police Department or his representative;

v. the Commissioner of Police or his representative;

vi. the Governor of the Central Bank of Belize or his representative;

vii. the Director of Public Prosecutions or his representative;

viii. the Comptroller of Customs or his representative;

ix. the Director of Immigration or his representative;

x. the Supervisor of Insurance or his representative;

xi. the Director General of the Financial Services Commission or his representative;

xii. the Director General of the Belize Tax Service or his representative; and

xiii. such other persons as the Ministry may, from time to time, appoint.

1.13 The Role of the Financial Intelligence Unit

28. The FIU is the leading AML Competent Authority and the ML Supervisory Authority in Belize. Its responsibilities shall include:

i. Investigating and prosecuting financial crimes;

ii. Ensuring coordination and cooperation between law enforcement agencies, Government departments, regulatory authorities, private institutions and members of relevant professions in methods and policies to prevent financial crimes;

iii. Sharing of examination or supervision information with the appropriate law enforcement authorities, if the FIU has reasonable grounds to suspect that a transaction involves the proceeds of crime, terrorism, or proliferation.

iv. Instructing any reporting entity to take such steps as may be appropriate including the freezing of funds and other financial assets or economic resources of any person or entity, to facilitate any investigation, prosecution or proceeding for a ML or TF offence whether in Belize or elsewhere;

v. Providing legal assistance to foreign jurisdictions with respect to property tracking, monitoring and forfeiture or freezing orders;

vi. Sharing of information and cooperating with foreign FIUs;

vii. Dealing with requests for legal assistance from foreign countries, law enforcement agencies and other regulatory bodies relating to financial crimes, property tracking, monitoring and forfeiture or freezing orders;

viii. Receiving, analyzing and assessing reports of suspicious transactions issued by reporting entities;

ix. Taking appropriate action or forwarding relevant information to the appropriate law enforcement authorities if reasonable grounds exist to suspect that the transaction involves proceeds of crime or terrorist financing;

x. Consulting with NAMLC and having regard to objective information available on countries that do not, or do not adequately apply FATF Recommendations, determine the countries in which an intermediary, introducer or third party that meets the conditions referred to in the MLTPA can be based;

xi. Compiling statistics and records, disseminating information in Belize and elsewhere as provided for by law, making recommendations based on any information received, issuing guidelines to reporting entities and advising the Minister accordingly;

xii. Creating training requirements and providing such training for any reporting entity as regards identification, record-keeping and reporting obligations under the MLTPA;

xiii. Requesting information from reporting entities, supervisory authorities, law enforcement agencies and other domestic agencies, for purposes of the MLTPA, without the need for agreements or arrangements as per section 11 of the MLTPA;

xiv. Providing periodical feedback to reporting entities, supervisory authorities, and other relevant agencies; and

xv. Entering the premises of any reporting entity during ordinary business hours to inspect records, ask questions, make notes, and take copies of such records, in exercising powers relating to the supervisory authority's role of ensuring compliance as set out in Section 21 of the MLTPA.

29. The FIU's responsibilities may also include:

i. Conducting research into trends and developments in the area of ML and TF. Research may also cover improved ways of detecting, preventing and deterring ML/TF/PF;

ii. Conducting necessary actions including research, consultation with or requesting information from any person, to assess the risk to Belize related to ML/TF/PF;

iii. Educating the public and creating awareness on matters relating to ML/TF/PF;

iv. Consulting with any relevant person, institution or organization in the exercise of its powers or duties under paragraph 27, as mentioned above;

v. Disclosing any report, information derived there-from or any other information it receives, to an agency of a foreign state or international organization with duties similar to those of the FIU if reasonable grounds are established to suspect that such information would be relevant to investigating proceeds of crime or investigating or prosecuting a serious crime;

vi. Disclosing any report to the supervisory authority to ensure compliance with the MLTPA; and

vii. Entering into agreements or arrangements with any domestic government institution or agency with respect to the exchange of information.

30. In instances where a financial institution is unsure of how to proceed with an unusual or suspicious transaction, it should liaise directly with the FIU for guidance and then make the appropriate report. Where the FIU believes, on reasonable grounds, that a transaction involves the proceeds of crime, the FIU will send a report for further investigation to the Director of Public Prosecutions, the Police Department, and any other appropriate authority.

1.14 The Role of the Central Bank of Belize

31. The Central Bank has been designated the supervisory authority for various financial institutions as listed in the Third Schedule of the MLTPA. The responsibilities of the Central Bank shall include:

i. Conducting onsite examinations or using other means to supervise and regulate particular reporting entities to ensure compliance with the obligations set out in the MLTPA;

a. By virtue of the DBFIA, IBA and CUA, the Central Bank has the power to compel the production of or to obtain access to all records, documents, or information relevant to monitoring compliance. This includes all documents or information related to accounts or other business relationships or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions. A court order shall not be necessary to facilitate production of such information;

ii. Issuing instructions, guidelines or recommendations to assist particular reporting entities to comply with the MLTPA;

iii. Developing national and internationally accepted standards applicable to reporting of suspicious activities;

iv. Imposing requirements for reporting entities to ensure that their foreign branches and subsidiaries adopt and enforce measures consistent with the MLTPA; where foreign branches or subsidiaries are unable to adopt and observe these measures, reporting entities should inform the designated supervisory authority or competent disciplinary authority. Towards this end,

a. financial institutions should pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply FATF Recommendations; and

b. where the minimum AML/CFT/CPF requirements of the home and host countries differ, branches and subsidiaries in host countries should apply the higher standard, to the extent that host country laws and regulations permit;

v. Submitting a report to the FIU of suspected suspicious transactions, activities or facts that may be related to ML, TF, PF or the proceeds of crime no later than within three working days;

vi. Cooperating with agencies performing similar functions, including exchange of information, in other countries;

vii. Adopting necessary measures to establish fit and proper criteria for owning, controlling or participating (whether directly or indirectly) in the directorship, management or operation of a financial institution;

viii. Imposing sanctions, as set out in Section 22(1) of the MLTPA, on reporting entities, select officers, and controlling owners that breach obligations established under the MLTPA;

ix. Maintaining statistics of measures adopted and sanctions imposed in enforcing the MLTPA, including keeping annual statistics of onsite examinations conducted;

x. Informing the FIU of sanctions imposed on reporting entities; and

xi. Informing the FIU upon the discovery of facts likely to constitute indication of ML/TF/PF.

32. Through periodic onsite examinations, the Central Bank, in its capacity as the supervisory and regulatory authority for financial institutions licensed or registered under the DBFIA, IBA, or CUA, will assess a financial institution's framework and compliance. Towards this end, identified deficiencies in policy or operations should be addressed by the financial institution within a specific timeframe as agreed to by the Central Bank. Depending on the gravity of non-compliance and/or the lack of responsiveness to previous findings, the Central Bank may enforce its powers under the DBFIA or the IBA. Furthermore, the Central Bank may instruct a financial institution to file an STR where the situation necessitates, provided that the financial institution has not yet filed such a report.

33. Accessing relevant reports and working papers prepared in the external and internal audit process, to evaluate adherence to know your customer (KYC) standards.

34. As home country supervisor, the Central Bank should have access to information on individual customer accounts to the extent necessary to enable proper evaluation of the application of KYC standards and an assessment of risk management practices.

35. The Central Bank should not be impeded by local bank secrecy laws from accessing information required to properly perform its functions to combat ML/TF/PF. In fulfilling its role as Supervisory Authority, the Central Bank shall share information (domestically and internationally) between competent authorities, as well as between financial institutions, where this is required.

36. In the case of branches or subsidiaries of international banking groups, as host country supervisor, the Central Bank retains responsibility for the supervision of KYC regulations (which would include an evaluation of the appropriateness of the procedures).

37. The Central Bank reserves the right to amend these Guidelines from time to time. A financial institution should continuously update its AML/CFT/CPF programme as industry standards evolve. At a minimum AML/CFT/CPF policies and/or procedures should be updated once every two to three years.

38. As supervisory authority, the Central Bank shall maintain high professional standards, including standards with respect to confidentiality. The Central Bank shall employ staff of high integrity and that are appropriately skilled, possessing technical and other resources to effectively perform their functions. Furthermore, adequate, and relevant training shall be provided to such persons on various aspects in the fight against ML/TF/PF.

39. The Central Bank's responsibilities may also include publishing decisions taken regarding sanctions imposed on financial institutions.

1.15 The Role of the Board and Senior Management of a Financial Institution

40. The Board of Directors is ultimately responsible for the effectiveness of the financial institution's AML/CFT/CPF framework. The Board's oversight role is intended to ensure, inter alia, that there is compliance with all the relevant laws and regulations and international standards. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

41. Directors and senior management should be aware that:

i. The use of a group-wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the financial institution and compliant with Belizean law, regulations, and guidelines. Failure to ensure compliance by the financial institution with the requirements of the MLTPA may result in significant penalties for directors, officers and the financial institution **(See Appendix 4)**;

ii. Subsidiaries and branches of a financial institution including those domiciled outside of Belize are expected to, at a minimum, comply with the requirements of the MLTPA and these Guidelines; and

iii. Where some of a financial institution's operational functions are outsourced, the financial institution retains full responsibility for compliance with local laws, regulations, and guidelines.

42. Directors should demonstrate their commitment to an effective AML/CFT/CPF programme by:

i. Understanding the statutory duties placed upon them, their staff and the entity they represent;

ii. Approving AML/CFT/CPF policies and procedures that are appropriate for the risks faced by the financial institution. Evidence of consideration and approval of these policies should be reflected in the Board minutes and noted in the policy;

iii. Appointing an individual within the organization to ensure that the financial institution's AML/CFT/CPF procedures are being managed effectively; and

iv. Seeking assurance that the financial institution is in compliance with its statutory responsibilities as it relates to AML/CFT/CPF. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems. (**See Section on Compliance and Audit**).

43. Senior management is responsible for the development of sound risk management programmes (**See Implementation of Risk-Based Approach**) and for keeping directors adequately informed about these programmes and their effectiveness. These programmes, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, should be formally documented and, at a minimum, irrespective of whether the financial institution receives funds from third parties or not, should provide for:

i. The development of internal policies, procedures, and controls for, inter alia:

a. The opening of customer accounts and verification of customer identity;

b. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);

c. Determining business relationships that the financial institution will not accept by requiring graduated customer acceptance policies and procedures with more extensive due diligence for higher risk customers;

d. Determining an exit strategy to terminate undesired relationships with existing customers;

e. The timely detection of unusual activities and reporting of suspicious transactions to the FIU;

f. Internal reporting; and

g. Records retention.

ii. The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, research of unusual transactions and reporting of suspicious activities;

iii. Designation of a Compliance Officer at an appropriate level of authority, seniority, and independence to coordinate and monitor the compliance program (**See Section on Compliance and Audit**).

iv. An ongoing training programme designed to ensure employees adhere to the legal and internal procedures and become familiar with the dangers they and the business entity face and on how their job responsibilities can encounter specified ML/TF risks;

v. Establishment of management information/reporting systems to scrutinize customer account activity and facilitate aggregate and group-wide monitoring of significant balances regardless of whether the accounts are held on balance sheet, as assets under management or on a fiduciary basis;

vi. An effective independent risk-based oversight function to test and evaluate the compliance program; and

vii. Screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the financial institution from being used for criminal activity. This should include but is not limited to inquiries about the personal history of the potential employee and verifying appropriate references for the individual.

44. Policies should be periodically reviewed for consistency with the business model, and product and service offering. Special attention should be paid to new and developing technologies.

SECTION II – IMPLEMENTATION OF RISK-BASED APPROACH

45. The Central Bank recognizes the diversity of the institutions it regulates, and seeks to establish that, overall, processes appropriate to institutions are in place and are operating effectively.

46. Financial institutions are responsible to utilize the risk-based approach in meeting their AML/CFT/CPF obligations that are governed primarily by section 15 of the MLTPA.

47. Financial institutions must employ a risk-based approach in determining:

i. Appropriate levels of CDD measures, including whether to apply enhanced CDD;

ii. Mitigation measures commensurate with the risks posed by the financial institution's customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, products, services, transactions and delivery channels;

iii. The scope and frequency of ongoing monitoring;

iv. Measures for detecting and reporting suspicious transactions; and

v. Whether and how to launch new products, services, or technologies.

48. Financial institutions should document a risk-based approach AML/CFT compliance program. This approach requires an assessment of the ML/TF risks posed by the nature of the FI's business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

49. Senior Management must take ownership of, and responsibility for, the periodic evaluation to assess if and to what extent the financial institution is vulnerable to ML/TF/PF because of its activities and operations.

50. Senior Management must conduct a risk assessment in which it identifies and assesses the ML/TF risks and other integrity risks, considering risk factors including those relating to, at a minimum, the customers, countries and/or geographic areas, products, services, transactions, and delivery channels.

51. In the risk assessment Senior Management must consider the extent of the financial institution's exposure to risks by reference to its organizational structure, its corporate culture, its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services.

52. The risk assessment should be proportionate and tailored to the nature, size, and complexity of the financial institution's business. For example, large financial institutions are likely to have a more sophisticated system and methodology for conducting a risk assessment.

53. Some smaller financial institutions with limited range of customers and minimal products or services may be satisfied, on reasonable grounds, that standardized profiles for combinations of customers and services are appropriate. A focus of such financial institutions' efforts should be on those combinations of customers and services that fall outside any of the standardized profiles.

54. Regardless of its nature, size, and complexity, each financial institution must begin assessing the risks it faces either before commencing business or as soon as is reasonably practicable afterwards, ensuring that any ML/TF risks that may arise are effectively managed.

55. The risk assessment must be documented and kept up-to-date. This means a periodic and documented update of the risk assessment must be conducted, typically every one to three years, at a minimum, and/or following a 'trigger' event such as a serious compliance incident that has taken place, or major change of the financial institution's operations. The update must be approved by Senior Management and the risk assessment report should be made available, without delay, to the Central Bank upon request.

56. Following the risk assessment, Senior Management must also establish a documented AML/CFT/CPF strategy in accordance with its risk assessment. In the case where a financial institution forms part of a group operating outside Belize, that strategy must protect both its global reputation and its Belize business. Hence, an automatic adoption by the financial institution of the global and/or regional risk assessment is unacceptable. Explicit attention should always be given to the specifics of Belize and the Belizean operations of the financial institution.

57. Additionally, each financial institution should ensure that it has sufficient capacity and expertise to manage the risks it faces. As risks and understanding of risks evolve, a financial institution's capacity, mitigating controls and expertise should also evolve proportionally.

2.1 Risk Management

58. Risk management is the process of measuring risks and applying appropriate mitigating measures to minimize risks. Senior Management of most financial institutions have experience managing the financial institution's inherent business risk and the effectiveness of controls to manage those risks. In the context of AML/CFT/CPF compliance, risk management is a tool to assist Senior Management in making decisions about the need for and allocation of AML/CFT/CPF compliance resources.

2.2 Conducting an Institutional Risk Assessment

59. Financial institutions should consider using the following steps to assess the level of identified risks that the business may face:

i. Identify and assess the institution's inherent risks. This is an assessment of the risk that the financial institution is currently undertaking.

ii. Establish risk-tolerance levels and compare with results in activity 19(i) above.

iii. Establish risk-mitigation measures by employing proper controls.

iv. Evaluate residual risks by determining the level of risk remaining after incorporating mitigation measures.

v. Monitor and review risks by using a proper governance regime.

60. Risk can be defined as a combination of the following:

i. The threat of an event;

ii. Vulnerability to such an event; and

iii. The consequences of the threatened event taking place.

61. A threat is a person, object, or activity with the potential to cause harm. In the AML/CFT/CPF context, a threat is the demand for services by criminals, terrorists, and their facilitators. Such demand is influenced by the types and scale of domestic and foreign crimes that result in tainted property. The national risk assessment process identifies threats at the national level. Financial institutions should use the national threats identified, as well as independently assess the threat of customers attempting ML/TF at the business or transactional level. Customers who pose a greater threat of ML/TF are higher-risk customers.

62. A vulnerability is anything that may be exploited by a threat, or that may support or facilitate a threat's activities. A financial institution's AML/CFT/CPF context includes its vulnerabilities, products, services, transactions, and delivery channels and weaknesses in its AML compliance program.

63. A financial institution should consider consequences of an AML/CFT/CPF compliance failure including:

i. Legal consequences;

ii. Regulatory consequences;

iii. Financial consequences;

iv. Operational consequences; and

v. Reputational consequences.

64. In simple terms, risk is a combination of the likelihood that something might occur and the consequences of such an occurrence.

65. The process outlined below is a guide to assist financial institutions in assessing their level of identified risks.

2.3 Identify and Assess Inherent Risk

66. Inherent risk is the risk that naturally exists based on the business activity before there are mitigating controls in place. Financial institutions should consider all relevant information when identifying and assessing inherent risk. This includes considering how the various aspects of their business may be targeted as a viable option to facilitate money laundering, financing terrorism and proliferation.

67. At a minimum, this analysis must identify and assess the financial institution's inherent risks based on the following criteria:

i. The type of customers:

a. Target market segments;

b. Profile and number of customers identified as higher risk;

c. Complexity, volume, and size of customers' transfers, considering the usual activity and the risk profile of its customers (e.g., whether the ownership structure is highly complex; whether the customer is a politically exposed person (PEP); whether the customer's employment income supports account activity).

ii. The countries or jurisdictions its customers are from (or located), and where the financial institution has operations;

a. The AML/CFT/CPF laws, regulations and standards of the country or jurisdiction and quality and effectiveness of implementation of the AML/CFT/CPF regime;

b. Contextual factors such as political stability, maturity and sophistication of the regulator and supervisory regime, level of corruption, and degree of financial inclusion.

iii. The financial institution's products, services, transactions, and delivery channels:

a. Nature, scale, diversity and complexity of the financial institution's business activities including its geographical diversity;

b. Nature of products and services offered by the financial institution;

c. Delivery channels, including the extent to which there is direct interaction between the financial institutions and the customer or the extent to which reliance is placed on technology, intermediaries, third parties, correspondents or non-face-to-face access;

d. The degree to which the operations are outsourced to other entities in the Group or third parties; and

e. The development of new products and new business practices, including new delivery mechanisms and partners; or the use of new or developing technologies for both new and pre-existing products.

68. The financial institution should also consider variables such as the purpose of the business relationship, the level of customer assets, volume of transactions and the regularity or duration of the business relationship. Further, financial institutions should consider the threats and vulnerabilities that have been identified through any national risk assessment. Financial institutions should assess how these (and any other aspects of their business) make their business vulnerable to identified risks.

69. In addition to information from a national risk assessment, financial institutions should consider information obtained from relevant internal or external sources when conducting or updating risk assessments. These sources include, but are not limited to:

i. The financial institution's head of business lines and relationship managers;

ii. Internal/external audit and regulatory findings;

iii. Independent reviews;

iv. Sectoral emerging risks and typologies;

v. Corruption indices and country risk reports;

vi. Guidance issued by regulators;

vii. Threat reports and typologies issued by the FIU and law enforcement agencies;

viii. Independent and public assessment of a country's or jurisdiction's overall AML/CFT/CPF regime such as Mutual Evaluation Reports, IMF Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes; and

ix. Public sources of adverse news or relevant public criticism of a country or jurisdiction, including FATF, CFATF and other FSRBs public statements.

70. Financial institutions should then assess the probability or likelihood that the aspects of their business may result in ML/TF. The result of this step will be a likelihood rating for each of the risk areas of its business. For example, a financial institution may rate each area from a range of high (highly likely) to low (unlikely) to be used for ML/TF.

2.4 Establish Risk Tolerance

71. Risk tolerance is the level of risk that a financial institution is willing to accept, and impacts decision about risk mitigation measures.

72. Each financial institution should consider:

i. The risks it is willing and unwilling to accept;

ii. Risks that should be escalated to Senior Management for a decision; and

iii. Whether the financial institution has sufficient capacity and expertise to effectively manage the risks it has or is willing to accept.

2.5 Establish Risk-Mitigation Measures

73. Where the level of risk is within a financial institution's risk tolerance, it must ensure that the risk-mitigation measures applied are commensurate with the level of risk identified. Where higher risks are identified, financial institutions must take enhanced measures to manage and mitigate those higher risks.

74. Each financial institution must document its internal controls and related policies and procedures to mitigate and manage the risks it identifies, as well as those identified by the Central Bank, or through any risk assessment carried out at a national level. These policies and procedures must be approved by Senior Management.

75. Some risk mitigation measures include:

i. Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both;

ii. Setting transaction limits for higher-risk customers or products;

iii. Determining the circumstances under which they may refuse to take on or terminate/cease high-risk customers/products or services; and

iv. Determining the circumstances requiring Senior Management approval (e.g., high-risk, or large transactions, when establishing a relationship with high-risk customers such as PEPs).

2.6 Evaluate Residual Risk

76. Residual risk is the level of risk remaining after the application of risk-mitigation measures. Regardless of the strength of a financial institution's risk-mitigation methods, there will always be some residual ML/TF risk, which a financial institution must manage. Where the level of residual risk exceeds a financial institution's risk tolerance, or where its mitigation measures do not adequately mitigate high risks, the strength of mitigation measures should be increased.

2.7 Monitor and Review Risks

77. The risk assessment should be kept up-to-date through periodic reviews and when risk factors change. Financial institutions should ensure that their risk assessment programme is reviewed to assess the implications of:

i. New products, services, practices, technologies and delivery channels;

ii. New ML/TF trends or typologies;

iii. New regulatory guidance;

iv. Changes in customer portfolios or conduct;

v. Changes in products, services and delivery channels;

vi. Changes in business practices; and

vii. Changes in the law.

78. These risk assessments must be made available upon request by the Central Bank. Financial institutions are also required to monitor compliance with internal policies, procedures, and controls, and enhance them if necessary. Where appropriate, having regard to the size and nature of their business, financial institutions must engage an independent audit function to test the internal AML/CFT/CPF policies, controls, and procedures. The independent audit provides an opportunity for each financial institution to consider whether its risk assessments are up to date.

2.8 New Products, Practices and Technological Developments Risk Assessment

79. Financial institutions must take such measures as may be needed to identify and assess the risks that may arise in relation to:

i. The development of new products and new business practices, including new delivery mechanisms; and

ii. The use of new and developing technologies for new and pre-existing products.

80. Financial institutions must undertake the risk assessment prior to the launch or use of such products, practices, and technologies, and should take appropriate measures, which are commensurate with the identified risks, to manage and mitigate those risks. FI's are also expected to establish a transparent process for product reviews and approvals.

81. Financial institutions offering internet-based and/or telephone products and services should ensure that they have reliable and secure methods to verify the identity of their customers. The level of verification used should be appropriate to the risks associated with the product or service. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their telephone and internet banking applications and, whenever appropriate, they should implement multi-factor verification measures, layered security, or other controls reasonably calculated to mitigate those risks.

2.9 Customer Risk Assessment (Risk Rating)

82. Every financial institution is required to develop and implement a risk-rating framework which is approved by its Board as being appropriate for the type of products offered by the financial institution, and capable of assessing the level of potential risk each customer relationship poses to the financial institution. As part of the ongoing onsite examination program, Central Bank examiners will assess

the adequacy of financial institution's risk-rating policies, processes, and procedures, considering the risks that have been identified by the financial institution or notified to it by the Central Bank, as well as the extent to which financial institutions have adhered to legislative requirements.

83. While each financial institution will determine the number and name of risk categories, the fundamental issue is the adoption of reasonable criteria for assessing risks.

84. As a minimum the risk-rating framework relating to client relationships should include:

i. Differentiation of client relationships by risk categories (such as high, moderate or low);

ii. Differentiation of client relationships by risk factors (such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size, volume and type of transactions, cash transactions, adherence to client activity profile);

iii. The KYC documentation and due diligence information requirements appropriate for each risk category and risk factor based on a prior risk analysis; and

iv. A process for the approval of the downgrading/upgrading of risk ratings through the periodic review of the customer relationship.

85. The risk-rating framework should provide for periodic review of customer relationships. This will allow the financial institution to determine whether a risk rating should be adjusted. The risk ratings for high-risk customers should be reviewed more frequently than for other customers, and senior management should determine how the heightened risks are to be managed and mitigated. Where the risks cannot be appropriately managed or mitigated, senior management should also determine whether the relationship should be continued. All decisions regarding high-risk relationships, as well as the basis for those decisions, should be properly documented.

86. The risk rating framework should consider customer acceptance, and ongoing monitoring policies and procedures that assist the financial institution in identifying the types of customers that are likely to pose a higher-than-average risk of ML, TF activities, or other identified risk activities. A more extensive CDD process should be adopted for higher-risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers. The risk-rating framework should produce for documentation any changes in a customer's risk rating and the reason(s) for such change.

87. In identifying the risk profile of any customer, financial institutions should consider factors such as the following risk criteria. These are not set out in any particular order, nor should they be considered exhaustive.)

i. Nature of the customer's business, which may be particularly susceptible to ML/TF risk, such as casinos or other businesses that handle large amounts of cash;

ii. Nature of activity;

iii. Frequency of activity;

iv. Type, value and complexity of the facility;

v. Status (whether dormant or active) of facility;

vi. Type of customer (e.g. potentate/PEP);

vii. For a corporate customer, an unduly complex ownership structure for no apparent reason;

viii. Whether there is any form of delegated authority in place (e.g., power of attorney);

ix. Type of product or service used by the customer (e.g., whether private banking, one-off transaction, mortgage);

x. Delivery channels (e.g., whether internet banking, wire transfers to third parties, remote cash withdrawals);

xi. Geographical origin of the customer;

xii. Geographical scope of the customer's business activities including the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with certain high-risk jurisdictions, or those known to the financial institution to lack proper standards in the prevention of ML, TF or in the CDD process;

xiii. Unwillingness of the customer to cooperate with the financial institution's CDD process for no apparent reason;

xiv. Pattern of account activity given the financial institution's information on the customer;

xv. Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered; and

xvi. Any other information that raises suspicion of the customer being connected to ML/TF.

88. Accordingly, a financial institution may apply CDD standards on a risk-sensitive basis, consistent with these Guidelines, depending on the type of customer, business relationship or transaction. Simplified CDD is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems. Alternatively, a financial institution should apply enhanced due diligence to customers where the risk of being used for ML/TF is high. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or specific higher-risk scenarios apply.

89. In addition to "Red Flags" appended to these Guidelines, typologies of ML/TF schemes are available at websites such as www.fatf-gafi.org to assist in risk categorization.

90. Financial institutions should ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories and that the requisite due diligence is being followed. In addition, financial institutions should periodically review their risk categories criteria as typologies evolve on practices by money launderers and terrorists.

2.10 Prospective Customers

91. Prior to establishing a business relationship, a financial institution should assess the potential risk inherent in each new client relationship having regard to the guidance provided in these Guidelines. This assessment should consider the products or facilities to be used by the customer and whether

and to what extent a customer may expose the financial institution to risk. Based on this assessment, the financial institution should then decide whether or not to establish or continue with a relationship.

SECTION III – KNOW YOUR CUSTOMER

3.1 Customer Due Diligence

92. CDD is an essential element of the effort to prevent the financial system from being used to perpetrate ML/TF. A financial institution is ultimately responsible for verifying the identity of their customers and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, which for the purposes of these Guidelines are the physical identity (e.g., name and date of birth) and the activity undertaken.

93. A financial institution must prohibit the acceptance of anonymous accounts or accounts in fictitious names. If a financial institution maintains numbered accounts, they must be maintained in such a way as to ensure compliance with these Guidelines. The financial institution should properly identify the customer and the customer identification records should be available to the AML/CFT/CPF Compliance Officer, other appropriate staff, and competent authorities.

94. Two important aspects of knowing your customer are:

i. Being satisfied that a prospective customer is who he claims to be and is the ultimate client; and

ii. Ensuring that sufficient information is obtained on the nature of the business that the customer expects to undertake, as well as any expected or predictable pattern of transactions. This information should be updated as appropriate and as opportunities arise.

95. As part of the due diligence process, a financial institution should:

i. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset[2] of a business relationship. This process should include, where appropriate:

a. Taking reasonable measures to understand the ownership and control structure of the customer;

b. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and

c. Discontinuing the transaction if customer documentation information is not forthcoming at the outset of the relationship.

ii. Employ enhanced due diligence procedures for high-risk customers or transactions or business

[2] For the purposes of these Guidelines, the outset of the relationship is the earlier of acceptance of the signed application/proposal, or the first receipt of funds from the customer.

relationships such as private banking operations, non-resident customers, trust arrangements, companies having nominee shareholders or customers who the financial institution has reasons to believe are being refused banking facilities by another financial institution (**See Section on Enhanced Due Diligence***)*;

iii. Update identification records, on a risk-focused basis, to ensure that all existing customer records are current and valid and conform to any new requirements (**See Section on Identification Procedures**);

iv. Monitor account activity throughout the life of the business relationship; and

v. Review the existing records if there is a material change in how the account is operated or if there are doubts about previously obtained customer identification data.

96. In effecting the due diligence process, a financial institution should:

i. Whenever possible, require prospective customers to be interviewed in person. Exceptions to this are outlined in the sections on **Non-face-to-face Customers and Introduced Business**;

ii. Use official or other reliable source documents, data, or information to verify the identity of the beneficial owner prior to opening the account or establishing the business relationship (whether permanent or occasional or whether natural person or legal arrangements). Identification documents which do not bear a photograph or signature, and which are easily obtainable (e.g., birth certificates) are not acceptable as the sole means of identification. Such forms of identification may be used along with a current photo-bearing identification with a unique identifier (e.g., passport or social security card). Customer identity can be verified using a combination of methods such as those listed at **Appendix 5**. Verification may involve the use of external electronic databases.

iii. In instances where original documents are not available, only accept copies that are certified by an approved person (**see Appendix 6**). Approved persons should print their name clearly, indicate their position or capacity together with a contact address and phone number;

iv. If the documents are unfamiliar, take additional measures to verify that they are genuine e.g., contacting the relevant authorities; and

v. Determine through a risk analysis of the type of applicant and the expected size and activity of the account, the extent and nature of the information required to open an account. Examples of documentation for different types of customers are set out in the section on **Identification Procedures**.

97. For the purpose of these Guidelines, the financial institution should seek to identify the customer and all those who have controlling interest or exercise control over the account/transaction (**See Section IV**). A customer includes:

i. A person that maintains an account with the financial institution;

ii. A person on whose behalf an account is maintained i.e., beneficial owner;

iii. The beneficiaries of transactions conducted by professional intermediaries such as lawyers,

accountants, notaries, business introducers or any other professional service providers; or

iv. Any person connected with a financial transaction that can pose a significant risk to the financial institution, including persons establishing business relations, purporting to act on behalf of a customer or conducting transactions such as:

a. Opening of deposit accounts;

b. Entering into fiduciary transactions;

c. Renting safety-deposit boxes;

d. Requesting safe custody facilities; and

e. Occasional transactions exceeding thresholds as discussed below or linked transactions under this benchmark, and all occasional wire transfers.

98. Generally, a financial institution should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, verification of customer identity and beneficial owner may be undertaken following the establishment of the business relationship provided that:

i. It is done as soon as reasonably practicable;

ii. It would be essential not to interrupt the normal conduct of business (e.g., non-face-to-face business and securities transactions); and

iii. The ML risks are effectively managed. Should a financial institution determine this to be an unacceptable risk, they should retain control of any funds received until verification requirements have been met. If the requirements are not met and the financial institution determines that the circumstances give rise to suspicion, it should make a report to the FIU.

99. Where a customer is permitted to utilize the business relationship prior to verification, financial institutions should adopt risk management procedures under which this may occur. These procedures should include a set of measures on the limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions outside of the expected norm for the type of relationship.

100. Where the financial institution is unable to satisfactorily complete CDD requirements, it should not open the account, commence business relations, or perform the transaction. It should also consider making an STR.

101. Where there is a suspicion that an asset is suspected to either stem from a criminal activity, is linked or related to, or is to be used to finance terrorism or a transaction relates to ML or TF, a financial institution should be cognizant of the possibility of tipping-off a customer when conducting due diligence. The financial institution should complete the transaction only if the customer is able to allay concerns as to the legitimacy of the transaction. If it is believed that performing CDD measures may tip-off the customer or potential customer to that suspicion, then the reporting entity shall not perform the CDD measures and must file an STR with the FIU no later than three days after forming the suspicion, in accordance with section 17(4) of the MLTPA.

3.2 Nature and Scope of Activity

102. When commencing a business relationship, a financial institution should record the purpose and reason for establishing the business relationship and the anticipated level and nature of activity to be undertaken. The extent of documentary evidence will depend on the nature of the product or service. Documentation about the nature of the applicant's business should also cover the source of funds to be used during the relationship.

103. Once a business relationship has been established, the financial institution should take reasonable steps to ensure that information collected in the CDD process is kept up to date by undertaking reviews of existing records, particularly for higher-risk customers or business relationships. A financial institution should refer to the relevant section of these Guidelines for guidance on when further verification of a customer's identity may be necessary.

104. Reasonable steps should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced, or a transaction is conducted with a person acting on behalf of others.

105. Normally the prospective customer should be interviewed personally. If he fails or is unable to provide adequate evidence of identity or if the financial institution is not satisfied that the transaction is bona fide, an explanation should be sought and a determination made as to whether to terminate the business relationship, verify the customer's identity, and/or whether to file an STR with the FIU.

106. In instances where the relationship is discontinued, funds held to the order of the prospective customer should be returned only to the source from which they came and not to a third party, unless directed to do otherwise by a court order.

SECTION IV – IDENTIFICATION PROCEDURES

107. A financial institution should observe the following when seeking to verify the identity of its customers:

i. In the case of prospective customers, a financial institution must verify customer identity before permitting such customers to become facility holders;

ii. Whenever the amount of cash involved in an occasional transaction exceeds BZ$30,000, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked, the identity of the person who conducts the transaction should be verified before the transaction is conducted;

iii. Whenever the amount of cash involved in an occasional transaction exceeds BZ$30,000 and it appears to a financial institution that the person conducting the transaction is doing so on behalf of any other person or persons, the identities of the third parties must be verified before the transaction is conducted;

iv. Whenever it appears that two or more occasional transactions are or have been deliberately structured to avoid lawful verification procedures in respect of the person(s) conducting the

transaction(s) and whenever the aggregate amount of cash involved in the transaction(s) exceeds BZ$30,000, verification should be conducted as soon as practicable after the financial institution becomes aware of the foregoing circumstances;

v. Whenever a wire transfer is conducted as set out in section V of this Guideline;

vi. Whenever a financial institution knows, suspects, or has reasonable grounds to suspect that a customer is conducting or proposed to conduct a transaction which:

a. Involves the proceeds of criminal conduct;

b. Is a violation of a freezing obligation; or

c. Is an attempt to avoid the enforcement of requirements of the MLTPA, verification should take place as soon as practicable after the financial institution has knowledge or suspicion in respect of the relevant transaction;

vii. Whenever a financial institution has reasonable grounds to suspect that funds as defined in the MLTPA or financial services provided by these institutions are related to or are to be used to facilitate an offence under the MLTPA, verification should take place as soon as practicable after such suspicions arise;

viii. Where satisfactory evidence of identity is required, no transaction should be conducted over the facility pending receipt of identification evidence and information. Documents of title should not be issued, nor income remitted (though it may be re-invested) in the absence of evidence of identity; and

ix. Where the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data, verification of identification should be undertaken.

4.1 Natural Persons

108. A financial institution should obtain relevant information on the identity of its customer and should seek to verify information on a risk basis, subjecting higher-risk customers to a higher level of due diligence. In some instances, verification may be satisfied by maintaining current photo-bearing identification with a unique identifier (e.g., passport, social security card, driver's license or the national identity card,), or through the use of reliable, independent source documents, data or information to prove to its satisfaction that the individual is who that individual claims to be.

109. A financial institution must obtain and document the following basic information when seeking to verify identity:

i. True name/names used and correct permanent residential address including postcode (if applicable);

ii. Valid photo-bearing identification, with unique identifier, (e.g., passport, social security card or driver's license);

iii. Date and place of birth and nationality;

iv. Contact details e.g., telephone number, fax number and e-mail address;

v. Signature;

vi. Purpose of the account;

vii. The nature of the business relationship; and

viii. Source of funds.

110. The following information may also be required when a financial institution seeks to verify identity:

i. Occupation and name of employer (if self-employed, the nature of the self-employment);

ii. Estimated level of account activity including:

a. Size in the case of investment and custody accounts; and

b. Balance ranges, in the case of current and deposit accounts;

iii. An indication of the expected transaction volume of the account; and any other information deemed appropriate and relevant.

111. In circumstances where the financial institution's customer is considered a high-risk client, the financial institution should also take reasonable measures to establish the customer's source of wealth and document findings.

112. Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted if certified by persons listed in **Appendix 6**.

4.1.1 Confirmation of Name and Address

113. One or more of the following steps is recommended to confirm addresses:

i. Checking the Register of Electors;

ii. Provision of a recent utility bill, tax assessment or bank or credit union statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);

iii. Checking the telephone directory; and

iv. Record of home visit.

114. The information obtained should demonstrate that a person of that name exists at the address given and that the facility holder is that person.

115. Both residence and nationality must be established to ensure that the facility holder is not from a nation that is subject to sanctions by the United Nations or similar prohibition from any other official body or government that would prohibit such business being transacted. **Appendix 2** lists websites which contain information on the status of sanctions.

116. Obtaining a customer's date of birth provides an extra safeguard if, for example, a forged or stolen passport or driver's license is used to confirm the identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

117. Confirmation of a person's address and/or nationality is also useful in determining whether a customer is resident in a high-risk country.

118. Information and documentation should be obtained and retained to support or give evidence of the details provided by the facility holder.

119. Identification documents, either original or certified copies, should be pre-signed and bear discernable photograph of the applicant, for example:

i. Current valid passport;

ii. Armed forces ID card;

iii. Driver's license;

iv. Voter's identification card;

v. Social security card; or

vi. Other documentary evidence as is reasonably capable of establishing the identity of the individual customer.

120. Where prospective customers provide documents with which a financial institution is unfamiliar, either because of origin, format or language, the financial institution must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation.

4.1.2 When Further Verification of Identity is Necessary

121. Where a customer's identity (and any beneficial owner) has been verified, further verification is mandatory if:

i. During the course of the business relationship the financial institution has reason to doubt the identity of the customer;

ii. A financial institution knows, suspects, or has reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which:

a. Involves the proceeds of crime; or

b. Is an attempt to avoid the enforcement of the MLTPA; (*in such cases, verification should take place as soon as practicable after the financial institution has knowledge or suspicion in respect of the relevant transaction*); and

iii. There is a material change in the way a facility is operated.

122. It is also recommended that re-verification should be carried out in respect of those customers whom a financial institution has reasonable grounds to suspect that their funds are related to or are to be used to facilitate a terrorism-related offence. In conducting the re-verification exercise, a financial institution should have regard to the fact that the purpose of re-verifying a customer's identity is to enable law enforcement to have access to the appropriate identification documentation and information.

123. A financial institution may also, as part of its own internal AML/CFT/CPF and KYC policies, re-verify a customer's identity on the occurrence of any of the following non-exhaustive "trigger events":

i. A significant transaction (relative to a relationship);

ii. A material change in the operation of a business relationship;

iii. A new product or account being established within an existing relationship;

iv. A change in an existing relationship which increases a risk profile (as stated earlier); and

v. The assignment or transfer of ownership of any product.

124. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ between financial institutions. It will also depend on the nature of the product or service being offered and whether personal contact is maintained enabling file notes of discussions to be made or whether all contact with the customer is remote.

125. Customer due diligence measures do not imply that financial institutions must repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. When an existing customer conducts a transaction, closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to re-verify identity or address. A financial institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information.

126. The opportunity to re-verify a customer can be taken to confirm the relevant customer information when a previously dormant account has been reactivated or if there has been no recent contact or correspondence with the customer within the last 12 months.

4.1.4 Certification of Identification Documents

127. A financial institution should exercise due caution when considering certified documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the financial institution's responsibility to satisfy itself that the certifier is appropriate. In all cases, a financial institution should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

128. For natural persons, face-to-face customers must, where possible, show a financial institution's staff original documents bearing a photograph and copies should be taken immediately, retained, and certified by a staff member.

129. Where it is impractical or impossible to obtain sight of original documents, a copy is acceptable where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the facility holder **(See Appendix 6)**.

130. In low-risk instances, an electronic copy of original documents may be used to verify identity. However, financial institutions must employ multi factor verification measures, layered security or other controls reasonably calculated to mitigate the risk of fraud.

131. A certifier must be a qualified practicing notary public.

132. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address, telephone, and facsimile number and where applicable, a license/registration number.

4.2 Corporate Customers

133. All financial institutions are to identify the beneficial owners of a corporate, partnership and trust customer. To satisfy itself as to the identity of the corporate customer, the financial institution should obtain:

i. Name of corporate entity;

ii. Date and place of incorporation or similar date of existence;

iii. Principal place of business;

iv. Nature of business;

v. Mailing address;

vi. Registered office address;

vii. Contact telephone and fax numbers;

viii. Name of regulator;

ix. Board resolution authorizing the opening of the account and conferring authority on signatories to the account;

x. The original or a certified copy of the Certificate of Incorporation, authenticated where the body is incorporated outside of Belize, or Certificate of Registration where the body was incorporated abroad but registered under the Companies Act;

xi. Satisfactory evidence of the identity of all account signatories, details of their relationship with the company and if they are not employees, an explanation of the relationship. All signatories must be verified in accordance with the identification and verification of identity requirements of natural persons;

xii. Identity information on the beneficial owner, this includes the natural persons with a controlling interest in the corporate entity (**see Appendix 9**). This information should extend, as far as practicable, to identifying those with a minimum of 25% shareholding, those who ultimately

own and have principal control over the company's assets, including anyone who is giving instructions to the financial institution to act on behalf of the company.

xiii. In situations where the natural persons with controlling interest cannot be identified or there are doubts about the information previously collected, identify a natural person who is exercising ultimate effective control through other means (**see Appendix 9**). Examples of control by other means include personal connections to those owning or controlling a legal person, financing the enterprise, historical or contractual association, or use/enjoyment/benefit of company assets.

xiv. In instances where the natural persons with controlling interest and persons exercising control through other means cannot be identified, identify the natural persons having the position of chief executive or a person of equivalent or similar position;

xv. Information on whether and where the corporate customer is listed on a stock exchange.

xvi. If the company is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification, and verification of the identity of shareholders is not required; and

xvii. Confirmation before a business relationship is established, by way of company search and/or other commercial inquiries that the applicant company has not been, or is not in the process of being dissolved, struck off the companies register, wound-up or terminated. Such confirmation may be verified by obtaining a current Certificate of Good Standing or equivalent document or alternatively, obtaining a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party.

134. It is strongly recommended that a financial institution obtains the following information and documents when seeking to verify the identity of corporate customers:

i. Certified Copy of Articles of Association of the entity;

ii. Description and nature of business, including date of commencement, products or services provided, location of principal business and name and location of the registered office and registered agent of the corporate entity, where appropriate;

iii. Purpose of the account, the estimated account activity (including volume, balance ranges in the case of current and deposit accounts; size in the case of investment and custody accounts), source of funds and source of wealth in circumstances where the financial institution's customer is considered high-risk;

iv. By-laws and any other relevant corporate documents filed with the Companies' Registry;

v. Recent audit financials or in-house financials;

vi. Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company and supported by a copy of the respective Board Resolution;

vii. Copies of share register/share certificates;

viii. Copies of the list/register of directors and officers of the corporate entity including their names and addresses;

ix. Certificate of good standing prepared by the company registry if the company has been established for more than a year;

x. Written confirmation that all credits to the account are and will be beneficially owned by the facility holder except in circumstances where the account is being operated by an intermediary for the purpose of holding funds in his professional capacity;

xi. Satisfactory evidence of identity must be established for at least two directors, one of whom should, if applicable, be an executive director where different from account signatories; and

xii. Such other official documentary and other information as is reasonably capable of establishing the structural information of the corporate entity.

135. It is sometimes a feature of corporate entities being used to launder money or finance terrorism that account signatories are not directors, managers, or employees of the corporate entity. In such circumstances, a financial institution should exercise caution, making sure to verify the identity of the signatories in accordance with the relevant section of these Guidelines. Where appropriate, a financial institution should closely monitor the ongoing business relationship.

136. Where it is impractical or impossible to obtain sight of original incorporation documents, a financial institution may accept a suitably certified copy in accordance with the procedures in these Guidelines.

137. Trading companies may sometimes form part of complex organizational structures which also involve trusts and foundations. Particular care should be taken to verify the legal existence of the corporate entity and to ensure that any person purporting to act on behalf of the corporate entity is authorized to do so. The principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Inquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, for example a financial institution may, where appropriate, visit the business/company to ensure that there is an actual physical presence.

138. In addition, if the financial institution becomes aware of changes in the company structure or ownership or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

139. Where the business relationship is being opened in a different name from that of the corporate entity, the financial institution should make a search for both names.

140. Where persons are already known to the financial institution and identification records are already in compliance with the requirements of these Guidelines, there is no need to verify the identity again.

141. When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, financial institutions must conduct periodic inquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. This maybe be conducted based on the customer's risk. This may be conducted based on the customer's risk. Such changes may be significant in relation to potential

ML/TF activity, even though authorized signatories have not changed.

4.2.1 Powers of Attorney

142. The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, a financial institution should verify the identities of holders of powers of attorney, the grantor of the power of attorney and third-party mandates in accordance with documentation required for natural persons. Records of all transactions undertaken in accordance with a power of attorney should be kept in accordance with the record keeping requirements of these Guidelines.

4.2.2 Partnerships and Unincorporated Business

143. A financial institution must obtain the following documents and information when seeking to verify the identity of partnerships and unincorporated businesses:

i. Identification evidence for all partners/controllers of a firm or business, in line with the requirements in these Guidelines for individual customers who are relevant to their firm's application to become a facility holder and who have individual authority to operate a facility or otherwise to give relevant instructions;

ii. Identification evidence for all authorized signatories, in line with the requirements in these Guidelines for individual customers. When authorized signatories change, care should be taken to ensure that the identity of the current signatories has been verified;

iii. A copy of the partnership agreement (if any) or other agreement establishing the unincorporated business; and

iv. A mandate from the partnership authorizing the opening of an account or the use of some other facility and conferring authority on those who will undertake transactions should be obtained.

144. In the case of limited partnership, identification evidence must be obtained for the General Partner in line with the requirements in these Guidelines for individual customers. The partners of a partnership should be regularly monitored, and verification carried out on any new partners whose identities have come to light as a result of such monitoring or otherwise.

145. The following may also be required when a financial institution seeks to verify the identity of partnerships and unincorporated businesses:

i. Description and nature of the business including:

a. Date of commencement of business;

b. Products or services provided; and

c. Location of principal place of business;

ii. The reason for establishing the business relationship and the potential parameters of the account including:

a. Size in the case of investment and client accounts;

b. Balance ranges, in the case of deposit and client accounts;

c. An indication of expected transaction volume of the account;

d. The source of wealth in circumstances where the financial institution's customer is considered a high-risk client;

e. The source of funds;

f. A copy of the last available financial statements where appropriate;

g. Written confirmation that all credits to the account are and will be beneficially owned by the facility holder except in circumstances where the account is being operated by an intermediary for the purpose of holding funds in his professional capacity; and

h. Such documentary or other evidence as is reasonably capable of establishing the identity of the partners or beneficial owners.

4.3 Other Legal Structures and Fiduciary Arrangements

146. Legal structures such as trusts, foundations, nominees, and fiduciary accounts can be used by criminals who wish to mask the origin of funds derived from crime if the trustee or fiduciary does not carry out adequate procedures. Particular care is needed on the part of the financial institution when the facility holder is a trustee or fiduciary who is not an exempted client or an eligible introducer. The principal means of preventing ML/TF through legal structures, nominee companies and fiduciaries is to verify the identity of the provider of funds, such as the settlor and also those who have the power to remove the trustees/advisors. The settlor may also be a sole trustee of the trust, in which case, identification documentation should be obtained in relation to him.

4.3.1 Trust Clients

147. A financial institution should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened, or a transaction is conducted. This applies especially if there are any doubts as to whether these clients or customers are acting on their own behalf.

148. At a minimum, the financial institution should obtain the following, whether the financial institution is a named trustee or is providing services to a trust:

i. Name of trust;

ii. Nature/type of trust;

iii. Country of establishment;

iv. Identity of the ultimate natural person providing the funds, if not the ultimate settlor.

149. The financial institution should normally, in addition to obtaining identification evidence for the

trustee(s) and any other person who is signatory on the account:

i. Make appropriate enquiry as to the purpose of the legal structure and the source of funds;

ii. Obtain identification evidence for the settlor, protector(s)/controller(s) and for such other person(s) exercising effective control over the trust which includes an individual who has the power (whether exercisable alone, jointly with another person or with the consent of another person) to:

a. Dispose of, advance, lend, invest, pay or apply trust property;

b. Vary the trust;

c. Add or remove a person as a beneficiary or to or from a class of beneficiaries;

d. Appoint or remove trustees;

e. Direct, withhold consent to or veto the exercise of a power such as is mentioned in (a) – (d) above.

iii. Obtain identification evidence for the beneficial owner(s) that is identified as a specifically named natural person, legal entity, or legal arrangement, taking the name of the person, entity or arrangement. For a beneficiary that is designated by characteristics or by class, obtaining sufficient information concerning the beneficiary to be satisfied that the identity information of the beneficiary is available at the time of payout.

iv. Verify the identity of the beneficiary after the business relationship has been established if it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the trust.

150. Ongoing due diligence should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets.

151. Where the settlor is deceased, written confirmation should be obtained for the source of funds in the form, for example, Grant of Probate and/or copy of the will creating the trust.

152. Where a corporate trustee acts jointly with a co-trustee, the identity of any non-regulated co-trustees should be verified even if the corporate trustee is covered by an exemption. The relevant guidance contained in this section for verifying the identity of natural persons, unincorporated associations or companies should be followed.

153. Copies of any documents should be certified as true copies. In addition, a cross-check should be made to ensure that any bank account on which the trustees have drawn funds is in their names and the identities of any additional authorized signatories to the bank account should also be verified.

154. Any application to open an account or undertake a transaction on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and should trigger further inquiries.

155. A financial institution is also required to verify the identity of any underlying beneficiary of a legal structure. It is recognized that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children, and some may only become vested on the occurrence of special events. Where the beneficiary has a vested interest in the legal structure, verification must be carried out (and documented) by the financial institution providing the facility unless the transaction is or has been introduced by another financial institution on behalf of the settlor and beneficiary and such financial institution is itself required to verify the identity of the settlor and beneficiary. In all circumstances, there should be verification of beneficiaries before the first distribution of assets. Further, verification of protectors/controllers should be undertaken the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice. **See Appendix 9**.

156. A financial institution should be particularly vigilant where there is no readily apparent connection or relationship of the settlor to the beneficiaries of a trust. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically, not in return for any consideration (payment, transfer of assets or provision of services), a financial institution should try as far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example where the beneficiary turns out to be a child of the settlor born out of wedlock) and a financial institution is encouraged to take this into account while pursuing necessary or appropriate inquiries.

157. Where the traditional relationship between the settlor and the trustee is absent, a financial institution should demonstrate that it understands the commercial rationale for the arrangement and has verified the identity of the various counterparties.

158. Verification of the identity of the trust is satisfied by obtaining a copy of the creating instrument and other amending or supplementing instruments.

159. A financial institution is required to inform the Central Bank and the FIU when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of these Guidelines.

4.3.2 Identification of New Trustees

160. Where a trustee whose identity has been verified, is replaced, the identity of the new trustee should be verified before the new trustee is allowed to exercise control over funds.

4.3.3 Foundations

161. A foundation is an entity which exists to support a charitable institution, and which is funded by an endowment or donations. This type of nonprofit organization may either donate funds and support to other organizations or provide the sole source of funding for their own charitable activities.

162. It will normally be necessary to obtain the following documented information concerning foundations:

i. The foundation's charter;

ii. The Registrar General's certificate of registration or document of equivalent standing in a foreign

jurisdiction should be obtained in order to confirm the existence and legal standing of the foundation;

iii. The source of funds. A financial institution should obtain and document information on the source of funding for the foundation. In cases where a person other than the founder provides funds for the foundation, a financial institution should verify the identity of that third party providing the funds for the foundation and/or for whom a founder may be acting in accordance with verification of identity procedures for natural persons; and

iv. A financial institution should obtain identification evidence for the founder(s) and for such officers and council members of a foundation as may be signatories for the account(s) of the foundation. A financial institution should follow the guidance provided when verifying the identities of signatories. Where the founder is a company, a financial institution should have regard to the guidance on corporate clients. Where the founder is an individual, a financial institution should follow the guidance provided for natural persons.

4.3.4 Executorship Accounts

163. Where a business relationship is entered into for the purpose of winding up the estate it should be verified in line with this guidance, depending on the nature of the executor (i.e., whether personal, corporate, or a firm of attorneys). However, the identity of the executor or administrator need not normally be verified when payment from an established bank account in the deceased's name is being made to the executor or administrator in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate. Payments to the underlying beneficiaries on the instructions of the executor or administrator may be made in accordance with the identification and verification requirements as set out in the section on Identification Procedures in these Guidelines.

164. If any suspicions are aroused about the nature or origin of assets comprising an estate that is being wound up, then a report of the suspicions should be made to the FIU.

4.4 Products and Services Requiring Special Consideration

165. Special consideration should be given to the following products and services, which may pose added risk. Financial institutions should perform and document a risk assessment of any new product, service, practice, or technology (prior to launch) and the continual documentation of risk assessment and management of such product, service, practice, or technology.

166. Financial institutions must review, identify and document the areas of potential ML/TF&PF risks and submit to the Central Bank for approval before new products, practices and technologies are launched.

4.4.1 Provision of Safe Custody and Safety Deposit Boxes

167. Where facilities hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that a financial institution will follow the identification procedures set out in these Guidelines.

4.4.2 Technological Developments

168. A financial institution should have policies in place or take such measures as may be needed to prevent the misuse of technological developments in ML/TF schemes. A financial institution offering internet-based and/or telephone products and services should ensure that it has reliable and secure methods to verify the identity of customers. The level of verification used should be appropriate to the risks associated with the product or service. A financial institution should conduct a risk assessment to identify the types and levels of risk associated with their telephone and internet banking applications and wherever appropriate, they should implement multi-factor verification measures, layered security or other controls reasonably calculated to mitigate those risks.

4.5 New Payment Methods

169. New payment methods (NPM) are recent and ongoing technological innovations in payment and value transfer systems, including, but not limited to:

a. Pre-paid cards and tokens;

b. Payments by mobile phone;

c. Digital wallets; and

d. Internet-based payment systems.

170. Financial institutions must meet their AML/CFT/CPF obligations under the MLTPA, Financial Services Commission Act and relevant regulations and must determine appropriate policies, procedures, and controls for all their business, including any NPMs.

171. This portion of the guidance provides additional information about challenges that NPMs present and additional appropriate measures for conducting enhanced due diligence and mitigating risk as a supplement to those measures described elsewhere in these Guidelines.

172. Financial institutions must assess the risks associated with NPMs and apply appropriate enhanced due diligence and ML/TF risk mitigation measures.

173. An initial risk assessment must be conducted prior to offering an NPM or entering a business relationship with an NPM product or service provider. The risks associated with each NPM or NPM product or service provider must also be assessed on an ongoing basis.

174. When assessing the risks associated with offering an NPM or entering into a business relationship with an NPM product or service provider, financial institutions should ensure that they assess the risks associated with each of the persons involved with an NPM and not only the risks associated with an NPM product or service itself.

175. Despite the range of NPMs in existence, several challenges are common to many NPMs. These challenges include the non-face-to-face nature of many NPM transactions, the possibility of anonymity that some NPMs offer and the difficulty of monitoring person-to-person payments and involve a range of regulated or unregulated service providers.

176. Each financial institution should be aware of the differences in the risks posed by an NPM that the

financial institution itself offers, as compared with the risks posed by an NPM product or service provider that enters a business relationship with a financial institution. Each financial institution should tailor its enhanced due diligence measures accordingly.

177. NPMs can develop and evolve rapidly. Financial institutions that contemplate offering NPMs or entering business relationships with NPM product or service providers should stay abreast of industry best practices and both national and international standards involving NPMs, and the risks associated with them.

4.5.1 NPM Risk Factors and Risk-Mitigation Measures

178. Financial institutions must have policies, procedures, and controls in place to prevent the misuse of any business involving NPMs for the purposes of ML/TF.

179. A financial institution's policies, procedures and controls must be commensurate with the risks it faces.

180. Each individual NPM and each NPM product and service provider has a unique set of features and persons associated with it. In assessing the features and persons associated with an individual NPM or NPM provider, financial institution should be aware of risk factors that are common to many NPMs. These risk factors include, but are not limited to:

i. A non-face-to-face interaction between the financial institutions, the customer and any third parties;

ii. Any possibility to transact anonymously;

iii. No limits, or high limits, on transactions;

iv. Person-to-person transactions;

v. Restrictions that preclude the transfer of information needed for effective CDD;

vi. An inability to monitor transactions within an NPM's system; and

vii. The use of service providers or agents that are not subject to effective AML/CFT/CPF regulation.

181. Where a financial institution identifies higher risks in connection with offering an NPM or entering a business relationship with an NPM product or service provider, it must take reasonable and appropriate steps to mitigate and manage those higher risks. Reasonable and appropriate steps may be called risk-mitigation measures or enhanced due diligence measures. In practice, there may be no distinction between the two.

182. NPM risk-mitigation measures may be considered as falling within several broad categories:

i. CDD;

ii. Usage limits;

iii. Geographic limits;

iv. Monitoring and record-keeping; and

v. Segmentation due diligence and controls.

4.5.2 NPM Customer Due Diligence

183. Financial institutions must mitigate the risks associated with non-face-to-face interactions and the potential for anonymity by applying an appropriate, risk-based approach to CDD for NPMs.

184. Where a financial institution enters a relationship with an NPM product or service provider, it should ensure that it understands and approves of the AML/CFT/CPF policies, procedures and controls the NPM provider has in place.

185. Nothing in the MLTPA or this Guideline permits a financial institution to engage in anonymous transactions. Where a financial institution is unable to apply CDD measures in accordance with section 15 of the MLTPA, the refusal or termination of the business relationship or transaction is required.

186. Where an NPM provides for anonymous transactions in very small amounts and only on an infrequent basis, the risks associated with anonymity may appear to be lower. However, an absence of CDD impedes a financial institution's ability to effectively monitor an NPM to ensure that transactions are not linked and remain small and infrequent. An absence of CDD also increases the likelihood of impersonation and other types of fraud that may be costly and damaging to a financial institution and its customers.

187. When an NPM offers any potentially anonymous functionality, whether when a customer purchases or enters a business relationship with the NPM, when registering or when adding, spending, transferring, or withdrawing value, a financial institution should engage with the NPM only after taking appropriate measures to mitigate the associated risks.

188. Where an NPM features limited CDD on low value and infrequent transactions, a financial institution should require customer identification and verification for transactions above an appropriate risk-based threshold amount and/or frequency.

189. Where an NPM account may be used in the transfer of value from one person to another, financial institutions should have regard to the guidance provided for Wire Transfers.

190. When an NPM offers any potentially anonymous functionality, the financial institution should aggregate NPM account information by collecting, retaining, and analyzing all relevant information that accompanies a transaction through the NPM. The aggregation of customer and transaction information can enable the financial institution to more effectively identify linked activity that, collectively, exceeds any threshold amount or frequency or appears abnormal or suspicious.

191. To aggregate customer and transaction information, financial institutions should identify transactions and accounts that are linked to the same IP address, e-mail address, telephone number, common funding source or more traditional CDD information such as a customer's name, physical address, date of birth or identity number.

192. Where an NPM allows a user to anonymously register for or otherwise access an NPM, financial

institutions should seek to ensure that transfers of value into the NPM, or withdrawals of value from the NPM, are possible only using an account, such as a bank or credit card account, that has been subjected to the identification and verification processes of a financial institution subject to AML/CFT/CPF regulation in Belize or in another jurisdiction that imposes equivalent AML/CFT/CPF standards.

193. Financial institutions should be aware of the possibility of person-to-person payments within an NPM system, which may allow an NPM account to send or receive significant value from other NPM accounts without ever interacting with a verified bank or credit card account. In such cases, financial institutions should monitor transactions between the NPM account and the financial institution for any abnormal or suspicious activity.

4.5.3 NPM Usage Limits

194. Financial institutions should mitigate the risks associated with a non-face-to-face interaction and the potential for anonymity by implementing appropriate usage limits for NPMs.

195. Usage limits are restrictions on the value, frequency, and types of transactions that an NPM can facilitate. The higher the ML/TF risks associated with an NPM are, the stronger and more numerous the usage limits should be. A lack of usage limits, or overly generous usage limits, should generally be considered a higher risk for ML/TF.

196. Examples of usage limits include restrictions on:

i. The amount of value that can be loaded into, transacted within or spent or withdrawn from an NPM in a given period of time;

ii. Funding sources, including restrictions on the acceptance of cash;

iii. The withdrawal of cash from an NPM via an Automated Teller Machine (ATM) or other method;

iv. The number or types of third parties able to send or receive value using an NPM; and

v. The number of accounts a person may hold with an NPM.

197. Where an NPM has a reduced CDD requirement, financial institutions should consider limiting the NPM to a single, low-value, non-reloadable use.

198. Financial institutions may consider limiting the utility of an NPM solely to person-to-business transactions.

199. Where person-to-person transactions are possible, financial institutions should use a risk-based approach to limit the value or frequency of those transactions. In considering the risks associated with person-to-person transactions, a financial institution should consider whether it has access to sufficient CDD and transaction information on all parties to the transactions and the ability to effectively monitor transactions in an ongoing manner.

200. Financial institutions may also consider requiring payments into or from the NPM system to be carried out via an account that has been subjected to the identification and verification processes of an AML/CFT/CPF financial institution.

201. Financial institutions should ensure that an NPM account may be frozen or blocked when deemed necessary.

4.5.4 NPM Geographic Limits

202. Financial institutions should consider whether any geographic limits, including any limits on cross-border functionality, must be placed on an NPM to mitigate the ML/TF risks associated with the NPM.

203. Financial institutions should consider the geographic scope of the expected use of a particular NPM and determine whether the use of an NPM outside of that geographic scope would be suspicious.

204. Financial institutions should ensure that appropriate geographic limits are put in place where:

vi. There is insufficient justification for an NPM to be used outside of a particular geographic area;

vii. The risks presented exceed a financial institution 's risk tolerance; or

viii. A particular geographic area is subject to international sanctions.

205. Where a financial institution enters a business relationship with an NPM product or service provider, the financial institution should consider whether the NPM provider is operating from or in any jurisdiction that poses a higher risk of ML/TF, from or in any geographic area subject to international sanctions, or from or in any jurisdiction where the NPM provider is not subject to adequate AML/CFT/CPF regulation and oversight.

206. Financial institutions should use IP addresses and other geolocation data of an NPM customer or service provider, bearing in mind that proxy servers and other protocols may mask a user's true location and bearing in mind that an NPM provider's IP address may not be indicative of the jurisdiction in which the NPM provider is regulated.

4.5.6 NPM Monitoring and Record-Keeping

207. Financial institutions should ensure that they are able to effectively monitor NPM transactions for any unusual or suspicious activity and compliance with international sanctions.

208. As with any financial product or service, financial institutions should establish norms for NPM transactions and conduct and identify any activity that falls outside those norms.

209. Financial institutions should use ongoing monitoring to determine an appropriate level of CDD, usage limits and geographic limits. Where monitoring indicates a significant change in the way an NPM is used, for example, a customer attempting to use an NPM to carry out a transaction that is larger than the customer's verified identity information will permit, financial institutions should apply any required CDD or implement any appropriate usage or geographic limits prior to determining whether to allow the transaction to proceed.

210. Where a financial institution itself offers an NPM, it must have access to all customer and transaction information and must conduct appropriate risk-based monitoring.

211. Where a financial institution establishes a business relationship with an NPM product or service provider, it may not have direct access to all customer and transaction information.

212. Financial institutions should maintain records of all relevant NPM customer and transaction information, including IP and e-mail addresses, in accordance with the guidance provided in Record-Keeping requirements set out in these Guideline.

4.5.7 NPM Segmentation Due Diligence and Controls

213. Financial institutions should put in place appropriate policies, procedures, and controls to mitigate the risks associated with the segmentation of an NPM product or service between different persons and jurisdictions.

214. Financial institutions should ensure that they understand all the parties involved with an NPM and the risks associated with each. Some NPMs may be managed entirely by the issuing entity. However, an NPM may also involve an issuing entity, a branded transaction service provider and a range of exchangers, distributors, agents, and other persons involved in sales, loading value, transferring value, spending value, and withdrawing value. All types and combinations of NPMs, including pre-paid cards, mobile payments, internet payment systems and payments involving virtual currency, may involve a broad range of persons.

215. Risks associated with the segmentation of an NPM product or service between different persons and jurisdictions include, but are not limited to:

i. Difficulty in conducting effective CDD;

ii. Difficulty in conducting ongoing monitoring;

iii. Loss of information, or an inability to access information;

iv. Unclear lines of communication and accountability; and

v. The involvement of NPM providers not subject to appropriate registration, licensing and AML/CFT/CPF regulation requirements.

216. Both prior to entering a business relationship with an NPM product or service provider and throughout any such relationship, a financial institution must assess whether and how each person and jurisdiction involved in the NPM may affect the financial institution's ability to fulfil its obligations under the MLTPA and these Guidelines. Where all risks identified and assessed can be effectively and appropriately mitigated, those risks should be mitigated. Where all risks identified and assessed cannot be effectively mitigated, a financial institution should not enter the business relationship.

217. Financial institutions considering a business relationship with an NPM provider should carry out due diligence as to the NPM provider under consideration. The purpose of the due diligence is to determine whether the NPM provider has the ability, capacity, and any required authorization to implement appropriate AML/CFT/CPF policies, procedures, and controls. Financial institutions must establish a written policy concerning the scope and frequency of initial and ongoing due diligence for NPM providers.

218. At a minimum, financial institutions carrying out due diligence as to an NPM service provider should consider the following:

i. Whether the NPM service provider is licensed or otherwise authorized to carry out the NPM's activities;

ii. Whether, where relevant, the service provider is effectively regulated;

iii. Whether the scope of any regulation includes compliance with the AML/CFT/CPF regulations of Belize or of a jurisdiction that imposes equivalent AML/CFT/CPF requirements;

iv. Whether any operational, financial, human resource, structural, legal or regulatory considerations may affect the service provider's ability to carry out effective CDD and ongoing monitoring, where relevant, or impede the financial institution 's access to relevant information held by the NPM service provider, including customer and transaction information;

v. Whether any confidentiality, secrecy, privacy, or data protection restrictions may impede the financial institution or any relevant Belize regulatory authorities from effectively monitoring the activities of the NPM service provider.

219. Where a financial institution is considering a business relationship with an NPM provider that is not subject to AML/CFT/CPF regulation in Belize or that is not in a jurisdiction that imposes equivalent standards, the financial institution should ensure that the NPM provider has appropriate CDD policies, procedures, and controls in place. Telecommunications companies, for example, that provide NPM payment intermediary services often hold customer information, but due diligence is required to determine whether that customer information has been obtained and maintained in accordance with the appropriate AML/CFT/CPF standards.

220. Financial institutions must not enter a business relationship with an NPM provider where access to required data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

221. Where an financial institution is establishing a business relationship with an NPM provider that is not subject to appropriate AML/CFT/CPF regulation and where the financial institution does not have ready access to appropriate transaction and customer information of that NPM product or service provider, the customer agreement between the financial institution and NPM provider should confirm that the financial institution will receive, upon request, transaction and customer information on users of the NPM.

222. The customer agreement should authorize the financial institution to continuously monitor and assess the NPM provider against the terms of the agreement in to ensure that any necessary corrective measures are taken promptly. The level of monitoring and assessment authorized by the customer agreement should be proportionate to the risks involved with the NPM's activities.

223. The customer agreement should permit the financial institution to periodically test whether the NPM provider complies with requests for information and should entitle the financial institution to terminate the relationship where the NPM service provider fails to perform according to the agreement.

224. The customer agreement should clarify the respective roles of the financial institution and the NPM

provider as regards compliance with international sanctions.

4.5.8 Agent Networks and other Third Parties

225. Where an NPM or other money value transfer business involves an agent network or other third parties, financial institution should ensure that the product or service provider has in place appropriate policies, procedures, and controls to assess and mitigate the risks associated with the involvement of agents and third parties. Financial institutions should require product and service providers to demonstrate that they have conducted appropriate background and reference checks on any agents or third parties.

226. Financial institutions should also require product and service providers to demonstrate that their agents or third parties are examined for compliance with appropriate AML/CFT/CPF obligations, and that appropriate policies, procedures and controls provide for ongoing training and supervision of the agents or third parties.

4. 6 Reliance on Third Parties to Conduct KYC on Customers

227. For the purposes of these Guidelines, third party is defined as an individual or other entity who is not a direct party to a contract, agreement, or transaction but who has an interest in or is affected by it.

228. Every financial institution must retain adequate documentation to demonstrate that its KYC procedures have been properly implemented and that it has carried out the necessary verification itself.

229. There are, however, certain circumstances in which it may be possible for a financial institution to rely on KYC procedures carried out by a bank, a financial institution as defined in the DBFIA, or a credit union. Examples of such circumstances are:

i. Where a financial institution is unable to readily determine whether an occasional transaction involves cash because a customer deposited funds into a facility held for and on behalf of the financial institution by another financial institution; or

ii. Where a financial institution being a facility holder of the financial institution, conducts a transaction on behalf of a customer, using the facilities of a financial institution, the financial institution may rely upon the written confirmation of the financial institution that it has verified the identity of the customer concerned.

230. Where such transactions are conducted in addition to obtaining written confirmation, a financial institution must also confirm the existence of the facility provided by the financial institution.

231. This exemption applies only to occasional transactions conducted by financial institutions that are facility holders of a financial institution. However, if the person on whose behalf the transaction is being conducted, is being introduced to the financial institution for the purpose of forming a business relationship with the financial institution, then that financial institution must carry out the appropriate due diligence and obtain the necessary evidence of identity.

4.6.1 Intermediaries

232. A financial institution is required to not only verify the identity of an intermediary but also to look through that entity to the underlying client(s) where the intermediary is not one of the financial institutions referred to as an eligible introducer (**see Section on Introduced Business**) and/or is not from a country with equivalent or higher AML/CFT/CPF standards of regulation. In these circumstances, measures must be taken to verify the identity of the underlying clients. In satisfying this requirement, the financial institution should have regard to the nature of the intermediary, the domestic regulatory regime in which the intermediary operates, to its geographical base and to the type of business being done. Where, however, the intermediary is one of the financial institutions referred to in the section on **Introduced Business**, such verification is not required.

4.7 Exemptions and Concessions

4.7.1 Financial Institutions

233. Verification of identity is not normally required when the facility holder is an eligible introducer (**see Section on Introduced Business**). A financial institution should verify that the financial institution does exist (e.g., is listed in the Bankers' Almanac or is a member of a regulated or designated investment exchange); and that is also regulated and subject to equivalent or higher AML/CFT/CPF standards of licensing and regulation.

234. In all cases the financial institution must be satisfied that it can rely on the eligible introducer. The financial institution may request from an eligible introducer such evidence as it reasonably requires to satisfy itself as to the identity of the introducer and robustness of its KYC policies and procedures.

4.7.2 Occasional Transactions

235. It is important for a financial institution to determine whether a facility holder is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship, as this can affect the verification requirements. The same transaction may be viewed differently by a financial institution and by an introducing intermediary, depending on their respective relationships with the facility holder. Therefore, where a transaction involves an intermediary, both the financial institution and the intermediary must separately consider their positions and ensure that their respective obligations regarding verification of identity and associated record keeping are met.

236. For the purpose of these Guidelines, an occasional transaction is one that is conducted by a person without an account or facility at the financial institution or a one-off transaction carried out by a person otherwise than through a facility in respect of which that person is a facility holder. Occasional transactions include:

i. Encashment of cheques drawn;

ii. Exchange of coins for cash;

iii. Purchase of foreign currency including purchase for holiday travel; and

iv. Transactions via remittance service providers.

237. Due diligence measures including identifying and verifying the identity of customers, should be

undertaken on, inter alia, on occasional transactions over BZ$30,000 or its equivalent in foreign currency, whether conducted in a single transaction or multiple operations that appear to be linked. A financial institution should also obtain information to understand the purpose and intended nature of the business relations, the nature of the customer's business and the source of funds.

238. In instances where the applicant is acting for a business who is conducting an occasional transaction above BZ$30,000, the financial institution should take the measures necessary to ensure that the applicant is legally authorized to act for the customer and conduct customer due diligence on the applicant to verify the identity of the person.

239. The extent of identity information and verification of occasional transactions below these thresholds is dependent on the materiality of the transaction and the degree of suspicion.

240. At a minimum, a financial institution should:

i. Identify and verify3 the persons conducting occasional transactions below the above thresholds;

ii. Maintain an effective system to monitor for abuse of occasional transactions; and

iii. Establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

241. Customers who conduct occasional transactions (whether a single transaction or a series of linked transactions) where the amount of the transaction or the aggregate of a series of linked transactions is less than BZ$30,000 or the equivalent in any other currency, are exempt from full verification requirements.

242. A financial institution needs to be aware at all times of cases where the total of a series of linked transactions exceeds the prescribed limit of BZ$30,000 and they should verify the identity of the customer in such cases. These are cases where in respect of two or more occasional transactions it appears at the outset or at a later stage, to a person handling any of the transactions that the transactions are linked and that the aggregate amounts of these transactions exceed or are likely to exceed BZ$30,000 or its equivalent.

243. As per best practice, a period of three months for the identification of linked transactions is normally acceptable. However, there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore, the relevant procedures for linking will ultimately depend on the characteristics of the product rather than an arbitrary time limit. For example, a financial institution should be aware of any obvious connections between the sender of funds and the recipient.

244. Verification of identity will not normally be needed in the case of an exempted occasional transaction referred to above. If, however, the circumstances surrounding the occasional transaction appear to the financial institution to be unusual or questionable, further inquiries should be made. If as a result of inquiries, the financial institution becomes aware of or suspects ML/TF, the financial institution must take steps to verify the proposed client's identity. Where ML is known or suspected, the financial institution should make an STR regardless of the size of the transaction. Where TF is known

[3] At a minimum, identification may consist of the customer's name and address, which is verified by valid photo-bearing ID with a unique identifier.

or suspected, the financial institution should make a report to the FIU in accordance with Section 17 of the MLTPA.

4.7.3 Exempted Customers

245. Documentary evidence of identity will not normally be required in the case of:

i. Superannuation schemes (retirement plans in which an employer makes a contribution into an account each month. The contributions are invested on behalf of an employee, who may begin to make withdrawals after retirement);

ii. Occupational retirement/pension plans which do not allow non-employee participation;

iii. Financial institutions regulated by the Central Bank and the Supervisor of Insurance;

iv. Foreign financial institutions located in a jurisdiction which is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank and Supervisor of Insurance;

v. Any central or local government agency or statutory body;

vi. Any one-off transaction of or below BZ$30,000 or its equivalent in foreign currency;

vii. Any one-off transaction carried out with or for a third party on the basis of an introduction by a person who has provided assurance that evidence of the identity of those third parties introduced by him have been obtained and recorded under procedures maintained by him, where that person identifies the third party and where:

a. Transactions fall within the BZ$30,000 threshold;

b. There are reasonable grounds to believe that the applicant for business is subject to an overseas regulatory authority which exercises regulatory functions and control;

c. There are reasonable grounds to believe that the applicant for business is based or incorporated in a country with equivalent standards in force.

246. Irrespective of the size and nature of the transaction or proposed transactions and exemptions set out above, identity must be verified in all cases where ML/TF is known or suspected. If ML is known or suspected, then a report must be made to the FIU. Knowledge or suspicion of terrorist financing should also be reported to the FIU. In both cases verification procedures must be undertaken if this has not already been done.

4.8 Enhanced Due Diligence

247. A financial institution should apply enhanced CDD measures on a risk sensitive basis for such customers assessed as presenting a higher risk for ML/TF. As such, a financial institution may conclude that the standard evidence of identity required under the identification procedures is insufficient and that it must obtain additional information about a particular customer.

248. The application of CDD measures commensurate with the ML/TF risks identified allows financial

institutions to meet two broad objectives. The first is to inform the financial institutions' periodic and ongoing risk assessment processes. The second is to provide a tailored basis for monitoring customer activity and transactions, so attempts to launder money and finance terrorism are more likely to be detected.

249. Enhanced due diligence must be applied in all circumstances where the ML/TF risks associated with a customer or the products, services, delivery channels or geographic location of counterparties with which the customer engages are assessed as higher than standard.

250. A financial institution may determine that a customer is high-risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption, and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.

251. The extent of additional information sought and of any monitoring carried out in respect of any particular customer or class/category of customer, will depend on the ML/TF risk that the customer is assessed to present to the financial institution. A financial institution should hold complete set of information in respect of those customers assessed as carrying a higher ML/TF risk or who are seeking a product or service that carries a higher risk of being used for ML/TF purposes.

252. The financial institution's policy framework should therefore include a description of the types of customers that are likely to pose a higher-than-average risk and procedures for dealing with such applications. High-risk customers should be approved by senior management and stringent documentation, verification and transaction monitoring procedures should be established. Applying a risk-based approach, enhanced due diligence for high-risk accounts may include, where deemed relevant, and with more frequency than applied for low-risk customers:

i. An evaluation of the principals;

ii. A review of current financial statements;

iii. Verification of the source of funds;

iv. Verification of source of wealth;

v. The conduct of reference checks;

vi. Checks of electronic databases; and

vii. Periodic reporting to the Board about high-risk accounts.

253. In addition, financial institutions should consider applying additional measures, such as:

i. Updating more frequently the identification and verification data for the customer, its beneficial owner(s) and any other persons with an ownership or controlling interest in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the financial institutions;

ii. Conducting enhanced ongoing monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of transactions requiring further examination; and

iii. Requiring the first payment to be carried out through an account in the customer's name via a financial institution subject to the MLTPA or via an institution that is situated in a country or territory other than Belize that imposes requirements equivalent to those in Belize that effectively implements those requirements, and that is supervised for effective compliance with those requirements;

254. A financial institution should give particular attention to the following business relations and transactions:

i. Where a customer has not been physically present for identification purposes;

ii. Correspondent relationships;

iii. Business relationships or occasional transactions with a PEP;

iv. Business relationship or occasional transaction with persons from or in countries and jurisdictions known to have inadequate AML/CFT/CPF measures; ; and

v. Business relationship or transaction represents a high risk of ML/TF, corruption or is subject to international sanctions;

vi. Corporate customers able to issue bearer shares or bearer instruments; and

vii. Where the customer's address is outside of Belize or where there is significant unexplained distance between the customer and the financial institution.

255. A business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of ML, corruption, TF or being subject to international sanctions where a person associated with the business relationship or occasional transaction is:

i. The government or a public authority within the country or territory;

ii. A PEP in relation to the country or territory;

iii. A person who is a resident in, citizen of or incorporated in the country or territory;

iv. A person having a registered office or other business address in the country or territory;

v. A person whose funds are or derive from either income arising in the country or territory, or assets held in the country or territory by or on behalf of the person; or

vi. Transacting from or with the country or territory.

256. A person associated with the business relationship or occasional transaction is any of the following:

i. Customer;

ii. Beneficial owner or controller of the customer;

iii. Third party for whom the customer is acting;

iv. Beneficial owner or controller of a third party for whom the customer is acting; or

v. Person acting or purporting to act on behalf of the customer.

257. Irrespective of whether financial institutions ultimately determine that enhanced due diligence is appropriate, the financial institutions should document its deliberations and the full rationale behind its decision. Financial institutions should ensure that its documented deliberations and reasoning are available promptly upon request to authorized authorities.

4.8.1 Politically Exposed Persons

258. The MLTPA defines PEPs as individuals in Belize or in a foreign country entrusted with public functions as well as persons entrusted with a prominent public function by an international organization, their immediate family members and close associates. These functions include:

i. Heads of state, heads of government, and senior politicians including Ministers and Ministers of State;

ii. Members of the House of Representatives and the Senate;

iii. Permanent Secretaries or Chief Executive Officers, as the case may be;

iv. Judges of the High Court and Court of Appeal and Magistrates;

v. Members of High Courts, Superior Courts of record, of constitutional courts, or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;

vi. Members of courts of auditors or of the boards of central banks;

vii. Ambassadors and chargés d'affaires;

viii. High-ranking officers in the armed forces;

ix. Law enforcement officers and senior officers above the rank of Sergeant;

x. Members of the boards and the Chief Executive Officer (by whatever name called) of government owned or controlled enterprises or authorities;

xi. Members of the administrative, management or supervisory bodies of State-owned enterprises; and

xii. Important political party officials.

259. The immediate family members of PEPs are their spouse, partner, children and their spouses or partners, parents, grandparents and grandchildren.

260. for the purposes of deciding whether a person is a close associate of a PEP, a financial institution must only have regard to information which is in that person's possession or is publicly known.

261. For the purpose of deciding whether a natural person is a PEP or a family member or close associate of a PEP, financial institutions should rely first and foremost on the information obtained through the application of CDD measures. Where financial institutions need to carry out additional checks and verification, they may rely upon a wide range of sources, including commercial databases, internet and media searches, including social media.

262. Where financial institutions need to carry out research to determine the level of risk of the business relationship with a PEP, they may rely upon a wide range of sources. Possible sources include internet and media searches as well as relevant reports, evaluations and databases on AML/CFT and corruption risk published by national, international and non-governmental organizations, which may provide valuable information and background on the PEP and highlight specific issues and industries of concern. Resources such as mutual evaluation reports, which assess the compliance of countries with the international AML/CFT/CPF standards. Actual knowledge concerning a natural person and the reputation of the natural person may also help assess the level of risk.

263. Concerns about the abuse of power by public officials and the associated reputation and legal risks which a financial institution may face, have led to calls for enhanced due diligence on such persons. This abuse of power may be for their own enrichment and/or the benefit of others through illegal activities such as receipt of bribes or fraud. Identifying PEPs can be problematic consequently, a financial institution is to develop and maintain "enhanced scrutiny" practices which may include the following measures to address PEPs risk:

i. Develop policies, procedures and processes such as the use of electronic databases to assess whether a customer is or has subsequently become a PEP;

ii. Take reasonable measures to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds of PEPs, both at the outset of the relationship and on an ongoing basis;

iii. Exercise greater scrutiny and conduct enhanced ongoing monitoring of all PEP accounts so that any changes are detected and consideration can be given as to whether such changes suggest corruption or misuse of public assets;

iv. Require senior management or the Board or directors to determine whether to commence or continue the relationship where a customer is found to be or subsequently becomes a PEP. Regular reviews, on at least an annual basis, should be undertaken to assess the development of the business relationship;

v. Assess country risks where financial relationships exist evaluating, *inter alia*, the potential risk for corruption in political and governmental organizations. A financial institution which is part of an international group might also use the group network as another source of information;

vi. Where a financial institution entertains business relations with entities and nationals of countries vulnerable to corruption, establish who the senior political figures are in that country and seek to determine whether customer relationships may be susceptible to acquiring such connections after the business relationship has been established; and

vii. Maintain vigilance where customers are involved in businesses which appear to be most vulnerable to corruption, such as, but not limited to trading or dealing in precious stones or precious metals.

264. In addition to the identifying and verifying the information normally requested for personal customers, the following information on a PEP should be gathered:

i. Estimated net worth, including financial statements;

ii. Information on immediate family members or close associates including those having transaction authority over the account; and

iii. References or other information to confirm the reputation of the client.

265. Detailed due diligence should include:

i. Close scrutiny of any complex structures (for example, legal structures such as corporate entities, trusts, foundations and multiple jurisdictions);

ii. The development of a profile of expected activity on the business relationship to provide a basis for future monitoring. The profile should be regularly reviewed and updated; and

iii. Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of unknown financial institutions and regular transactions involving sums just below a typical reporting threshold.

266. A financial institution must bear in mind that provision of financial services to corrupt PEPs exposes the institution to reputational risk and costly law enforcement measures. Hence, a financial institution is encouraged to be vigilant in the identification of PEPs from all jurisdictions (particularly from high-risk countries) who are seeking to establish relationships.

267. A financial institution should ensure that timely reports are made to the FIU where proposed or existing business relationships with PEPs give grounds for suspicion.For the purposes of these Guidelines, once persons are identified as PEPs, they may always be considered as PEPs. The handling of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk and not just a timeline.

268. For the purposes of these Guidelines, once persons are identified as PEPs, they may always be considered as PEPs. The handling of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk and not just a timeline.

269. Financial institutions should apply a risk-based approach in determining whether a natural person who has been entrusted with a prominent public function but no longer holds that position should still be considered a PEP. At a minimum, such a natural person should be considered a PEP for a period of five years after leaving office. Possible risk factors for considering a natural person as a PEP for an extended period of time include:

i. The level of (informal) influence that the natural person could still exercise;

ii. The seniority of the position that the natural person held as a PEP; and

iii. The linkage (both formal and informal) between the natural person's previous and current positions and functions.

270. A financial institution should ensure that timely reports are made to the FIU where proposed or existing business relationships with PEPs give grounds for suspicion.

4.8.2 Non-Profit Organizations

271. Non-Profit Organizations (NPOs) may pose specific risks of ML/TF for a financial institution. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of the funds.

272. NPOs differ in size, income, structure, legal status, membership, and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social, or fraternal purposes or for carrying out other types of "good works". NPOs can range from large regional, national, or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support. While terrorist financing may occur through small, non-complex transactions, enhanced due diligence may not be necessary for all clients that are small organizations, dealing with insignificant donations for redistribution among members. A financial institution should, therefore, determine the risk level of activities in which the NPO is engaged.

273. To assess the risk, a financial institution should focus inter alia on:

i. Purpose, ideology or philosophy;

ii. Geographic areas served (including headquarters and operational areas);

iii. Organizational structure;

iv. Donor and volunteer base;

v. Funding and disbursement criteria (including basic beneficiary information);

vi. Record keeping requirements; and

vii. Its affiliation with other NPOs, Governments or groups.

274. Where a facility holder is an NPO, it will normally be necessary to obtain the following documented information:

i. An explanation of the nature of the proposed entity's purposes and operations;

ii. The identity of all signatories to the account and/or anyone authorized to give instructions on behalf of the entity. This information should also be verified; and

iii. The identity of Board members and trustees, where applicable.

275. As part of the verification process, a financial institution should confirm that the organization is registered under the appropriate laws and should carry out due diligence against publicly available terrorist lists. As part of ongoing monitoring activity, a financial institution should examine whether funds are being sent to high-risk countries.

276. In the case of a corporate entity, the account opening procedures should be in accordance with the procedures for corporate customers. Likewise, in the case of trusts and foundations, account opening procedures in accordance with the requisite sections of these Guidelines should be employed.

277. Where a NPO is registered as such in an overseas jurisdiction, it may be useful for the financial institution to contact the appropriate charity commission or equivalent body to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. A financial institution should satisfy itself as to the legitimacy of the organization by, for example, requesting sight of the constitution.

278. A financial institution should refer to **Appendix 2** for a list of relevant websites which provide information on non-profits organizations and charities.

279. Whilst it is not practical to obtain documentary evidence of identity of all donors, a financial institution should undertake a basic "vetting" of all NPOs established in other jurisdictions, in relation to known ML and TF activities. This includes a reasonable search of public information, verifying that the NPO does not appear on any terrorist lists nor that it has any association with ML and that identification information on representatives/signatories is obtained. Particular care should be taken where the organizations' funds are used for projects located in high-risk jurisdictions.

4.8.3 Non-Face-to-Face Customers

280. The rapid growth of financial business by electronic means increases the scope for non-face-to-face business and increases the risk of criminal access to the financial system. Customers may use the internet, the mail service, or alternative means because of their convenience or because they wish to avoid face-to-face contact. Consequently, special attention should be paid to risks associated with new and developing technologies.

281. Non-face-to-face transactions carry an inherent risk of forgery and fraud, which a financial institution should take care in their internal systems, policies, and procedures to mitigate. The extent of verification for non-face-to-face customers will depend on the nature and characteristics of the product or service provided and the assessed ML/TF risk presented by the customer.

282. Where a customer approaches a financial institution by post, telephone, transmission of instructions or applications via facsimile or similar means, or over the internet, whereby it will not be practical to seek a passport or other photographic identification document, verification of identity should be sought from a financial institution in a country that is subject to equivalent or higher AML/CFT/CPF standards of regulation.

283. Where the customer has not been physically present for identification purposes, a financial institution may complete applications but should take specific and adequate measures to compensate for the higher risk, most notably for forgery and fraud, by applying one or more of the following measures before establishing a business relationship:

i. Obtaining documents certified by approved persons listed at **Appendix 6**;

ii. Ensuring that all company documents are signed by the Company Secretary;

iii. Perform one or more additional checks designed to mitigate the risk of identity fraud. This may include requesting additional documents to complement those which are required for face-to-face customers, including more than one photo-bearing ID;

iv. Making independent contact with the customer, for example by telephone on a listed business or other number which has been verified prior to opening an account or conducting a transaction;

v. Requesting third party introduction e.g., by an introducer as noted in the section on **Introduced Business**;

vi. Communicating with the customer at an address that has been verified (such communication may be in the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);

vii. Requiring internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;

viii. Using a reliable, independent digital identification verification application or tool that is adequately protected against internal and external manipulation or falsification to avoid creating false identities; and

ix. Requiring the first payment to be carried out through an account in the customer's name via a financial institution subject to the MLTPA.

284. In addition, the financial institution may:

i. Carry out employment checks (where applicable) with the customer's consent through a job letter or verbal confirmation on a listed business or other number;

ii. Require the first payment to be carried out through an account in the customer's name with another bank subject to equivalent or higher CDD standards; and

iii. Obtain any other information deemed appropriate.

285. Where initial checks fail to identify the customer, additional checks should be independently confirmed and recorded. If the prospective customer is required to attend a branch to conduct the first transaction, or to collect account documentation or credit/debit cards, then valid photo-bearing identification should be obtained at that time.

286. Where a financial institution or its subsidiary initiates transactions in its role as a securities broker or in the sale of mutual funds without establishing face-to-face contact and obtaining all the relevant documentation, it should make all efforts to obtain such information as soon as practicable. In accepting such transactions, a financial institution should:

i. Set limits on the number and aggregate value of transactions that can be carried out;

ii. Indicate to customers that failure to provide the information within a set timeframe, may trigger the termination of the transaction; and

iii. Consider submitting an STR.

287. Any subsequent change to the customer's name, address, or employment details of which the financial institution becomes aware should be recorded and be regarded as a "trigger" event. Generally, a KYC review would be undertaken as part of good business practice and due diligence process, but it would also serve for ML/TF prevention.

288. File copies of supporting evidence should be retained. A financial institution that regularly conducts one-off transactions should record the details in a manner which allows cross reference to transaction records. Such a financial institution may find it convenient to record identification details on a separate form to be retained with copies of any supporting material obtained.

289. An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file.

290. Financial institutions should be cognizant of the risks associated with customers approaching a financial institution by post, telephone, or the internet in a deliberate effort to avoid face-to-face contact.

4.8.4 Introduced Business

291. A financial institution may rely on other regulated third parties to introduce new business in whole or in part, but the ultimate responsibility remains with the financial institution for customer identification and verification.

292. Where a business relationship is being instituted, the financial institution is obliged to carry out KYC procedures on any client introduced to it by another financial institution unless the financial institution is an eligible introducer able to provide the financial institution with copies of all documentation required by the financial institution's KYC procedures.

293. A financial institution should:

i. Document in a written agreement the respective responsibilities of the two parties;

ii. Satisfy itself that the entity or introducer has in place KYC practices at least equivalent to those required by Belizean law and the financial institution itself and that the third party is regulated and supervised and is effectively implementing the FATF Recommendations on regulation, supervision and monitoring;

iii. Carry out a risk assessment to determine whether it is appropriate for it to rely on the intermediary or third party and, if so, whether it should put in place any measures to mitigate the additional risk;

a. the stature and regulatory track record of the intermediary or third party;

b. the adequacy of the framework to combat ML and TF in place in the country in which the intermediary or third party is based and the period of time that the framework has been in place;

c. the adequacy of the supervisory regime to combat ML and TF to which the intermediary or third party is subject;

d. the adequacy of the measures to combat ML and TF in place at the intermediary or third party;

e. previous experience gained from existing relationships connected with the intermediary or third party;

f. the nature of the business conducted by the intermediary or third party;

g. whether relationships are conducted by the intermediary or third party on a face-to-face basis;

h. whether specific relationships are fully managed by an introducer;

i. the extent to which the intermediary or third party itself relies on third parties to identify its customers and to hold evidence of identity or to conduct other due diligence procedures, and if so who those third parties are; and

j. whether or not specific intermediary or introduced relationships involve politically exposed persons, family members or close associates of politically exposed persons or other higher risk relationships.

iv. Maintain ultimate responsibility for customer identification and verification of customer identity.

v. Immediately obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship without delay;

vi. Satisfy itself that an introducer continues to conform to the criteria set out above (e.g., conduct periodic reviews);

vii. Consider terminating the relationship where an introducer fails to provide the requisite customer identification and verification documents; and

viii. Consider terminating the relationship with an introducer who is not within the financial institution's group, where there are persistent deviations from the written agreement.

294. The Central Bank, as Supervisory Authority, may extend the status of eligible introducer to banks or financial institutions subject to specific guidance. An eligible introducer must be one of the following regulated financial institutions:

i. A bank or financial institution licensed by the Central Bank; or

ii. A company carrying on life assurance business as regulated by the Supervisor of Insurance;

295. A foreign financial institution may also act as an eligible introducer if it meets all of the following conditions:

i. It must exercise functions similar to those of the financial institutions listed at paragraph 245 (i-ii) above;

ii. It must be based in a country with equivalent or higher AML/CFT/CPF standards of regulation; and

iii. There must be no obstacles which would prevent the financial institution from obtaining the original documentation.

296. When a prospective customer is introduced from within a financial institution's group, provided the identity of the customer has been verified by the introducing regulated parent company, branch, subsidiary or associate in line with the standards set out in these Guidelines, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. However, the financial institution should:

i. Satisfy itself that the group applies CDD and record keeping requirements and programmes against ML/TF/PF;

ii. Ensure that the implementation of the CDD and recordkeeping requirements are supervised at a group level by the relevant Supervisory Authority;

iii. Ensure that any higher country risk, as publicly identified by FATF as a country with strategic AML/CFT/CPF deficiencies, is adequately mitigated by the AML/CFT/CPF policies of the group;

iv. Retain copies of the identification records in accordance with the requirements in the MLTPA; and

v. Obtain written confirmation from a group member confirming completion of verification (**See Appendix 7**).

297. Where a third party satisfies the definition of eligible introducer, a financial institution may place reliance upon the KYC procedures of the eligible introducer; but remains ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the eligible introducer that is being relied upon is satisfactory for these purposes. Satisfactory evidence is evidence that the eligible introducer is subject to AML/CFT/CPF standards of regulation that are equivalent to or higher than such standards in Belize. Only senior management should take the decision that reliance may be placed on the eligible introducer and the basis for deciding that normal due diligence procedures need not be followed should be part of the financial institution's risk-based assessment.

298. Notwithstanding any reliance on an eligible introducer's KYC procedures, a financial institution should ensure that it immediately obtains all the relevant information pertaining to a customer's identity. The financial institution is ultimate responsibility for customer identification and verification of customer identity. The Central Bank will also require that a financial institution has clear and legible copies of all documentation in its possession within 30 days of receipt of written confirmation of the eligible introducer that they have verified customer identity in accordance with their national

laws. The eligible introducer must certify that any photocopies forwarded are identical with the corresponding originals. This certification should be provided by a senior member of the introducer's management team and may be endorsed on the written confirmation (that a client's identity has been verified) provided by the introducer. If documents are not obtained within 30 days of receipt of the introducer's written confirmation, the account should be suspended and if after a further reasonable period, the financial institution still does not receive the documents, the business relationship must be terminated.

4.8.5 Professional Service Providers

299. Professional service providers act as intermediaries between clients and the financial institution. They include lawyers, accountants and other third parties that act as financial liaisons for their clients. When establishing and maintaining relationships with professional service providers, a financial institution should:

i. Verify the identity of the professional service provider;

ii. Adequately assess account risk and monitor the relationship for suspicious or unusual activity;

iii. Understand the intended use of the account, including the anticipated transaction volume, products and services used, and geographic locations involved in the relationship; and

iv. Obtain the identity of the beneficial owners of the client funds where it is not satisfied that the intermediary has in place due diligence procedures equivalent to the standard of these Guidelines.

300. Where pooled accounts are managed by:

i. Providers on behalf of entities such as mutual funds and pension funds; or

ii. Lawyers or stockbrokers representing funds held on deposit or in escrow for several individuals, and funds being held are not co-mingled (i.e., there are sub-accounts), the financial institution should identify each beneficial owner. Where funds are co-mingled, the financial institution should take reasonable measures to identify the beneficial owners. Subject to the Bank's approval, the latter is not required where the provider employs at minimum, equivalent due diligence standards as set out in these Guidelines and has systems and controls to allocate the assets to the relevant beneficiaries.

301. A copy of the professional service provider's license and a Certificate of Good Standing from the Registrar of Companies should be obtained to confirm its existence and legal standing.

302. In cases whether the professional service provider and the product iIs an account into which monies are pooled, provided that where the pooled account is held in a country other than Belize, the financial institution must ensure the following:

i. The country imposes requirements to combat ML/TF which are equivalent to those in the MLTPA and these Guidelines;

ii. The independent professional has effectively implemented those requirements;

iii. The independent professional is supervised for AML/CFT/CPF requirements; and

iv. Information on the identity of the persons on whose behalf monies are held in the pooled account is available on request to the institution which acts as a custodian for the account.

4.8.6 High-Risk Countries

303. Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to a financial institution. Conducting business relationships with customers who are either citizens of or domiciled in such countries exposes the financial institution to reputational risk and legal risk. A financial institution is encouraged to consult publicly available information to ensure that they are aware of countries/territories which may pose a higher risk. A financial institution should refer to **Appendix 2** for a list of relevant websites.

304. Caution should also be exercised in respect of the acceptance of certified documentation from individuals and entities located in high-risk countries and territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability. Where transactions to and from such countries appear to have no economic or visible lawful purpose, a financial institution should investigate the background and purpose of such transactions, as far as is reasonably practicable, and document findings.

4.8.7 Bearer Shares

305. Bearer shares can provide a significant level of anonymity, which can be abused by those seeking to use companies for criminal intent. Financial institutions should be cautious with such legal persons, and legal arrangements as the use of bearer shares may serve to obscure beneficial ownership.

306. In assessing the risks of a particular business relationship or transaction, financial institutions should consider whether any legal person or arrangement that is a customer, beneficial owner or other associated person has issued or has the potential to issue bearer shares.

307. Where a financial institution decides that companies registered in Belize represent an acceptable business risk, the financial institution should ensure that the bearer shares are retained by the registered agent. Furthermore, the financial institution should sign an undertaking for the registered agent to inform the financial institution of any proposed change in ownership of the company or of any changes to records relating to these shares.

308. Where a financial institution decides that companies not registered in Belize, with nominee shareholders represent an acceptable business risk, they should exercise care in conducting transactions. A financial institution should employ enhanced due diligence measures to ensure it can identify the beneficial owners of such companies and should immobilize bearer shares as a means of monitoring the identity of such companies by, for example, requiring custody by:

i. The financial institution, or its subsidiary, regulated affiliate, parent or holding company;

ii. A recognized regulated financial institution in a jurisdiction with equivalent AML/CFT/CPF standards; and

iii. Requiring the prior approval before shares can be exchanged. Towards this end, procedures should be established that at a minimum, requires the financial institution to:

a. Obtain an undertaking in writing from the beneficial owner stating that immediate notification will be given to the financial institution if the shares are transferred to another party;

b. Ensure that where bearer shares are not held by the financial institution, they are held in secure custody by a named custodian which has undertaken to inform the financial institution of any proposed change in ownership of the company or of any changes to records relating to these shares and the custodian; and

c. Have the undertaking certified by an accountant, lawyer or equivalent professional, depending on the risk assessment of the customer.

309. Financial institutions should open accounts for legal persons or arrangements capable of issuing bearer shares only where the holders and, where different, the ultimate beneficial owners are identified and verified.

310. Where a potential or existing customer refuses to allow the immobilization of all bearer instruments, financial institutions should terminate or decline to accept the business relationship or transaction and must consider whether any reporting requirements have been implicated.

4.8.8 Correspondent Banking

311. Correspondent banking relates to the provision of banking services by one bank (correspondent) to another bank, usually domiciled overseas (respondent). A correspondent bank faces added risks, as it may have no relationship with the customers of the respondent bank. Examples of correspondent banking include wire/fund transfers, trade related and treasury/money market activities.

312. The decision to approve a respondent relationship should depend, *inter alia*, on the financial institution's assessment of the counterpart's ML/TF prevention and detection systems and controls, and the quality of bank supervision and regulation in the counterpart's country.

313. Banks and financial institutions should not enter into or continue correspondent banking relationships with shell banks.

314. A financial institution that offers correspondent banking services should obtain senior management approval before establishing new correspondent relationships. Towards this end, a financial institution should conduct due diligence on its respondent banks on a risk basis and a review of the correspondent banking relationship should be conducted at least annually.

315. Where a correspondent relationship involves the maintenance of "payable-through accounts", financial institutions should be satisfied that the respondent financial institution has performed all the normal CDD obligations on those customers that have direct access to the accounts of the correspondent financial institution and the respondent financial institution is able to provide customer identification data upon request to the correspondent financial institution.

316. A financial institution should obtain the following on the respondent bank:

i. Information on the ownership, board and senior management;

ii. Nature of the respondent's business;

iii. Assessment of the risk profile (consider the location and nature of major business activities, customer base and determine from publicly available information the reputation of the respondent);

iv. Satisfy itself that there is an adequate AML/CFTAML/CFT/CPF programme in place and is compliant with FATF Recommendations. This includes understanding whether relationships are conducted by the respondent on a non-face-to-face basis and the extent to which the respondent relies on third-parties to identify and hold evidence of identity to conduct other due diligence on its customers;

v. Confirmation that the respondent does not maintain business relations with shell banks;

vi. Assessment of the quality of bank supervision and regulation in the respondent's country, including whether it has been subject to a ML/TF investigation or regulatory action; and

vii. Evidence of senior management's approval before establishing the relationship.

317. A financial institution should document the responsibilities of each institution in relation to KYC measures.

318. Transactions conducted through correspondent relationships need to be monitored according to perceived risk. Where the respondent bank or counterparty is not regulated by a country with equivalent or higher AML/CFT/CPF standards of regulations, additional due diligence should be carried out.

319. Where a relationship is deemed high-risk e.g., located in a high-risk jurisdiction, further to standard due diligence, a financial institution should undertake a more detailed understanding of the:

i. AML/CFT/CPF programme of the respondent bank and its effectiveness;

ii. Effectiveness of the respondent's group programme;

iii. Respondent's owners, directors, and senior managers; and

iv. Ownership structure.

320. The volume and nature of transactions from high-risk jurisdictions flowing through respondent accounts provided by a financial institution or those with material deficiencies should be monitored against expected levels and destinations and any material variances should be explored.

321. Staff dealing with correspondent banking accounts should be trained to recognize high-risk circumstances and be prepared to challenge respondents over irregular activity, whether isolated transactions or trends, and file an STR where appropriate.

322. A financial institution should guard against passing funds through accounts without taking reasonable steps to satisfy itself that sufficient due diligence has been undertaken by the remitting bank on the underlying client and the origin of funds. In these circumstances, the financial institution must be satisfied that the respondent institution is able to provide KYC documentation on the underlying customer, upon request.

323. Financial institutions should ensure that the correspondent banking relationship and its transactions are subject to annual review by senior management.

324. A financial institution should consider terminating the accounts of respondents who fail to provide satisfactory answers to reasonable inquiries including, where appropriate, confirming the identity of customers involved in unusual or suspicious transactions.

325. Financial institutions should not enter or continue a banking relationship whether there is knowledge or suspicion that the respondent or any of its customers are engaged in ML, TF or violating freezing obligations.

326. Where it acts as the ordering financial institution, the financial institution should obtain, retain and verify the full originator information, i.e., the originator's name, account number (or unique identifier where the originator is not an account holder), and address[4] for wire transfers in any amount. Verification of existing customers should be refreshed where there are doubts about previously obtained information. A financial institution should apply enhanced scrutiny for wire transfers that do not contain complete originator information.

327. As ordering financial institution, the financial institution should include in cross-border wire transfers above the BZ$2,000 threshold, full originator information in the message or payment form accompanying the wire transfer. Batch transfers that include cross-border wire transfers sent by a money/value transfer service provider should be treated as cross-border transfers.

328. As the ordering financial institution conducting a domestic transfer above the BZ$2,000 threshold, the financial institution should include full originator information. However, the financial institution may send only the originator's account number (or unique identifier) where full originator information can be made available to:

i. The receiving financial institution and the Bank within three business days of receipt of a request; and

ii. Domestic law enforcement authorities upon request.

329. On the other end of the spectrum, respondent banks should apply similar considerations when entering a correspondent banking relationship. A financial institution that is a respondent bank should obtain the following on the correspondent bank:

i. Information on the ownership, board and senior management;

ii. Assessment of the risk profile (consider the location and nature of major business activities);

iii. Satisfy itself that there is an adequate AML/CFT/CPF programme in place; and

iv. Evidence of senior management's approval before establishing the relationship.

[4] It is permissible to substitute national identity number/customer identity number/date and place of birth.

4.9 Reduced Customer Due Diligence

330. As discussed in the section on **Implementation of Risk-based Approach**, the financial institution's policy document should clearly define the risk categories/approach adopted and associated due diligence, monitoring, and other requirements. All financial institutions governed by these Guidelines should be licensed/registered and appropriately regulated and may apply reduced due diligence to a customer provided it satisfies itself that the customer is of such a risk level that qualifies for this treatment.

331. As a general rule concerning any business relationship or occasional transaction, financial institutions must apply the full range of CDD measures, including the requirements to identify and verify the identity of the customer, the ownership and control structure of the customer, beneficial owners, the person having the position of chief executive or similar or equivalent position and any other persons with an ownership or controlling interest in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the financial institutions.

332. In limited circumstances, where the cumulative ML/TF risks are low, financial institutions may consider applying reduced or simplified CDD measures in accordance with the Central Bank's Simplified Due Diligence Guidelines and this guidance.

333. The application of simplified due diligence measures is permissible only after assessing the ML/TF risks associated with a business relationship or occasional transaction and the products, services, delivery channels, or countries or geographic areas with which the customer engages. Determinations concerning the application of simplified due diligence measures must be made only after considering the results of Belize's national risk assessment and the risk assessments carried out by the financial institutions.

334. Financial institutions may consider applying reduced or simplified due diligence measures only in circumstances such as:

i. Where an application to conduct business is made by a financial institution that is subject to requirements to combat ML/TF consistent with FATF Recommendations and is supervised for compliance with those requirements, such as:

a. An entity regulated by the Central Bank under the DBFIA or IBA;

b. An entity regulated by the Supervisor of Insurance in Belize;

c. An entity regulated by the Registrar of Credit Unions in Belize; or

d. A statutory body.

ii. Where there is a transaction or series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity;

iii. Public companies that are listed on a stock exchange or similar situations that are subject to regulatory disclosure requirements;

iv. Government administrations or enterprises;

v. Life insurance policies where the annual premium is no more than BZ$2,000 or a single premium of no more than BZ$5,000;

vi. Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

vii. A pension superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

viii. Beneficial owners of pooled accounts held by designated non-financial businesspersons if they are subject to requirements to combat ML/TF consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring compliance with those requirements.

ix. Where an existing customer opens a new account unless the condition described at sub-item (ii) above holds. However, if the source of funds/wealth originates from an external source, or from a country where, for example, it is believed that there is a high level of drug trafficking or corruption, reduced due diligence should not apply.

x. Where a financial institution acquires the business of another regulated entity, whether in Belize or elsewhere, and it is satisfied that the due diligence standards of the acquired institution are at least equivalent to that set in these Guidelines, it need not re-verify the customers.

335. Reduced CDD measures may only be applied if the financial institution has conducted and documented a risk assessment.

336. Reduced CDD measures may only be applied to customers resident in another country if that country has effectively implemented the FATF Recommendations.

337. Reduced CDD measures are not acceptable whenever there is suspicion of ML or TF, or specific higher-risk scenarios apply.

338. Financial institutions are permitted to determine the extent of CDD measures that may be applied on a risk-sensitive basis, consistent with these Guidelines.

339. Financial institutions should keep risk findings up to date and in writing, such that any circumstances affecting the assessed risks are identified and fully considered in determining whether the risk findings remain appropriate or whether they must be revised.

340. Irrespective of whether a financial institution ultimately determines that reduced or simplified due diligence is appropriate, the financial institutions should document its deliberations and the full rationale behind its decision. A financial institution should ensure that its documented deliberations and reasoning are available promptly upon request to authorized authorities to demonstrate that it has met its CDD requirements.

341. If the financial institution is not satisfied that equivalent standards have been followed or the customer records are not consistent with the requirements of these Guidelines, the financial institution should seek to identify and verify the identity of customers who do not have existing relationships with the

financial institution.

342. Financial institutions should determine whether products meet the criteria for simplified due diligence and ensure that any reduced or simplified CDD measures applied are commensurate with the assessed risks.

343. Financial institutions may, based on their risk assessments, apply simplified CDD to specifically defined lower-risk customers or products and services. Such instances may include but are not limited to:

i. Customers whose sole source of funds is a salary credit to an account or with a regular source of income from a known source which supports the activity being undertaken;

ii. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment); and

iii. Financial products or services that provide appropriately defined and limited services to certain types of customers. For customers who do not have photo identification or have limited identification documentation such as tourists or those who are socially or economically vulnerable such as the disabled, elderly, minors, or students, a 'tiered' CDD approach allows financial access with limited functionality. For example, a financial institution may offer banking accounts with low transaction/payment/balance limits with reduced documentation requirements.

iv. Access to additional services such as higher transaction limits or account balances or access to diversified delivery channels should only be allowed if and when the customer can satisfy additional identification requirements. Where this obtains financial institutions must have monitoring systems to ensure that transaction and balance limits are observed.

344. Where a financial institution decides to apply reduced or simplified CDD measures, it must:

a. Maintain and document up-to-date risk findings concerning the products, services, customers, business relationships (including outsourcing and reliance relationships), countries and geographic areas associated with the business;

b. Ensure that the level of CDD applied is commensurate with the assessed risks;
Conduct ongoing monitoring of the business relationship;
Report any knowledge or suspicion of ML/TF; and

c. Where relying upon another person or financial institutions for the purposes of applying CDD, periodically test the quality of the CDD measures the relied upon entity applies and the willingness and ability of the relied upon entity to provide CDD information upon request.

4.9.1 Examples of Simplified Due Diligence Measures

345. The Simplified CDD measures described below are for guidance only and should be read in conjunction with Simplified Due Diligence Guidelines issued by the Central Bank. **See** Appendix 8 for minimum simplified CDD measures allowed by the Central Bank.

346. Where a financial institution determines, based on its risk assessment that the ML/TF risks are low, the financial institution may apply one or more of the following Simplified CDD measures:

i. Adjust the timing of CDD where the product or transaction has features that limit its use for ML/TF purposes.

Financial institutions may verify the customer's or beneficial owner's identity after the establishment of the business relationship where financial products or services provided have limited functionality or restricted services to certain types of customers for financial inclusion purposes. For example, limits may be imposed on the number or total value of transactions per week/month; the product or service may only be offered to nationals or only domestic transactions may be allowed. Verification of identity may occur when the transaction threshold or time limit is met. Similarly, general insurance products such as car insurance present low ML/TF risk so verification of identity may be postponed until there is a claim or until the customer requests additional insurance products. In such instances, financial institutions must ensure that:

a. This does not result in a de facto exemption from CDD and that the customer or beneficial owner's identity will ultimately be verified.

b. The threshold or time limit is set at a reasonably low level;

c. Systems are in place to detect when the threshold or time limit has been reached; and

d. CDD is not deferred or obtaining relevant information about the customer is not delayed where higher risk factors exist or where there is suspicion of ML/TF.

ii. Adjust the quantity of information requested from the customer for identification, verification or monitoring purposes.

Customers warranting Simplified CDD based on their risk profile should not be required to produce two (2) forms of ID as a minimum requirement. Financial institutions may:

a. Verify identity on the basis of one document only; or

b. Assume the nature and purpose of the business relationship because the product is designed for one particular use only.

iii. Adjust the quality or source of information obtained for identification, verification, or monitoring purposes.

Where the risk associated with all aspects of the relationship is very low, financial institutions may rely on the source of funds to meet some of the CDD requirements, for example, the purpose and intended nature of the relationship may be inferred where the sole inflow of funds are government pension or benefit payments.

iv. Adjust the frequency of CDD updates and reviews of the business relationship.

For example, this may be applied when trigger events occur such as the customer requesting a new product or service or when a certain transaction threshold is reached. Financial institutions

must ensure that this does not result in a de facto exemption from keeping CDD information up-to-date.

v. Adjust the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only.

Where financial institutions choose to do this, they must ensure that the threshold is set at a reasonable level and that systems are in place to identify linked transactions which, when aggregated, exceed the threshold.

4.10 Retrospective Due Diligence

347. Where the identity information held on existing customers does not comply with the requirements of these Guidelines, a financial institution is required to develop a programme for ensuring compliance (within a two-year time frame in accordance with the section on **Implementation of Risk-Based Approach** in these Guidelines), based on materiality and risk. A financial institution should:

i. Record its non-compliant business relationships, noting what information or documentation is missing;

ii. Establish a framework for effecting retrospective due diligence, including the setting of deadlines for the completion of each risk category. The timing of retrofitting can be linked to the occurrence of a significant transaction, when the customer documentation standards change substantially, when there is a material change in the way that an account is operating, when the institution becomes aware that it lacks sufficient information about an existing customer or when there are doubts about previously obtained CDD data; and

iii. Establish policies for coping with an inability to obtain information and documentation, including terminating the relationship and making a suspicious report.

348. Where a financial institution deems on the basis of risk and materiality, that it is not practical to retrofit a customer (e.g., the settlor has died; the account is inactive or dormant), exemption of such accounts should be approved by the Compliance Officer and senior management, ratified by the board and documented on the individual's file.

4.11 Termination of Relationship

4.11.1 Requirements to Cease Transactions

349. If a financial institution is unable to apply CDD measures including ongoing monitoring in relation to a customer, then, the financial institution must:

i. In the case of a proposed account or transaction, not open the account or carry out the transaction for the customer;

ii. In the case of a proposed business relationship or occasional transaction, not establish that business relationship or carry out that occasional transaction with the customer;

iii. In the case of an existing business relationship, terminate the business relationship with the customer; and

iv. In the case where the financial institution has doubt about the veracity or adequacy of previously obtained customer information, not establish the relationship or terminate the business relationship; and

v. Consider whether the financial institution is required to make a disclosure to the FIU in accordance with its obligations under the MLTPA and this guideline.

350. Where the immediate termination of a business relationship is impracticable due to contractual or legal reasons outside of the control of the financial institution, the financial institution must ensure that the risk is managed and mitigated effectively until such time as termination of the relationship is practicable.

351. Where funds have already been received and the financial institution concludes that the circumstances support the making of a report to the FIU, the financial institution must retain the funds until a competent authority has given consent for the funds to be transferred to another account or person.

352. Where funds have already been received and the financial institution concludes that there are no grounds for making a report to the FIU, the financial institution will need to determine whether to retain the funds while seeking other ways of being reasonably satisfied as to the customer's identity, or whether to return the funds to the original source from which they came. Returning the funds in such circumstances is part of the process of terminating the business relationship; it is closing the account rather than carrying out a transaction with or on behalf of the customer.

SECTION V - ELECTRONIC PAYMENTS TRANSFERS

5.1 Wire/Funds Transfers

353. For the purpose of these Guidelines, wire transfer and funds transfer refer to any transaction carried out on behalf of an originator through a financial institution by electronic means for availability to a beneficiary at a beneficiary financial institution. The originator and the beneficiary may be the same person.

5.1.1 Pre-Conditions for Making Funds Transfers – Verification of Identity of Originators

354. A financial institution that initiates wire transfers on behalf of originators ("originating financial institutions") must ensure that the originator information conveyed in the payment message or instruction is accurate and has been verified.

355. The verification requirement is deemed to be met for account holding customers of the originating financial institution once the customer's identity has been verified and the verification documentation has been retained. In such cases, the originating financial institution may assign to the wire transfer a unique identifier that would link the account holding customer and his relevant identification information to the wire transfer.

356. Before initiating one-off wire transfers on the instructions of non-account holding customers, the originating financial institution must verify the identity, address, and source of funds, if necessary, of the originator.

357. The originating financial institution may apply simplified due diligence for wire transfers below BZ$2,000 provided that such transfers are considered to present a low risk of ML or TF.

5.1.2 Cross-Border Wire Transfers – Complete Originator Information

358. Complete information must accompany all wire transfers for both the originator and beneficiary.

359. Complete information on the originator means the originator's:

a. Name;

b. Address; and

c. Account number.

360. Complete information on the beneficiary means the beneficiary's:

a. Name; and

b. Account number.

361. Where the originator is a natural person, the originator's address may be substituted with the originator's date and place of birth, customer identification number or national identity number.

362. Where an originator or beneficiary does not have an account number, the PSP must substitute it with a unique identifier that allows the transaction to be traced to the beneficiary.

363. Where the originator is a legal person, the address should be the address where the company's business is conducted.

364. Where the originator is a trust or trustee, the address should be the address of the trustee.

365. Where an originator is a bank acting on its own behalf and not on behalf of any underlying customer, the Bank Identifier Code (BIC) constitutes complete Originator information. Nonetheless, the account number should be included where available. Where an originator has a Business Entity Identifier (BEI) or Legal Entity Identifier (LEI), the BEI or LEI, together with the account number, constitute complete Originator information. Institutions utilizing BICs, BEIs or LEIs should be aware that the omission of an address may result in requests for the address from an intermediary financial institution or beneficiary financial institution.

366. The extent of the information supplied in each field of the payments message will be subject to the conventions of the messaging system used. For example, where the wire transfer is debited from a joint account, the originating financial institution may demonstrate that it has met its legal obligation to provide an originator's name where, dependent upon the size of the field, it provides the name of one or more account holders.

367. Where the wire transfer is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier or transaction number which permits the transfer to be traced back to the originator. Unique identifier is defined as a combination of letters, numbers or symbols determined by a financial institution in accordance with the protocols of the payment and settlement system, or messaging system, used to effect the transfer of funds. Similarly, the transaction number should identify and link a particular Originator to the wire transfer.

368. Only the address of an originator may be substituted with the originator's date and place of birth, or national identity number or customer identification number. A national identity number may be used for originators resident in countries that issue such numbers. However, for originators resident in other countries, it must be remembered that other numbers such as a National Insurance or Social Security number, passport number or driver's license number are not National Identity Numbers. A customer identification number may be an internal reference number that is created by the originating financial institution which identifies an originator, and which will continue throughout a business relationship, or may be a number contained in an official document such as National Insurance or Social Security number, passport number or driver's license number.

369. Originators should be provided with an opportunity to request substitute information for an address on transfers. It follows that in the event a beneficiary financial institution (i.e., a financial institution that receives funds on behalf of a beneficiary) demands the originator's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the originator's consent or under judicial compulsion should the address be additionally provided.

5.1.3 Originating Financial Institution

370. Originating financial institutions must ensure that each cross-border transfer of funds includes complete information on the originator and beneficiary.

371. Where the originator is an accountholder at the Originating financial institutions, the originating financial institutions must ensure, before transferring funds, that the complete information on the originator conveyed in the payment is accurate and has been verified.

372. The complete information of an account-holding originator is accurate and verified if the information has been satisfactorily obtained and verified, in accordance with the MLTPA and these Guidelines. Nevertheless, several factors may cause a PSP to conduct additional CDD on an accountholder prior to authorizing the transfer. These factors include but are not limited to the financial institution's risk tolerance and risk assessments, the involvement of any third-party service provider, the involvement of higher-risk persons or jurisdictions and the size and nature of the transfer that has been requested in the context of the accountholder's previous transactions and conduct.

373. In the case of a transfer from a joint account, a financial institution may demonstrate that it has met its legal obligation to provide a customer name where, dependent on the size of the field, it provides the name of either or both account holders.

374. Financial institutions should send payments through a messaging system capable of carrying all of the complete information on the originator and beneficiary. Where the size or types of a messaging system's fields are such that the complete information cannot be included, the financial institutions should use a different messaging system or provide the complete information to the beneficiary financial institutions and any intermediary financial institutions by an agreed form of communication, whether within a messaging system or otherwise.

375. The originator's name, address (or permitted alternative) and account number should match the information that the financial institutions hold in respect of the originator's account(s). Financial institutions generally populate the messaging system's information fields from customer databases. Any request to alter the customer information sent via the messaging system should be subject to a rigorous and documented referral and approval mechanism. This is to ensure that any altered transfer instruction is approved on an exceptional basis only in cases where the financial institutions is entirely

satisfied that the reason for quoting alternative information with an originator's account number is legitimate.

376. Where the originator is not an accountholder and the transfer is $2,000 or less, the originating financial institutions must obtain information establishing the originator's identity and address. Where the address is substituted with an originator's date and place of birth, customer identification number or national identity number, that customer information must be obtained. Financial institutions are not required to verify the information obtained for such transactions; nonetheless, it is advisable to do so in all cases. Where a transaction is carried out in several operations that appear to be linked and together exceed $2,000, the verification requirements are to apply.

377. Where the originator or beneficiary is not an accountholder or the transfer is otherwise not drawn from a bank account, the originator or beneficiary's financial institutions, respectively, must produce and include with the transfer a unique identifier that allows the transaction to be traced back to the originator or beneficiary.

378. The unique identifier identifies a payment and allows it to be traced back to an originator or beneficiary. The customer identification number identifies an originator or beneficiary and refers to a record held by the originator or beneficiary PSP, respectively, that contains a customer's name and address, national identity number and/or date and place of birth.

379. For all transfers of funds, where all the required information is not available or where any of the information that is available is meaningless or otherwise incomplete, originating financial institutions must not allow the transfer to be executed. In practice, some messaging systems will allow a transfer to proceed without each required field being populated. Financial institutions should nonetheless have risk-based policies, procedures, and controls to identify and ensure the prevention of any transfers for which meaningless or incomplete information has been included in any field.

380. Originating financial institutions should consider all aspects of ordering and executing a transfer as factors in assessing whether there is knowledge, suspicion, or reasonable grounds for suspicion of ML/TF with respect to any transfer of funds or any related transaction. Circumstances that may indicate knowledge, suspicion, or reasonable grounds for suspicion of ML/TF include, but are not limited to:

i. An originator who is unwilling or unable to provide the complete information required;

ii. An originator for whom the complete information cannot be verified, where it is required to do so;

iii. An originator seeking to alter the customer information sent via the messaging system for reasons that the financial institution is not able to fully confirm as legitimate;

iv. A transfer with missing, meaningless or otherwise incomplete information;

v. An originator seeking to route the transaction through apparently unnecessary intermediary financial institutions; and

vi. An originator seeking to ensure that the complete information does not reach all financial institutions involved in the execution of the payment.

381. The originating financial institutions must keep records for five years of complete information on the originator and beneficiary that accompanies transfers of funds. The originating financial institutions should also maintain records of all information received from the beneficiary financial institutions and any intermediary financial institution, including requests for information. All records should be kept in accordance with the guidance provided in the record-keeping requirements.

5.1.4 Domestic Wire Transfers – Reduced Originator Information

382. Where the originating and beneficiary financial institution are both located within Belize, wire transfers need be accompanied only by the originator's account number or a unique identifier or a transaction number which permits the transaction to be traced back to the originator. However, if requested by the beneficiary financial institution, complete originator information must be provided by the originating financial institution within three business days of such request from the beneficiary financial institution or supervisory authority.

5.1.5 Batch File Transfers

383. Where there is a batch file transfer from a single originator and the beneficiary PSP is situated outside Belize, complete information will be considered to have been transferred, provided that:

i. The batch file transfer contains complete information on the Originator and each of the beneficiaries for each individual transfer;

ii. The individual transfers of funds carry the account number of the Originator or a unique identifier where an account number is not available; and

iii. The complete information provided on all beneficiaries is fully traceable within the beneficiary country. Only routine transactions should be batched.

5.1.6 Wire Transfers via Intermediaries

384. An intermediary financial institution is a financial institution, other than the originating or beneficiary financial institution, that participates in the execution of funds transfers. Intermediary financial institutions must, subject to the following guidance on technical limitations, ensure that all information received on the originator which accompanies a wire transfer is retained with the transfer throughout the payment chain. Intermediary financial institutions must ensure that, for each cross-border transfer of funds, all information received on the originator and beneficiary is kept with the transfer.

385. Intermediary financial institutions should forward transfers through a messaging system capable of carrying all the complete information on the originator and beneficiary.

386. Where technical limitations associated with a messaging system prevent all information received on the originator and beneficiary from accompanying the transfer, an intermediary financial institution may nonetheless use the messaging system with technical limitations, provided that:

i. The intermediary financial institution informs the beneficiary financial institution and any downstream intermediary financial institutions of any missing, meaningless, or otherwise incomplete information by an agreed form of communication, whether within a messaging service or otherwise; The intermediary financial institution keeps a record, for at least five years,

of all the information received from the originating financial institution or any other intermediary financial institution; and

ii. Within three working days of receiving any request from the beneficiary financial institution, the intermediary financial institution makes available to the beneficiary financial institution all the information on the originator or beneficiary that the intermediary financial institution has received.

387. Intermediary financial institutions must take reasonable measures commensurate with their risk-based policies, procedures, and controls and consistent with straight-through processing to identify transfers of funds that lack complete information for the originator or beneficiary.

388. Where an intermediary financial institution becomes aware, when receiving a transfer of funds, that information on the originator or beneficiary is incomplete or missing, the intermediary financial institution must either:

i. Reject the transfer;

ii. Request the complete information on the Originator and beneficiary; or

iii. Make an internal SAR to the reporting officer.

389. Where it knows or suspects that information provided by the originating financial institution has been stripped or altered at any point in the payment chain.

390. At all times, financial institutions must adhere to the acts, regulations, and guidelines regarding tipping-off offences.

391. Where an originating financial institution or intermediary financial institution regularly fails to supply complete information, the intermediary financial institution must report that fact to the Central Bank and must take steps to attempt to ensure that the originating financial institution or intermediary financial institution provides complete information. Those steps may include:

i. Issuing warnings to the originating financial institution or intermediary financial institution;

ii. Setting deadlines for the originating financial institution or intermediary financial institution to provide complete information;

iii. Rejecting future transfers from the originating financial institution or intermediary financial institution; or

iv. Determining whether to restrict or terminate the business relationship with the originating financial institution or intermediary financial institution.

392. Intermediary financial institutions should have risk-based policies, procedures, and controls for the following:

i. Identifying transfers, including those carried out with straight-through processing, that lack complete information or include meaningless or otherwise incomplete information;

ii. Determining when to execute, reject or suspend such transfers; and

iii. Determining appropriate follow-up action with originating financial institutions, beneficiary financial institutions, other intermediary financial institutions, and competent authorities.

393. Intermediary financial institutions should consider all aspects of receiving and forwarding a transfer of funds as factors in assessing whether the transfer of funds or any related transaction is suspicious and whether a report must be made to the reporting officer. Circumstances that may indicate a transfer of funds or any related transaction is suspicious include but are not limited to:

i. A transfer with missing, meaningless or otherwise incomplete information;

ii. A transfer that has been routed through one or more intermediary financial institutions, apparently without a legitimate purpose; and

iii. A transfer that appears to have been routed through the intermediary financial institution for the purpose of preventing information from reaching the beneficiary financial institution.

394. Where a financial institution controls both the originator and beneficiary side of a transfer of funds, the financial institution must:

i. Consider all the information from both the originator and beneficiary sides to determine whether to make a disclosure to the FIU; and

ii. Where a decision is made to make a disclosure to the FIU, the financial institution must also make a disclosure to the relevant financial intelligence unit in any country affected by the transfer of funds and make relevant transaction information available to the FIU.

395. The intermediary financial institution should maintain records of all information received from the originating financial institution, beneficiary financial institution and any other intermediary financial institutions. All information includes information pertaining to the payment, including requests for information, whether received through a messaging system or any other means. All records should be kept in accordance with the record-keeping requirements.

5.2 Record Keeping Requirements

396. A financial institution should maintain all necessary records on transactions, identification data, account files and business correspondence for at least five years following the completion of the transaction, or longer if requested by a competent authority in specific cases and upon proper authority. This applies regardless of whether the account or business relationship is ongoing or has been terminated.

397. The particulars of the wire transfer to be recorded must be of sufficient detail to enable the transfer to be accurately described and reconstructed, to provide evidence for prosecution of criminal activity, if necessary. This information, together with information on the Originator (including the originator's identity verification documentation) must be retained by the originating financial institution for a period of five years from execution of the transfer.

398. A financial institution should ensure that all customer and transaction records and information on wire transfers are made available, on a timely basis, to domestic competent authorities upon

appropriate authority.

5.3 Beneficiary Financial Institutions – Checking Incoming Payments

399. Prior to transferring funds, a beneficiary financial institution must ensure that the identity of the beneficiary is accurate and verified for any transfer of funds over $2,000 and for any transfer of funds that is carried out in several operations that appear to be linked and together exceed $2,000.

400. Where the beneficiary is an accountholder at the beneficiary financial institution, the beneficiary's identity is accurate and verified if the information has been satisfactorily obtained and verified in accordance with the MLTPA and these Guidelines. Nevertheless, several factors may cause a PSP to conduct additional CDD on an accountholder before disbursing any funds from the transfer. These factors include but are not limited to the PSP's risk tolerance and risk assessments, the involvement of any third-party service provider, the involvement of higher-risk persons or jurisdictions and the nature of the transfer that has been received in the context of the accountholder's previous transactions and conduct.

401. Where the beneficiary is not an accountholder and the transfer exceeds $2,000, the beneficiary financial institution must satisfactorily obtain and verify the identity of the beneficiary prior to the disbursement of any funds to the beneficiary. In addition, PSPs must verify the beneficiary's identity where a transaction is carried out in several operations that appear to be linked and together exceed $2,000.

402. Where the beneficiary is not an accountholder and the transfer is $2,000 or less, the beneficiary financial institution must obtain information establishing the originator's identity. PSPs are not required to verify the information obtained for such transactions; nonetheless, it is advisable to do so in all cases. Where a transaction is carried out in several operations that appear to be linked and together exceed $2,000, the verification requirements must apply.

403. Where the beneficiary is not an accountholder, the beneficiary financial institution must ensure that the originating financial institution produced and included with the transfer a unique identifier that allows the payment to be traced back to the originator.

404. Beneficiary financial institutions must have effective policies, procedures, and controls, including post-event monitoring or real-time monitoring where feasible, to detect whether incoming transfers of funds include all required information.

405. In practice, some messaging systems will not allow a transfer to reach a beneficiary financial institution without each required field being populated. Beneficiary financial institutions must have risk-based policies, procedures, and controls to identify transfers for which meaningless or incomplete information has been included in any field.

406. Where a beneficiary financial institution becomes aware, while processing a payment, that it is missing required information or that the required information provided is meaningless or otherwise incomplete, the beneficiary financial institution must:

i. Reject the transfer;

ii. Request the complete information on the originator and beneficiary; or

iii. Make an internal STR to the compliance officer.

407. A beneficiary financial institution should also take one or more of the steps outlined above where it knows or suspects that information provided by the originating financial institution, or any intermediary financial institution has been stripped or altered at any point in the payment chain.

408. At all times, PSPs must adhere to the acts, regulations and guidance notes addressing tipping-off offences.

409. Where an originating financial institution is identified as having regularly failed to comply with the originator information requirements, the beneficiary financial institution should give the originating financial institution a reasonable time within which to correct its failures. Where the originating financial institution, after being given a reasonable time within which to do so, fails to provide the missing information, the beneficiary financial institution should either refuse to accept further transfers from that originating financial institution or decide whether to terminate or restrict its business relationship with that originating financial institution. The beneficiary financial institution must advise the Central Bank of any decision to reject future transfers, or to terminate or restrict its relationship with the non-compliant originating financial institution within 10 business days of such decision being taken.

410. Where, despite the beneficiary financial institution taking the steps described above, a originating financial institution still regularly fails to provide all required information on the originator and beneficiary, the beneficiary financial institution must either reject any future transfers of funds from the originating financial institution or determine whether to restrict or terminate the business relationship with the originating financial institution, either completely or in respect of funds transfers.

411. Beneficiary financial institutions should also apply the above steps to intermediary financial institution that regularly fail to provide the complete information on the originator and beneficiary or that regularly fail to provide, upon request, all information received on the originator and beneficiary from the originating financial institutions and any other intermediary PSPs.

412. Where real-time monitoring is not feasible, beneficiary financial institutions must conduct post-event monitoring through the use of risk-based sampling to determine whether complete information on the originator and beneficiary is included with each transfer. Such sampling may include but is not limited to:

i. Cross-border transfers of funds;

ii. Transfers involving higher-risk customers and jurisdictions, as identified by the

iii. PSP's risk assessment processes;

iv. Transfers involving multiple intermediaries;

v. Transfers involving originating financial institutions or intermediary financial institutions that have previously failed to provide all required information;

vi. Transfers involving PSPs known via reliable sources to have stripped or altered information provided by the originating financial institution;

vii. Transfers for which alternative information has been substituted for the originator's address;

viii. Transfers above the $2,000 threshold to non-accountholders; and

ix. Transfer chains involving two or more PSPs that are bound by different sanctions regimes.

413. Beneficiary financial institutions must consider all aspects of receiving a transfer of funds as factors in assessing whether the transfer of funds or any related transaction is suspicious and whether a report must be made to the reporting officer. Circumstances that may indicate a transfer of funds or any related transaction is suspicious or that there are reasonable grounds to be suspicious include but are not limited to:

i. A transfer with missing, meaningless or otherwise incomplete information;

ii. A transfer that has been routed through one or more intermediary PSPs, apparently without a legitimate purpose;

iii. A transfer that appears to have been routed through one or more intermediary PSPs for the purpose of preventing information from reaching the beneficiary financial institution; and

iv. A transfer for which there is evidence to suggest that a person other than the named beneficiary is the intended final recipient.

414. Where a financial institution controls both the originator and beneficiary side of a cross-border transfer of funds, the financial institution must:

i. Consider all the information from both the originator and beneficiary sides to determine whether to make a disclosure to the FIU; and

ii. Where a decision is made to make a disclosure to the FIU, the financial institution must also make a disclosure to the relevant financial intelligence unit in any country affected by the transfer of funds and make relevant transaction information available to the FIU.

415. Although it is possible that a beneficiary may, in fact, be a conduit for an undisclosed 'final recipient' to serve a criminal objective, financial institutions should understand the beneficiary to be the person named in the transfer as the beneficiary of the payment, unless there is evidence to suggest that another person will benefit.

416. The beneficiary financial institution must maintain records of all information received from the originating financial institution and any intermediary financial institution for at least five years. All information includes information that pertains to the transfer, whether received through a messaging system or through any other means. The beneficiary financial institution must also maintain records of its verifications of beneficiary identities. All records should be kept in accordance with the MLTPA and these Guidelines.

417. It is expected that originator information requirements will be met by a combination of the following:

SWIFT payments on which mandatory originator information fields are not completed will fail to process and the payment will not be received by the beneficiary financial institution. Current SWIFT validation prevents payments being received where the mandatory information is not present at

all. However, it is accepted that where the originator information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system.

5.4 Exemptions

418. The following payment types are exempt:

a. Transfers where the originator withdraws cash from his or her own account;

b. Transfers by credit or debit card so long as the beneficiary has an agreement with the financial institution permitting payment for goods or services and a unique identifier (allowing the payment to be traced back to the originator) accompanies all transfers;

c. Direct debits from accounts authorized between two parties so long as a unique identifier, allowing the payment to be traced back to the originator, accompanies all transfers;

d. Transfers to public authorities for the payment of fines, penalties, duties, or other taxes within Belize; and

e. Transfers where both the originator and beneficiary are financial institution acting on their own behalf.

5.5 Minimum Standards

419. The above information requirements are minimum standards. A financial institution may elect to supply complete originator information with transfers which are eligible for a reduced information requirement where systems permit, thereby limiting the likely incidence of inbound requests for complete information. To ensure that the data protection position is beyond any doubt, it would be advisable to ensure that terms and conditions of business include reference to the information being provided.

5.6 Card Transactions

420. As indicated above, credit or debit transactions for goods and services are out of the scope of these requirements provided that a unique identifier, allowing the transaction to be traced back to the originator, accompanies the movement of the funds. The 16-digit Card PAN number serves this function.

421. Complete originator information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a beneficiary's beneficiary financial institution located in Belize.

5.7 Offences and Fines

422. A financial institution that fails to comply with these provisions commits an offence and shall be liable to a fine up to BZ$100,000, as per section 19 of the MLTPA.

SECTION VI - ONGOING MONITORING OF BUSINESS RELATIONSHIPS

423. Once the identification procedures have been completed and the client relationship is established, a financial institution should monitor the conduct of the relationship or account to ensure that it is consistent with the nature of business stated when the relationship or account was opened.

6.1 Monitoring

424. A financial institution is expected to have systems and controls in place to monitor on an ongoing basis, relevant account activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

425. Ongoing monitoring is an integral part of a financial institution's AML/CFT/CPF programme and supports several objectives:

i. Maintaining a proper understanding of a customer's activities;

ii. Ensuring that CDD documents and other records are accurate and up to date;

iii. Providing accurate inputs for the financial institution's risk assessment processes;

iv. Testing the outcomes of the financial institution risk assessment processes; and

v. Detecting and scrutinizing unusual or suspicious transactions.

426. Failure to adequately monitor a customer's business relationship may expose a financial institution to abuse by criminals and may call into question the adequacy of the financial institution AML/CFT/CPF policies, procedures and controls and the integrity or fitness and properness of the financial institution's management.

427. Ongoing monitoring of a business relationship includes:

i. Scrutinizing transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) and other aspects of the business relationship to ensure that the transactions and customer's conduct are consistent with the financial institution's knowledge of the customer and their risk profile;

ii. Investigating the background and purpose of all complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose and recording in writing the findings of the investigation; and determining whether a customer is a PEP;

iii. Determining whether a customer relationship involves a country or territory that represents a higher risk for ML, corruption, TF or being subject to international sanctions, including but not limited to a country that has been identified by the FATF or CFATF as being higher risk;

iv. Reviewing existing documents, data, and information to ensure that they are up to date, adequate and relevant for the purpose of applying CDD measures by undertaking reviews of existing records; and

v. Adjusting risk profiles and risk assessments based on information reviewed.

428. If it appears to a reporting entity that an applicant requesting it to enter into any business relationship or transaction, whether or not in the course of a continuing business relationship, is acting on behalf of another person, the financial institution shall establish the true identity of any person on whose behalf or for whose ultimate benefit the applicant may be acting in the proposed transaction, whether as a trustee, nominee, agent or otherwise.

429. When establishing and maintaining relationships with cash-intensive business, a financial institution should establish policies, procedures, and processes to identify high-risk relationships; assess AML/CFT/CPF risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity.

430. Depending on the type of business each financial institution conducts and the nature of its client portfolio, each may wish to set its own parameters for the identification and further investigation of cash transactions. For those customers deemed to be particularly high-risk, a financial institution should implement sound practices, such as periodic onsite visits, interviews with the business' management, or closer reviews of transactional activity.

431. Financial institution should determine the scope and frequency of ongoing monitoring using a risk-based approach considering the nature, size and complexity of their business and the level of risk to which they are exposed.

432. Financial institutions should direct greater monitoring resources toward those products, services and business relationships presenting a higher risk of ML/TF than those presenting a lower risk. Financial institutions must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of ML/TF.

433. In determining a proper allocation of monitoring resources, financial institutions should consider the:

i. Size and complexity of the financial institution;

ii. Nature, scope and delivery channels of the products and services the financial institution;

iii. Most recently published ML/TF national risk assessments;

iv. Financial institution's own risk assessment findings; and

v. Nature, scope, and effectiveness of the financial institution's existing monitoring systems.

434. With respect to the customer, financial institutions should consider:

i. The nature, amount and frequency of the transactions;

ii. Geographic connections;

iii. Whether the customer is known to use other products and services;

iv. Whether the customer can be categorized according to activity or turnover and whether the customer's conduct falls outside any norms established for any categories identified; and

v. Whether the customer presents a higher than standard risk for ML/TF.

6.2 Keeping CDD Information Up to Date

435. Once a business relationship has been established, reasonable steps should be taken by the institution to ensure that due diligence information is kept up to date.

436. When putting in place policies and procedures to keep CDD information up to date, financial institutions should pay particular attention to the need to remain alert to, and capture, information about the customer that will help them understand whether the risk associated with the business relationship has changed. Examples of the information financial institutions should capture include an apparent change in the source of the customer's funds, marital status, address, ownership structure, or behaviour that is consistently out of line with the behaviour or transaction profile the financial institution had expected.

437. A change in the customer's circumstances is likely to trigger a requirement to apply CDD measures to that customer. In those situations, financial institutions may not need to re-apply all CDD measures, but should determine which CDD measures to apply, and the extent of the CDD measures they will apply. For example, in lower risk cases, financial institutions may be able to draw on information obtained during the business relationship to update the CDD information they hold on the customer.

438. In addition, it is recommended that records for high-risk customers are updated at least annually.

6.3 Establishing Norms

439. Bearing in mind that some criminal activity may be so widespread as to appear to be the norm, financial institutions should establish norms for lawful transactions and conduct for its products or services and for any categories of transaction or customer it designates. Once a financial institution has established norms for lawful transactions and conduct, it must monitor the business relationship, including transactions and patterns of transactions, to identify transactions and conduct falling outside the norm.

440. Where a relationship changes significantly, financial institutions should apply further CDD measures to ensure a proper understanding of the relationship, including its purpose and nature and to determine whether any transaction or conduct is unusual or suspicious.

441. Financial institutions should have policies, procedures, and controls in place for customers who have not had contact with the financial institution for some time, in circumstances where regular contact might be expected. Where an account or relationship is dormant, financial institutions should be able to identify any person seeking reactivation and any unauthorized use.

442. Depending on the nature of the business each financial institution carries out and the nature of its customer portfolio, each financial institution should establish norms for cash transactions and the identification of unusual cash transactions or proposed cash transactions. Given the international

nature of the business conducted by many financial institutions cash transactions may be relatively uncommon, whereas for some banks, credit unions or remittance service providers offering services to local customers, cash transactions may be a normal everyday service.

6.4 Systems for Monitoring

443. Monitoring may take place both in real time as transactions or conduct take place and after the event by reviewing the transactions or conduct that a customer has undertaken. Irrespective, any system of monitoring should ensure at its core that:

i. Transactions and conduct are flagged in exception reports for further review;

ii. The exception reports are reviewed promptly by the appropriate person(s); and

iii. Appropriate and proportionate action is taken to reduce the possibility of ML/TF occurring without detection.

444. A financial institution should calibrate its monitoring systems to identify for review all higher-risk activity, including:

i. All complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose;

ii. Transactions or conduct falling outside of the expected norm for a customer, product, or service; and

iii. Transactions or conduct involving any suspicious transaction or sanction related transaction.

445. ML/TF typologies are numerous and constantly evolving. The employees involved in the design, application and updating of a monitoring system should understand the range of potential indicators of suspicious transactions and conduct as they pertain to the financial institution's products, services, and delivery channels. A financial institution's monitoring system should apply the full range of potential indicators to the transactions and conduct being monitored.

446. A financial institution should not calibrate its monitoring system to produce only the volume of transaction reporting that existing employees are capable of reviewing. Each financial institution should determine if additional compliance resources are necessary to monitor and review the risks present in its business. Likewise, a financial institution should calibrate its monitoring system to avoid producing large numbers of 'false positives', which require excessive employee resources to scrutinize.

6.5 Automated Monitoring System

447. Subject to the needs identified through a financial institution's ongoing risk analysis, a monitoring system may be either manual or automated to the extent that a standard suite of exception reports is produced. Larger financial institutions and financial institutions with greater volume or turnover associated with a particular product or service are more likely to require some level of automated monitoring.

448. Where an automated or computerized system is contemplated, financial institutions should satisfy

themselves that:

i. The system sufficiently monitors for appropriate ML/TF typologies, higher-risk persons and geographic connections;

ii. The typologies, higher-risk persons, and geographic connections for which the system monitors are regularly updated.

iii. The system is appropriate for and/or sufficiently adjustable to the product or service to which it is to be applied; and

iv. The system provides the user with the reasons that unusual customer behaviour or a transaction is flagged.

449. Where an automated monitoring system is used, financial institutions should ensure that staffing levels and skillsets are appropriate for the purpose of overseeing the automated system. Certain tasks and skills cannot be automated, including employee intuition, perceptions acquired through direct interaction with a customer and the ability, through practical experience, to recognize transactions and conduct that appear to fall outside the established norm for a product, service, or customer.

450. It is recognized a computer system may not be a practical option for some financial institutions due to cost, the nature of the business or difficulties of systems integration. In such circumstances a financial institution should ensure it has comparable alternative systems in place, which provide sufficient controls and monitoring capability for the timely detection and reporting of suspicious activity.

6.6 "Hold Mail" Accounts

451. "Hold Mail" accounts are those where the account holder has instructed the financial institution not to issue any correspondence to the account holder's address.

452. Regardless of the source of "Hold Mail" business, evidence of identity of the account holder should be obtained by the financial institution in accordance with CDD requirements in these Guidelines.

453. It is recommended that a financial institution have controls in place for when existing accounts change status to "Hold Mail" and that the necessary steps to obtain the identity of the account holder are taken where such evidence is not already on the financial institution's file.

454. Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the account holder's address. There are of course many genuinely innocent circumstances where a "c/o" address is used, but a financial institution should monitor such accounts more closely as these accounts may represent additional risk.

455. "Hold Mail" accounts should be annually monitored and reviewed. A financial institution should establish procedures to conduct annual checks of the current permanent address of "Hold Mail" customers.

SECTION VII - UNUSUAL & SUSPICIOUS TRANSACTIONS

456. Suspicious transactions are financial transactions that give rise to reasonable grounds to suspect that they are related to the commission of a ML or TF offence. These transactions may be unusual or large or may represent an unusual pattern that has no apparent or visible economic or lawful purpose. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or a very high account turnover that is inconsistent with the expected pattern of transactions. In some instances, the origin of the transaction may give rise to suspicion. For examples of "Red Flags" see **Appendix 8**.

457. A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and determination of consistent transaction limits. Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis.

458. A financial institution should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations.

459. If transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be available to assist law enforcement agencies and the FIU for at least five years.

460. A financial institution should refer to established websites for entities such as FATF, FinCEN, OFAC, UN Security Council and other recommended websites, as highlighted in **Appendix 2**. These websites provide country advisories, information on countries vulnerable to corruption, countries under increased monitoring, high-risk jurisdictions subject to a call for action, specially designated nationals, and persons.

461. This information should be regarded in conjunction with the Orders issued by the FIU and notices issues by the Group of Supervisors.

462. Where a country continues not to apply or insufficiently applies the FATF Recommendations, appropriate counter-measures to protect the international financial system from ML/TF should be applied including but not limited to:

i. Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from countries with strategic deficiencies;

ii. Enhance relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

iii. In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT/CPF systems;

iv. Warning non-financial sector that financial transactions with natural or legal persons within the identified country might run the risk of ML/TF;

v. Limiting business relationships or financial transactions with the identified country or persons in that country; and

vi. Determine to cut off financial transactions with individuals, entities, or countries that are prohibited under domestic or international laws.

463. A financial institution should develop and establish clear policies, procedures, and processes to detect unusual or suspicious activity in all types of business transactions, products and services offered (for example wire transfers, credit/debit cards and ATM transactions, lending, trust services and private banking).

i. Effective manual and/or automated systems should be developed to enable staff to monitor transactions undertaken throughout the course of the business relationship on a single, consolidated and group-wide basis, and to identify activity that is inconsistent with the financial institution's knowledge of the customer, their business and risk profile; and

ii. Customer-specific limits should be determined based on an analysis of the risk profile of customers, the volume of transactions and the account turnover. This may result in consolidated limits that are multiple limits or aggregate limits.

464. A financial institution should not grant blanket reporting exemptions and should:

i. Clearly document their policy for the granting of such exemptions including the requirements for exemption, officers responsible for preparing and authorizing exemptions, the rationale for establishing threshold limits, the review of exempt customers and procedures for processing transactions.

ii. Maintain authorized exempt lists showing threshold limits established for each qualifying customer; and

iii. Document all investigations and conclusions, including the decision taken when not to file an STR, along with the signature of appropriate staff with such authority.

iv. Monitor currency exchanges and international wire transfers.

465. For the purposes of these Guidelines, a transaction includes an attempted or aborted transaction.

7.1 Internal Reporting Procedures

466. To facilitate the timely detection and reporting of suspicious transactions, a financial institution should:

i. Require customers to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount (i.e., wire transfers) as the financial institution determines, to ascertain the legitimacy of the funds. Appendix 11 indicates a specimen of a Declaration of Source of Funds (DSOF) form. Where electronic reports are employed instead of the form, they should capture the information included on the Appendix and should be signed by the customer; Identify a suitably qualified and experienced person to whom unusual and suspicious reports are channeled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the FIU (**See Sections on External Reporting and Compliance and Audit**);

ii. Require its staff to document in writing their suspicion about a transaction; and

iii. Require documentation to support internal inquiries. The documentation submitted must be adequate to establish a connection between the person(s) and the suspicious activity or transaction.

467. Financial institutions must put in place appropriate policies and procedures to ensure suspicious activity is identified, enquired into, documented, and reported.

468. Financial institutions' policies and procedures should provide guidance to staff on the legal reporting requirements when identifying and reporting unusual activities internally. This includes attempted transactions, regardless of the amount, as well as the degree and extent of investigations that is appropriate prior to reporting an STR to the FIU.

469. The financial institutions' policies and procedures for suspicious transaction reporting must ensure that:

i. The financial institution's employees are trained to identify and report suspicious activity related to criminal property and ML/TF;

ii. The financial institution's employees provide a UTR to the compliance officer where there is knowledge, suspicion or reasonable grounds for suspicion that funds or assets acquired are derived from criminal activity or that a person is involved in ML/TF;

iii. The financial institution develops and implements an internal form to be used to document and report unusual transactions.

iv. The financial institution's reporting officer considers all UTRs in light of all relevant and available information and requires appropriate inquiries to be made; and

v. The financial institution's employees understand that it is a criminal offence to disclose to any person other than the reporting officer or the FIU any knowledge, suspicion, or reasonable grounds for suspicion that a disclosure has been filed with the FIU or any other information or other matter likely to prejudice any investigation, which might be conducted following such a disclosure.

470. Unusual transaction must be promptly reported to the compliance officer.

471. Financial institutions must establish internal reporting procedures that, among other things, ensure that all employees know when, how and to whom they must report.

472. All internal reports of knowledge, suspicion, or reasonable grounds for suspicion must reach the compliance officer.

473. Line managers may be permitted to add comments to an internal report indicating evidence that may assist the compliance officer in determining whether the suspicion is justified or whether there are reasonable grounds for suspicion, but no line manager or any other person may prevent an internal report from reaching the compliance officer.

474. Whether or not an employee consults a colleague, the legal obligation remains with the employee to decide independently whether a report should be made; they must not allow any colleague to decide for them.

475. Reporting lines should be short with a minimum number of people between the person with reason to report and the compliance officer. Such an approach ensures speed, confidentiality and integrity in the reporting process and swift access to the compliance officer.

476. Each internal report along with supporting documentation submitted to the compliance officer should be documented or recorded electronically and retained in accordance with the Record-Keeping requirements in this Guideline.

477. Each internal report should include full details of the customer, transaction, act or conduct in question and as full a statement as possible of the information or conduct giving rise to the knowledge, suspicion, or reasonable grounds for suspicion.

478. Once an employee has reported their suspicion in an appropriate manner to the reporting officer or to a natural person to whom the reporting officer has delegated the responsibility to receive such internal reports, the reporting employee has fully satisfied their statutory obligation.

479. Where a transaction is inconsistent in amount, origin, destination or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and inquiries should be made to ascertain whether the business relationship is being used for ML/TF purposes. A financial institution should record the findings of their inquiries in writing.

480. Where a financial institution conducts inquiries and obtains a satisfactory explanation for the unusual transaction or pattern of transactions, it may be concluded that there are no grounds for suspicion, thus further actions may not be necessary, except for the documentation of the reasons for such determination.

481. Where a financial institution conducts inquiries and a satisfactory explanation of the transaction is not provided by the customer, it may be concluded that grounds for suspicion exists, which require the refusal of the transaction and the filing of an STR with the FIU.

482. A financial institution should ensure that all contact between its institution and the FIU and/or law enforcement agencies is reported to the Compliance Officer or MLRO so that an informed overview of the situation can be maintained.

7.2 Evaluation and Determination by the Compliance Officer

483. The compliance officer must have the ultimate authority to evaluate unusual transactions and determine whether an STR is appropriate under the MLTPA.

484. A financial institution's compliance officer must consider each report in light of all available information and determine whether it gives rise to knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

485. The compliance officer must diligently consider all relevant material to ensure that no vital information is overlooked when determining whether to make an external report to the FIU.

486. The financial institution must permit the compliance officer to have access to its personnel and any relevant information, including CDD information, in the financial institution's possession. The reporting officer must also have the ability to require additional relevant information to be obtained from the customer if necessary or from any relied upon party or any party carrying out

AML/CFT/CPF measures under an outsourcing arrangement.

487. Any approach to the customer or to a relied upon party or introducing intermediary should be made with due regard to the risk of violating the tipping-off rules.

488. Given the need for timely reporting, the reporting officer should consider when it is appropriate to make an initial report to the FIU prior to completing a full review of the business relationship and any linked or connected relationships. Any initial report must be followed promptly by a comprehensive STR.

489. If the reporting officer determines that a report to the FIU is not appropriate, the reasons for the determination should be clearly documented and retained in accordance with the guidance provided on Record-Keeping.

7.3 External Reporting

490. The national reception point for disclosure of STRs is the FIU. Reports should be in the format determined by the FIU (**See Appendix 12**). However, where a matter is considered urgent, an initial report may be made by contacting the FIU by telephone or e-mail to be followed-up by the requisite STR form by the following working day.

491. A financial institution is required by law to report, within three days to the FIU, where the identity of the person involved, the transaction, proposed transaction or attempted transaction or any other circumstance concerning that transaction lead the financial institution to have reasonable grounds to suspect that a transaction:

i. Involves proceeds of crime to which the MLTPA applies;

ii. Involves or is linked or related to or to be used for terrorism, terrorist acts or by terrorist organizations or for the financing of terrorism; or

iii. Is of a suspicious or an unusual nature.

492. This requirement to report suspicious transactions should apply regardless of whether such transactions are thought to involve tax matters, given the requirements under Section 17(4) of the MLTPA to report **any** transaction, proposed transaction or attempted transaction suspected to relate to the commission of a ML/TF offence, terrorist act or suspected to be the proceeds of crime.

493. Where a suspicious report has been filed with the FIU, and further unusual or suspicious activity pertaining to the same customer or account arises, a financial institution should file additional reports with the FIU.

494. A licensed/registered financial institution, its directors, officers, employees, owners, or other representatives as authorized by law are protected under the MLTPA from any action, suit, or proceedings for breach of any restriction on disclosure of information, if a suspicious activity is reported in good faith to the FIU, even if the precise underlying criminal activity is not known, and regardless of whether illegal activity actually occurred. It is against the law for employees, directors, officers, or agents of a financial institution to disclose that an STR or related information on a specific transaction has been, is being or will be reported to the FIU.

495. Where a person is a client of both the financial institution and another group member, and a suspicious report is prepared by the latter, the Belize FIU should be notified.

496. The FIU will continue to provide information, on request, to a disclosing institution in order to establish the current status of a specific investigation.

SECTION VIII –– TARGETED FINANCIAL SANCTIONS

497. The obligations of financial institutions with respect to targeted financial sanctions are set forth primarily in sections 12 and 68 of the Money Laundering & Terrorism (Prevention) Act (MLTPA). Notices of the Director of the Financial Intelligence Unit (FIU) under section12 of the MLTPA or Orders of the High Court under section 68 of the MLTPA have the effect of ordering the freezing the funds or assets of Listed Persons and prohibiting providing them with financial or other related services.

498. Financial institutions should make their sanctions compliance programme an integral part of their anti-money laundering/combating the financing of terrorism/combating proliferation financing (AML/CFT/CPF) compliance programme, subject to several key differences described in this Guidance Notes.

499. The guidance provided in this Guidance Notes is not exhaustive. Although this guidance focuses on financial sanctions and asset freezes, financial institutions must also be aware of the nature and requirements of other types of sanctions measures. It is the responsibility of each entity to put in place policies, procedures and controls that ensure compliance with the sanctions regime.

500. Financial sanctions are enforcement measures the international community uses to achieve, maintain, or restore international peace and security in a specified regime. Financial sanctions are imposed on an entity, regime, or natural person within a regime by the United Nations (UN), European Union (EU), or United Kingdom (UK) as a tool to comply with certain foreign policy or national security objectives. The effect of sanctions is to:

i. Limit the provision of certain financial services; and

ii. Restrict access to financial markets, funds, goods, services and economic resources.

501. Financial sanctions are largely imposed to:

i. Coerce a regime or natural persons into changing their behaviour, or aspects of it, by increasing the cost on them to such an extent that they decide to cease the offending behaviour;

ii. Constrain a target by denying it access to key resources needed to continue its offending behaviour, including the financing of terrorism or nuclear proliferation;

iii. Signal disapproval, resulting in stigmatizing and potentially isolating the target, or as a way of sending broader political messages domestically or internationally; and

iv. Protect the value of assets that have been misappropriated from a country until such assets can be repatriated.

502. Measures that are frequently applied through international sanctions include:

i. Financial sanctions, including asset freezes, bans on investment or access to capital markets, limitations on banking activities or relationships and restrictions on the provision of other financial services or advice;

ii. Trade controls on the importation, exportation, or financing of specified goods, services, equipment, and activities; and

iii. Directions to cease all business with a specific person, group, sector, or country. The primary sources of international sanctions affecting Belize's financial institutions are the UN and EU.

8.1 The Belize Sanctions Regime

503. Most of Belize's international sanctions are brought into force through the MLTPA.

504. The scope of restrictions varies, and financial institutions must review the relevant provisions of the MLTPA together with each Notice issued by the FIU in accordance with section 12 of the MLTPA and each Order issued by the High Court in accordance with section 68, together with any accompanying lists, annexes, schedules, updates, or amendments, to ensure compliance with the specific requirements including:

i. Asset freezing;

ii. Prohibitions against provision of financial and other related services; and

iii. Reporting.

505. An asset freeze generally prohibits dealings with frozen funds or economic resources belonging to or owned, held, or controlled by a sanctions target. An asset freeze may also prohibit making funds, economic resources and, in some cases, financial services available, directly, or indirectly, to or for the benefit of a sanctions target. Asset freezing can, therefore, affect any transaction or business relationship in which a customer, counterparty, beneficial owner, trustee, or other party is a sanctions target or is acting on behalf of or for the benefit of a sanctions target.

506. Indirect payments are those made to someone acting on behalf of a sanctions target. A payment that is for the benefit of a sanctions target is a payment that is made to a third party to satisfy an obligation of a sanctions target.

507. When a legal or natural person is named as a sanctions target, their name is recorded on The Belize Consolidated Sanctions List (Consolidated List). In that case, an asset freeze and restrictions on the provision of financial or other related services will also apply to entities that are wholly or jointly owned or controlled, directly or indirectly, by a sanctions target. Although entities owned or controlled by a sanctions target may not be included on the consolidated list, such entities are nonetheless subject to financial sanctions.

508. To assess whether a legal person or entity is owned by another person or entity, financial institutions should determine whether the sanctions target owns more than 50% of the proprietary rights of an entity or has a majority interest in it. If this criterion is met, then financial sanctions apply both to the

sanctions target and to the majority-owned entity.

509. 'Owned' is interpreted to include direct and indirect ownership. If it is determined that a sanctions target is the ultimate beneficial owner of an entity, for example, where the sanctions target owns a corporate body that, in turn, owns another corporate body, then all entities that are part of the ownership chain are subject to financial sanctions.

510. To assess whether a legal person or entity is controlled by another person or entity, financial institutions should consider whether, with regard to the legal person or entity, a sanctions target:

511. Has the right or exercises power to appoint or remove a majority of the members of the administrative, management or supervisory body of such a legal person or entity;

i. Has appointed, solely as a result of the exercise of the sanctions target's voting rights, a majority of the members of the administrative, management or supervisory bodies of a legal person or entity who have held office during the present and previous financial year;

ii. Controls alone, pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity;

iii. Has the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered into with that legal person or entity or to a provision in its memorandum or articles of association, where the law governing that legal person or entity permits it being subject to such an agreement or provision; or

iv. Has the right to exercise a dominant influence referred to in the point above without being the holder of that right, including by means of a front company.

512. As required by sections 68 (5R), and (5S) of the MLTPA, sanctions in effect in Belize require financial institutions to inform the FIU of any instance in which:

i. The financial institution knows, suspects, or has reasonable cause to suspect that a customer or any person with whom the financial institutions have or has had dealings is a sanctions target; or

ii. The financial institution or sanctions target has breached a sanction.

513. Any report described in paragraph above must be made to the FIU, and a copy should be provided to the Central Bank.

8.2 Compliance with the Belize Sanctions Regime

514. Each financial institution must have adequate policies, procedures, and controls to comply with the Belize sanctions regime.

515. A financial institution's policies, procedures and controls should be documented and approved by its board of directors or senior management.

516. Each financial institution's policies, procedures and controls must enable it to conduct screening including ongoing screening of its customers and transactions to determine whether it is conducting or may conduct business involving any sanctioned person, entity, or activity.

517. The financial institution's sanctions checking processes should be proportionate to the nature and size of its business and should be likely to identify all target matches with sanctions targets.

518. A financial institution's process of determining which sanctions compliance measures is proportionate and likely to identify all target matches differs in a key manner from the risk-based approach for AML/CFT/CPF compliance.

519. Whereas a financial institution may choose to have a higher risk tolerance with regard to AML/CFT/CPF compliance and, therefore, may choose to transact with higher-risk customers, a financial institution may not choose to transact in violation of the Belize sanctions regime. There is, therefore, no room for risk tolerance in sanctions compliance. Any financial institution that provides any funds or financial services to sanctions target or fails to freeze the assets of a sanctions target, is in breach of the sanctions regime and liable to be prosecuted.

520. Although sanctions compliance is a rules-based approach, a financial institution's assessment of its risk of exposure to sanctioned persons, entities and activities is expected to assist in preventing the financial institution from breaching the sanctions regime. Each financial institution should conduct such a risk assessment, conducting it in line with what is prescribed for the AML/CFT/CPF assessment and keeping it up-to-date with reference to the following non-exhaustive list of risk factors:

i. Customers, products and activities;

ii. Distribution channels;

iii. Complexity and volume of transactions;

iv. Processing and systems;

v. Operating environment;

vi. Screening processes of intermediaries;

vii. Geographic risk; and

viii. Any other relevant sanctions regulations.

521. To tailor its sanctions compliance measures to the nature and size of its business, a financial institution should take the following steps:

i. Understand and identify the applicable sanctions;

ii. Develop and document appropriate policies, procedures and controls in order to comply with the sanctions;

iii. Apply the sanctions compliance policies, procedures and controls that have been developed and documented;

iv. Maintain up-to-date sanctions information; and

v. Regularly review, test, and improve the sanctions compliance policies, procedures and controls

put in place.

522. Each financial institution should ensure that its sanctions-related policies, procedures, and controls effectively guide the institution in:

i. Ensuring up-to-date knowledge of the applicable sanctions;

ii. Tailoring sanctions compliance measures to the financial institution's business;

iii. Screening the financial institution's customers, transactions, third-party service providers and geographic connections for potential matches with sanctions targets;

iv. Reviewing potential matches to identify target matches;

v. Freezing assets or taking any other required action in the event of a target match;

vi. Reporting target matches and any breaches;

vii. Ensuring appropriate staff awareness and training; and

viii. Documenting and recording actions taken to comply with the sanctions regime and the rationale for each such action.

523. Reviewing the effectiveness of the financial institution's policies, procedures, and controls. Each financial institution must ensure that it knows its business and does not breach the sanctions regime. Financial Institutions should ensure that effective policies, procedures, and controls are implemented to prohibit and detect attempts by employees or customers to:

i. Omit, delete, or alter information in payment messages for the purpose of avoiding detection of that information by other payment service providers in the payment chain; or

ii. Structure transactions for the purpose of concealing the involvement of a sanctions target.

8.3 Other Unilateral Sanctions Regimes

524. Where a financial institution has a presence or is otherwise active in a jurisdiction outside of Belize, it may be required to comply with the sanctions requirements of that other jurisdiction. Transacting with a customer or counterparty in another jurisdiction may also trigger the sanctions requirements of that jurisdiction, even if a financial institution has no presence there.

525. Financial institutions should obtain legal advice to understand which sanctions regimes apply to which aspects of their business and to ensure that they correctly comply with applicable sanctions while not incorrectly applying sanctions regimes of other jurisdictions to Belize business.

526. Where a financial institution operates in a number of jurisdictions, a consistent group policy should be established to assist local business units in ensuring that their local procedures meet minimum group standards while also complying with local requirements.

8.4 Training

527. Each financial institution should implement a sanctions-related employee training and awareness programme that is appropriate for the financial institution's business as well as the level of the employee.

528. The form, structure, and scope of a financial institution's training and awareness programme should be in line with these guidelines, bearing in mind the differences between complying with AML/CFT/CPF obligations and sanctions obligations.

529. The substance of the training and awareness programme should, at a minimum, include the financial institution's policies, procedures, and controls for:

i. Complying with new sanctions that come into force;

ii. Ceasing compliance with sanctions that have been retired from effect;

iii. Screening for applicable sanctions targets;

iv. Reporting target matches and any breaches;

v. Documenting actions taken to comply with the sanctions regime and the rationale for each such action; and

vi. Communicating changes to the financial institution's sanctions obligations, including changes to its sanctions-related policies, procedures, and controls.

8.5 Documentation and Record-keeping

530. Financial institutions should ensure that appropriate record is made of the following:

i. The financial institution's sanctions-related policies, procedures and controls;

ii. Actions taken to comply with the sanctions regime;

iii. Information sought and obtained to confirm or eliminate a potential match;

iv. The persons who decide whether a potential match is a target match;

v. The rationale for the decision; and

vi. The information used for preparing and contained in any report to the FIU.

531. Financial institutions, at a minimum, should retain record of the following information about any potential match, whether it turned out to be a true match or a false positive:

i. The information or other grounds that triggered the match (e.g., a 'hit' provided by screening software);

ii. Any further checks or inquiries undertaken;

iii. The relevant sanctions regime;

iv. The person(s) involved, including any members of compliance or senior management who authorized treatment of the match as a false positive;

v. The nature of the relationship with the person or entity involved, including attempted or refused transactions;

vi. Subsequent action taken (e.g., freezing accounts); and

vii. Whether the financial institution consulted with or filed a report with the FIU.

532. All related records should be retained in accordance with the record-keeping requirements in this Guideline.

8.6 Reviewing Effectiveness

533. Each financial institution should monitor its policies, procedures, and controls to ensure full, up-to-date, and timely compliance with rapidly changing sanctions obligations.

534. A financial institution should make the review of its sanctions-related policies, procedures, and controls part of its AML/CFT/CPF independent audit.

535. Senior management is responsible for the effectiveness of a financial institution's sanctions-related policies, procedures, and controls. The compliance officer may be the appropriate person to grant authority to:

i. Oversee the establishment, maintenance and effectiveness of the sanctions-related policies, procedures and controls;

ii. Monitor compliance with the relevant acts, regulations, and guidance; and

iii. Access all necessary records in a timely manner in order to respond to any information gathering authorized by an order.

8.7 Screening Customers and Transactions

536. Financial institutions should screen their business and transactions for any person, entity, activity or good that is a sanctions target. Screening should be conducted against appropriate lists, such as UN sanctions and Belize's consolidated list of all orders.

537. Screening should be conducted every three months and within hours of a new Order being issued. Screening should be conducted for new accounts and ongoing transactions.

538. Financial institutions should screen not only their customers but, wherever possible, any other related parties, including, but not limited to, the following:

i. Counterparties; trustees and similar persons;

ii. Beneficial owners, directors, signatories and similar persons of customers, counterparties and

third-party service providers;

iii. Persons authorized by power of attorney; and

iv. The geographic connections of the abovementioned persons and entities.

539. At a minimum, each financial institution should screen every related party for which verification of identity is sought under the financial institution's risk-based policies, procedures, and controls.

8.8 Non-Standard CDD Measures

540. Where a financial institution chooses not to screen any customer or related party, it should be aware that it is increasing its likelihood of committing a sanctions offence.

541. Financial institutions should screen the payment information associated with transfers of funds to identify any potential sanctions targets. Financial institutions should screen information contained within the payment messages, cover messages or batch files of any messaging system, as well as any information associated with the transfer of funds that is conveyed by any other means.

8.9 Timing and Scope of Screening

542. Initial screening of customers and related parties should take place during the establishment of a business relationship or as soon as possible thereafter.

543. Where a financial institution conducts screening after the establishment of a business relationship, it should be aware that it risks transacting with sanctions target in breach of the sanctions.

544. The screening of payment information should take place on a real-time basis. A financial institution may accept an incoming payment prior to screening for a sanctions target, but it must not forward any payment, disburse any funds, or otherwise make funds or assets available to any party prior to screening.

545. Financial institutions should consider conducting post-event screening only for incoming transactions, provided that the financial institution maintains control over the funds or assets and no funds or assets are made available to any other parties prior to the completion of screening.

8.10 Screening software

546. Financial institutions may choose to use commercially available screening software; other financial institutions may rely on manual screening.

547. Where a financial institution chooses to use screening software, the financial institution should ensure that the software will flag potential matches with sanctions targets in a clear and prominent manner.

548. Financial institutions should understand the capabilities and limits of any software and ensure that the software is appropriate given the nature and size of the business and the volume and types of data the business uses, including data held in any legacy systems.

549. Where automated software screening is used, financial institutions should monitor and test the ongoing effectiveness of the software and ensure that adequate contingency arrangements are in place

in the event that the software fails.

550. Financial institutions should, wherever possible, use a screening system with 'fuzzy matching5' capabilities. These capabilities are often tolerant of multinational and linguistic differences in spelling, transliteration, formats for dates of birth and similar data. 'Fuzzy matching' systems may also screen for the reversal of names, the removal of numbers or the replacement of numbers with words, which are techniques that have been used in an attempt to evade sanctions.

551. A sophisticated 'fuzzy matching' system will have a variety of settings, allowing financial institutions to set greater or lesser levels of 'fuzziness' in the matching process. In determining an appropriate level of 'fuzziness', a financial institution should ensure that all potential matches are flagged.

8.11 Reliance and Outsourcing

552. In determining its screening policies, procedures and controls, a financial institution should not assume that the introduced business has been screened for sanctions compliance or that any screenings conducted were adequate or maintained up to date.

553. Financial institutions may choose to outsource to a third-party service provider some or all of its sanctions screening or other sanctions-related processes, bearing in mind that a financial institution cannot contract out of its statutory and regulatory obligations under the Belize sanctions regime. Financial institution should ensure that the responsibilities in any outsourcing relationship are clearly set forth in a service level agreement. Financial institutions should satisfy themselves that the service provider is providing an effective service.

554. Financial institutions must not rely upon or enter into any outsourcing arrangement with a third party where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

8.12 Reporting Matches and Breaches

555. Financial institutions should investigate potential matches with sanctions targets to determine whether there are any target matches.

556. A target match arises where a financial institution knows, suspects, or has reasonable grounds to suspect that it is conducting or may conduct business involving a sanctions target.

557. A financial institution may need to seek sufficient information from relevant parties to enable it to determine whether it has knowledge, suspicion, or reasonable grounds for suspicion of a target match. A financial institution should ensure that there is a clear rationale for any decision that a potential match is not a target match.

558. Financial institutions should maintain a record of the information sought and obtained, the person or persons involved in the review of the potential match, and the rationale for the decision made.

559. Financial institutions must ensure that they have clear internal and external reporting processes for reporting target matches to the FIU and the Central Bank of Belize (Central Bank).

560. Where a financial institution identifies a target match, it should verify whether the sanctions target is listed in a Notice or an order that has been given effect in Belize.

561. Where a financial institution identifies a target match for sanctions that are in effect in Belize, the financial institution must:

i. Immediately comply with the terms of the order by immediately freezing any funds or economic resources, where required, or taking any other required action; and

ii. Not enter into financial transactions or provide financial assistance or services in relation to the sanctions target, and not engage in any other activity sanctioned under the directive unless there is an exemption in legislation on which the financial institution can rely;

iii. Immediately report the target match to the FIU in a manner specified by the FIU.

iv. When informing the FIU of a target match or that a financial institution or a sanctions target has breached a sanction, the financial institution should copy the Central Bank and include the following:

v. The information or other matter on which the knowledge, suspicion or reasonable grounds for suspicion or breach is based;

vi. Any information held by the financial institution about the sanctions target by which the target can be identified; and

vii. The nature and amount, quantity or value of any funds or economic resources held by the financial institution in relation to the sanctions target.

562. Where a financial institution freezes assets, it should do so immediately upon discovering the target match and should ensure that relevant staff do not process any further transactions without an express direction from senior management. Freezing and/or ceasing the provision of services must take place immediately upon detection and then should be followed by the filing of the relevant form.

8.13 Suspicious Transaction Reports and Tipping-Off

563. Where a financial institution has knowledge, suspicion, or reasonable grounds for suspicion that funds or assets involve criminal property, it must comply with its obligations under the MLTPA.

564. The fact that a target is subject to sanctions is public information, and there is no prohibition on financial institutions informing customers or third parties of a target's sanctioned status. Informing customers or third parties of a target's sanctions status is not a tipping-off offence. Remember however that freezing and/or ceasing the provision of services must take place immediately upon detection and then should be followed by the filing of the relevant form.

565. By contrast, where a financial institution has filed a suspicious transaction report (STR) with the FIU, disclosing the fact that the STR was filed is a tipping-off offence.

8.14 Penalties for Non-compliance

566. Financial institutions must be aware that, in contrast to AML/CFT/CPF measures, which generally permit financial institutions to set their own timetables for verifying and updating customer due diligence (CDD) information, a financial institution risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect. In addition, whereas a financial institution may choose to transact with a higher-risk natural person or entity, it may not transact with any natural person or entity subject to the sanctions regime in breach of such regime.

567. The sanctions regime applies to natural persons as well as legal persons and arrangements. Where any financial institution is guilty of an offence and that offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the financial institution, or any person who was purporting to act in any such capacity, both that person and the financial institution are guilty of that offence and liable to be proceeded against and punished accordingly in accordance with the MLTPA.

SECTION IX - COMPLIANCE AND AUDIT

568. All financial institutions are required to establish a point of contact with the FIU in order to handle the reported suspicions of their staff regarding ML, TF or PF. A financial institution is required to appoint a Compliance Officer to undertake this role. Such officer is required to be registered with the FIU, by way of a letter to the Director stating the qualifications and experience of this officer as per Section 18(3) of the MLTPA.

569. Financial institutions must appoint a compliance officer, who must be at the managerial level, is appropriately qualified and trained, and is required to:

i. Establish a risk-based compliance program and maintain internal policies, procedures, controls and systems approved by senior management as required by the MLTPA are in place; and

ii. Implement and monitor the compliance program to ensure continuous compliance with the act, regulation, and this Guideline.

570. The Compliance Officer must be at managerial level and possess the appropriate level of authority, seniority, and independence.

571. Good governance practices require that the Compliance Officer should be independent of the receipt, transfer, or payment of funds, or the management of customer relationships and assets. In considering the independence of the Compliance Officer, consideration should be given to any potential conflicts of interest that may arise between the compliance function and any other responsibilities discharged by the Compliance Officer. In determining independence, the following should be taken into account:

i. The nature of the reporting lines between the Compliance Officer and management of operating/business units. Ideally, the Compliance Officer should have a direct reporting line to the Board of Directors (or relevant Committee of the Board) of the institution and where necessary to senior management. The Compliance Officer should not have a reporting line to a senior manager with business line responsibilities. For smaller companies where independence may not be practical, consider administrative reporting to a business line manager and functional

reporting to a more senior officer or to the Board. Ultimately, the financial institution must be able to demonstrate the independence of the Compliance Officer in form in instances where practically, independence cannot be achieved functionally.

ii. Potential conflicts of interest between their compliance responsibilities and any other responsibilities that the Compliance Officer may have. In general, the Compliance Officer should not have any other responsibilities than that of compliance. However, depending on the scale and nature of business, a financial institution with less than BZ$20,000,000 in assets may choose to combine the functions of the Compliance Officer with the functions of another officer of the bank, except that of the Internal Auditor. Where feasible financial institutions should make appointments that avoid conflicts of interest. Financial institutions should ensure that remuneration of the Compliance Officer is not related to the performance of any one business line within the organization.

iii. For consistency and to ensure ongoing attention to the compliance regime, the appointed Compliance Officer may delegate certain duties to other employees. However, where such a delegation occurs, the Compliance Officer retains responsibility and accountability for the compliance program. The Compliance Officer must have:

a. Unfettered access to, and direct communications with Senior Management and the Board; and

b. Timely and uninhibited access to customer identification, transaction records and other relevant information throughout the organization.

572. The Compliance Officer should:

i. Undertake the responsibility for developing a compliance program and maintaining internal policies, procedures, controls, and systems appropriate to adopt a risk-based approach;

ii. Develop a program to communicate policies and procedures within the entity;

iii. Monitor compliance by staff with the financial institution's internal AML program and any relevant law relating to AML/CFT/CPF;

iv. Obtain access to all records that are necessary or expedient for the purpose of performing his functions;

v. Receive internal reports and consider all such reports to determine whether the information or other matters contained in the transaction report gives rise to a knowledge or suspicion that a customer is engaged in ML/TF/PF;

vi. Issue, in his/her own discretion, external reports to the FIU, as soon as practicable after determining that a transaction warrants reporting (but within the prescribed three-day period);

vii. Monitor the accounts of persons for whom a suspicious report has been made;

viii. Establish and maintain ongoing awareness and training programs for staff at all levels and establish standards for the frequency and means of training;

ix. Report at least annually to the board of directors (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat ML/TF;

x. Review compliance policies and procedures to reflect changes in legislation or international developments;

xi. Participate in the approval process for high-risk business lines and new products, including those involving new technologies; and

xii. Act as liaison and be available to discuss with the Central Bank or the FIU matters pertaining to the AML/CFT/CPF function.

573. A financial institution may also appoint a MLRO to supervise the Compliance Officer. The MLRO should be a qualified member of the financial institution's senior management.

574. The financial institution's senior management should ensure that the MLRO has sufficient resources, including time, employees, technology, and direct access to and support from senior management. The MLRO must also be adequately trained. In the case of the MLRO's absence, arrangements should be made to ensure proper coverage of duties and awareness among employees of any changes to the procedures to follow when suspicion arises.

575. The MLRO should have direct access to the Central Bank and, where appropriate, law enforcement agencies to ensure that any knowledge, suspicion, or reasonable grounds for suspicion of ML/TF is properly and promptly disclosed. The MLRO must be free to liaise with the FIU on any question of whether to proceed with a transaction.

576. The financial institution's senior management should ensure that the MLRO has immediate access to the relevant business information, including, but not limited to:

i. CDD and ongoing monitoring records; and

ii. Transaction details.

577. Senior management should ensure that all relevant employees of the financial institution are aware of the MLRO's identity and any deputies and that all relevant employees are aware of the procedures to follow when knowledge, suspicion, or reasonable grounds for suspicion of ML/TF arises.

578. Depending on the financial institution's size or the structure of a financial group, the duties of the compliance officer and/or MLRO may be delegated to additional senior, appropriately qualified, and trained natural persons within the financial institution or group. The appointment of one or more permanent deputy MLROs may also be necessary. In these cases, the principal or group MLRO should ensure that roles and responsibilities are clearly defined and that employees know where to direct reports of knowledge, suspicion, or reasonable grounds for suspicion of ML/TF.

579. All financial institutions are required to obtain the approval of the Central Bank to appoint a fit and proper person as a Compliance Officer, MLRO and their deputies.

580. Financial intuitions are required to notify the Central Bank of the name and contact information of the Compliance Officer and MLRO. This notification should include a statement that the Compliance Officer and MLRO are fit and proper persons;

581. Financial institutions should notify the Central Bank of the name and contact information of any MLRO or Compliance Officer deputies. Receipt of such information enhances the Central Bank's ability to communicate effectively with financial institutions.

582. A financial institution is to notify the Central Bank where there are any changes to the designations of the Compliance Officer and/or MLRO or any deputies within seven (7) business days;

583. The compliance officer and MLRO may be the same natural person.

584. Where they are not the same person, the Compliance Officer and the MLRO should maintain open lines of communication and understand each other's roles and responsibilities. The relationship should be clearly defined and documented.

585. The role, standing and competence of the Compliance Officer and the MLRO and the manner in which the financial institution's policies, procedures and controls are designed and implemented impact directly on the effectiveness of a financial institution's AML/CFT/CPF arrangements and the degree to which the financial institution is in compliance with Belize's acts and regulations.

9.1 The Alternate Compliance Officer

586. Financial institutions are required to appoint a fit and proper officer as an interim alternate to the Compliance Officer. The Alternate Compliance Officer should have the same responsibilities as the Compliance Officer, during periods of prolonged absences by the Compliance Officer, such as vacation and sick leave. Consequently, all requirements and responsibilities stipulated for the Compliance Officer apply equally to the Alternate Compliance Officer.

587. Financial institutions are required to register the Alternate Compliance Officer with the FIU, by way of a letter to the Director stating the qualifications of this officer as per Section 18(3) of the MLTPA.

588. The MLRO, Compliance Officer and Alternate Compliance Officer are expected to act honestly and reasonably and to make determinations in good faith.

9.2 Periodic Report

589. At least once a year, the compliance officer should report to the Board of Directors or a committee of the Board on the operation and effectiveness of the financial institution's AML/CFT/CPF policies, procedures, and controls. Senior management should determine the scope and frequency of information it feels is necessary to discharge its responsibilities. A financial institution may determine that the compliance officer needs to report to the Board of Directors more frequently. The periodic report should contain the actions and outcomes of any relevant quality assurance, independent audit, or internal audit reviews of the financial institution's AML/CFT/CPF processes and the outcomes of the financial institution's risk assessments.

590. The periodic report may also include:

i. The means by which the effectiveness of the financial institution's policies, procedures and controls has been managed and tested;

ii. Identification of compliance deficiencies and details of action taken or proposed to address any such deficiencies;

iii. Failure to apply Belize requirements in branches and subsidiaries, any advice received from the Central Bank and details of action taken;

iv. The number of internal disclosures to the MLRO, the number of subsequent external reports submitted to the FIU, any perceived deficiencies in internal or external reporting procedures and the nature of action taken or proposed to address such deficiencies, such as CDD reviews, ongoing monitoring reviews/projects and AML/CFT/CPF training taken by the Compliance Officer and MLRO;

v. Information concerning the training program for the preceding year, which employees have received training, the methods of training and the nature of the training;

vi. Changes made or proposed in respect of new or revised acts, regulations, guidance or best practices;

vii. A summary of risk assessments conducted or updated with regards to customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions;

viii. The nature of actions taken with regards to jurisdictions that do not sufficiently apply the FATF Recommendations, or which are the subject of international countermeasures and the measures taken to manage and monitor business relationships connected with such jurisdictions; and

ix. Any recommendations concerning additional resource requirements to ensure effective compliance with the financial institution's statutory and regulatory obligations.

591. Where a financial institution is part of a group or involved in multiple jurisdictions, a consolidated report may be appropriate.

592. At the time the Board of Directors receives a report on the operation and effectiveness of the financial institution's AML/CFT/CPF policies, procedures, and controls, it should consider the report and take any and all necessary actions in a timely manner to remedy any deficiencies identified.

9.3 Internal Controls

593. In addition to a formal AML/CFT/CPF policy statement, financial institutions must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to prevent operations related to ML/TF to:

i. implement the customer identification requirements;

ii. implement record keeping and retention requirements;

iii. implement the monitoring requirements including the identification and scrutiny of:

a. complex or unusually large transactions;

b. unusual patterns of transactions which have no apparent economic or visible

c. lawful purpose; and

d. any other activity which the reporting entity regards as particularly likely by its nature to be related to ML/TF/PF or the breach or evasion of targeted financial sanctions.

iv. implement the reporting requirements;

v. implement communication measures to make its officers and employees aware of the ML/TF related laws, guidelines, procedures, and policies including CDD, freezing and suspicious transaction reporting.

vi. screen persons before hiring them as employees;

vii. Monitor and manage compliance with, and the internal communication of, such policies and procedures in order to prevent activities related to ML/TF or violation of targeted financial sanctions.

viii. Disseminate warning notices and other information received from a supervisory authority or the FIU;

ix. Ensure that a foreign branch or subsidiary or financial a group member observes the AML/CFT/CPF and targeted financial sanctions implementation system that is consistent with Belize's requirements and the FATF Recommendations;

x. Guard against the use of technological developments in for the purposes of ML/TF/PF or violation of targeted financial sanctions, including through the performance and documentation of a risk assessment of any products or services (prior to launch) and the continual documentation of risk assessment and management of such products and services, in a form available to share with the supervisory authority;

xi. Establish or continue business relationships or entering into transactions involving countries on a list published by the FIU, of jurisdictions which are non-compliant, or do not sufficiently comply with the FATF Recommendations;

xii. Identify, assess, and understand its ML/TF/PF and breach or evasion of targeted financial sanctions risks (depending on the type of customers, business relationships, countries or geographic areas, services, delivery channels and products.

xiii. Mitigate risk through mechanisms which include:

a. consideration of the National Risk Assessment or of the reporting entity's risk assessment results or conclusions;

b. the ability to effectively supply information to the supervisory authority; and

c. the application of enhanced measures where the reporting entity's risk assessment identifies a higher risk; and

d. the monitoring and management of compliance with , and the internal communication of such policies and procedures to prevent activities related to ML/TF, and the break or evasion of targeted financial sanctions.

xiv. Establish systems to respond promptly to inquiries from a supervisory authority (in respect of a reporting entity under the authority's supervision), the FIU or a police officer:

a. whether it maintains, or has maintained during the previous five years, a business relationship with any person; and

b. the nature of that relationship.

594. All such policies, procedures and controls must be risk-sensitive, based on a variety of factors, including:

i. The nature, scale and complexity of the financial institution's business;

ii. The diversity of its operations, including the financial institution's geographical connections;

iii. Its customers;

iv. The business of its customers;

v. Its business relationships;

vi. Its products, services and delivery channels;

vii. Its transactions, including their volume, size, and frequency; and

viii. The degree of risk assessed in each area of its operations.

9.4 Application of Group Policies

595. Where a Belize financial institution has branches, subsidiaries, representative offices, or members of any financial group located in a country or territory other than Belize, it must communicate its AML/CFT/CPF policies and procedures to all such entities.

596. Belize financial institutions must also ensure that all branches, subsidiaries, and representative offices located outside Belize apply AML/CFT/CPF measures at least equivalent to those set out in Belize's acts and regulations.

597. A financial group's policies and procedures must provide for the group-wide sharing of information required for the purposes of CDD, ongoing monitoring, record-keeping, and other ML/TF risk management policies, procedures, and controls.

598. Group-level AML/CFT/CPF functions must be provided with customer, account and transaction information from branches and subsidiaries where required for AML/CFT/CPF purposes, including information on transactions or customers which appear unusual and have resulted in a disclosure relating to knowledge, suspicion, or reasonable grounds for suspicion of ML/TF/PF.

599. Financial institutions should establish and maintain adequate safeguards for the confidentiality and use of the information exchanged.

600. Individual financial institutions and financial groups must have access to customer, account and transaction information from branches and subsidiaries where necessary for the purposes of ongoing monitoring.

601. Where operational activities of a Belize financial institution are undertaken by employees in other jurisdictions, those employees should be subject to the same AML/CFT/CPF policies and procedures applied to Belize employees. Senior management must ensure that all suspicious transactions or activities that give rise to knowledge, suspicion, or reasonable grounds for suspicion of ML/TF/PF and are linked with a Belize financial institution or Belize person are reported to the MLRO in Belize.

602. Where the AML/CFT/CPF standards in the country or territory hosting a branch or subsidiary are more rigorous than those required by Belize's acts and regulations, financial institutions should ensure that those higher standards are implemented.

603. Where the law of a country or territory other than Belize does not permit the application of AML/CFT/CPF measures at least equivalent to those in Belize, it must inform the Central Bank accordingly and must take additional measures to manage the risks of ML/TF/PF effectively.

604. Financial institutions that have informed the Central Bank that the law of a country or territory other than Belize does not permit the application of AML/CFT/CPF measures at least equivalent to those in Belize should follow any advice, recommendations, or directions from the Central Bank as to the action to take.

605. Where a financial institution finds that additional measures are insufficient for the purposes of effectively mitigating the ML/TF risks and particularly where effective AML/CFT/CPF policies, procedures or controls are likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions, financial institutions must inform the Central Bank. The financial institution should follow any advice, recommendations, or directions the Central Bank provides as to the action to take, including any advice, recommendation, or direction that the relationship be terminated.

9.5 Independent Audit

606. Each financial institution must ensure that its AML/CFT/CPF policies, procedures and controls are objectively evaluated by a qualified and independent person.

607. An auditor is qualified if it has the requisite subject matter expertise and proficiency to competently review the financial institution's AML/CFT/CPF policies, procedures, and controls. Such expertise and proficiency may be evidenced by continuing training, and professional education focused on AML/CFT/CPF, including internationally recognized certifications. The Certified Public Accountant designation is an outstanding and well-respected credential, but alone it has no direct correlation with AML/CFT/CPF.

608. An auditor is independent if it maintains independence in mental attitude in all matters relating to the audit. Any person who is involved in establishing or performing any of the financial institution's ongoing AML/CFT/CPF compliance processes should not conduct an audit, determine the scope of an audit, or have the authority to alter the contents of an audit report prior to its delivery to senior management and the financial institution's governing body. A financial institution that seeks to use

an external party to conduct an AML/CFT/CPF independent audit should evaluate the independence of the persons approving and signing the agreement with the external party, as well as the independence of the persons responsible for approving the scope of the audit. A financial institution that seeks to use in-house employees to conduct an AML/CFT/CPF independent audit should evaluate the reporting lines of the audit employees and verify their independence when reporting audit results.

609. The independent audit function must provide for a documented audit of the financial institution's AML/CFT/CPF policies, procedures, and controls, including those policies, procedures and controls relating to compliance with international sanctions. Financial institutions must conduct an audit to monitor, and sample test the implementation, integrity and effectiveness of their AML/CFT/CPF policies, procedures and controls on a regular basis. The audit must be conducted on a frequency consistent with the financial institution's size and risk profile. The audit should be conducted more frequently when the Board of Director and senior management becomes aware of any gap or weakness in the AML/CFT/CPF policies, procedures, or controls or when senior management deems it necessary due to the financial institution's assessment of the risks it faces.

610. Where appropriate, having regard to the risk of ML/TF and the size of the business, the audit may be undertaken by internal audit departments. The audit should be adequately resourced to help ensure AML/CFT/CPF compliance.

611. The audit function should:

i. Assess the reliability, integrity, and completeness of the financial institution's AML/CFT/CPF policies, procedures, and controls, including with respect to:

a. Risk assessment;

b. Risk mitigation and other measures to manage higher risks;

c. CDD;

d. Ongoing monitoring;

e. Detecting and reporting knowledge, suspicion and reasonable grounds for suspicion of ML/TF/PF;

f. International sanctions;

g. Record-keeping and retention; and

h. Reliance and outsourcing relationships;

ii. Evaluate the financial institution's risk assessment processes and the risk ratings the financial institution has assigned with respect to its size, customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions;

iii. test and evaluate how effectively compliance policies, laws, regulations, and these guidelines are being implemented. Such reviews should be carried out on a frequency consistent with the

financial institution's size and risk profile. The review process should identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions. Test compliance with the relevant laws and regulations;

iv. Test the AML/CFT/CPF controls for the financial institution's transactions and activities, with an emphasis on higher risk areas;

v. Assess employees' knowledge of the relevant Belize acts, regulations and guidance, the financial institution's policies, procedures and controls and the role of each relevant employee within the financial institution;

vi. Assess the adequacy, accuracy and completeness of employee training and awareness programs; and

vii. Review the financial institution's past audit reports to assess the efficacy with which the financial institution has implemented previously recommended changes.

612. The audit must be documented or recorded electronically and retained in accordance with these Guidelines.

613. The results of the audit should be reported directly to senior management and the financial institution's governing body for timely action. A smaller financial institution that does not have an established internal audit department may introduce a regular review by the Board of Directors or their external auditors to satisfy management that the requirements under the law and as per these Guidelines are being met.

614. The Central Bank recognizes, however, that the designation of a Compliance Officer or the creation of an internal audit department may create difficulties for some small financial institutions. Where the financial institution is part of a larger regulated financial or mixed conglomerate, the Group Compliance Officer may perform the compliance services, or the Group Internal Auditor may perform the internal audit services. Where this is not possible, a financial institution may, subject to the financial institution's agreement, outsource the operational aspects of the compliance or internal audit function to a person or firm that is not involved in the auditing or accounting functions of the financial institution. Notwithstanding, the responsibility for compliance with the MLTPA and the Guidelines remains that of the financial institution and the requirements of this section will extend to the agent. A financial institution should have a local control function and be in a position to readily respond to the Central Bank and FIU on AML/CFT/CPF issues.

SECTION X - RECORD-KEEPING

615. To demonstrate compliance with the MLTPA and to facilitate investigations undertaken by the FIU, a financial institution should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including those related to customer identification, business transactions, internal and external reporting, and training.

10.1 Transaction Records

616. A financial institution should retain all records of business transactions for a minimum of **five years**

after the completion of the business transaction or termination of the business relationship, whichever is later.

617. However, it may be necessary for a financial institution to retain records, until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where:

i. There has been a report of a suspicious activity; or

ii. There is an ongoing investigation relating to a transaction or client.

618. At a minimum, in order to establish a financial profile and a satisfactory audit trail, records relating to transactions which must be kept should include the following information:

i. The name, address, occupation of the beneficial owner of an account and, where appropriate, principal activity of each person conducting the transaction or on whose behalf the transaction is being conducted;

ii. The volume of funds flowing through an account;

iii. The nature of the transaction;

iv. The date on which the transaction was conducted;

v. Details of the transaction including the amount of the transaction, source and destination of the funds and the currency and form (i.e. cash, cheques, etc.) in which it was denominated;

vi. The form of instruction and authority;

vii. Details of the parties to the transaction; and

viii. Where applicable, the facility through which the transaction was conducted, and any other facilities directly involved in the transaction.

10.2 Verification of Identity Records

619. For the purpose of verifying the identity of any person, a financial institution must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the FIU.

620. The obligation to retain records also applies where a financial institution verifies the identity of any person by confirming the existence of a facility provided by an eligible introducer financial institution. In this instance, the records that are retained must be such as are reasonably necessary to enable the FIU to readily identify, at any time, the other financial institution, the relevant facility and to confirm that the other financial institution has verified the person's identity.

621. Records relating to the verification of the identity of customers must be retained for at least five years from the date the person ceases to be a customer or after the verification was carried out, whichever is the latter.

622. In keeping with best practices, the date when a person ceases to be a customer is the date when:

i. A one-off transaction was carried out or the last in the series of transactions;

ii. A business relationship is severed i.e., the closing of the account(s); or

iii. Proceedings commence to recover debts payable on insolvency.

623. Where formalities to end a business relationship have not been undertaken but five years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction.

624. In the case of a financial institution that is liquidated and finally dissolved, the relevant verification and transaction records must be retained by the liquidator or the financial institution for the balance of the prescribed period remaining at the date of dissolution.

625. A financial institution should ensure that records held by an affiliate outside Belize, at a minimum, comply with the requirements of Belizean law and these Guidelines.

626. Records, including but not limited to credit slips, debit slips and/or cheques, should be retained in a format, whether hard copy, electronic, scanned or microfilm, that is admissible in court and that would facilitate reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity and to enable a financial institution to comply swiftly with information requests from the FIU. This applies whether or not records are stored off the premises of the financial institution.

627. It is recognized that it is unrealistic to expect copies of all material to be retained indefinitely and it is accepted that some prioritization is necessary. The objective is to allow the retrieval of relevant information, to the extent that it is available, without undue delay.

628. When a financial institution merges with or takes over another entity, it should ensure that the records described above can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a financial institution, the financial institution is responsible for retrieving those records before the end of the contractual arrangement. The nature of records that should be retained is set out below:

10.3 Customer Due Diligence

629. Financial institutions must retain all records obtained in the course of conducting CDD. Such records include those obtained during the application of both initial and ongoing CDD measures.

630. Records relating to verification of identity should comprise a copy of any official identity document(s), or if such a copy is not readily available, the information contained in the official identity document and information reasonably sufficient to obtain a copy of the document.

631. Where CDD is applied using online or other electronic databases, financial institutions, must retain are cord of the means by which each verification was completed and, where applicable, the data supporting each verification.

632. Financial institutions should maintain records concerning:

i. Data obtained through the application of CDD and ongoing monitoring measures;

ii. Copies or records of official identification documents;

iii. Customer verification documents;

iv. Customer-related data obtained from any reliable and independent source;

v. Information obtained during a customer visit to a financial institution's agent or premises;

vi. Information obtained for the purposes of enhanced CDD or ongoing monitoring;

vii. Verification information as to beneficial ownership;

viii. Information concerning the nature of the business and the purpose and intended nature of the business relationship;

ix. Account files, account statements and business correspondence; and All business transaction records.

10.4 Internal and External Records

633. A financial institution should maintain records related to unusual and STRs. These should include:

i. All reports made by staff to the Compliance Officer;

ii. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;

iii. Consideration of those reports and of any action taken; and

iv. Reports by the Compliance Officer to senior management and the board of directors.

10.5 Training Records

634. In order to provide evidence of compliance with Section 4(1) (b) and (c) of the MLPA Regulations, at a minimum, a financial institution should maintain the following information:

i. Details and contents of the training program provided to staff members;

ii. Names of staff receiving the training;

iii. Dates that training sessions were held;

iv. Test results carried out to measure staff understanding of ML/TF requirements; and

v. An ongoing training plan.

10.6 Retrieval of Records

635. Regardless of whether a transaction was undertaken by paper or electronic means, the record retention requirements are the same.

636. Records, including copies of original documents, may be kept in hard copy or electronic format, provided that financial institutions can retrieve them without delay.

637. Where records, whether in physical or electronic form, are held outside of Belize or by any third party, it is the responsibility of the Belize financial institution to ensure via due diligence, contracting and periodic testing that the records are retrievable without delay and do in fact meet Belize legal requirements.

638. Financial institutions should ensure that appropriate policies, procedures, and controls are in place to protect the integrity and confidentiality of the records it maintains. Where data is stored in either primary or backup form, financial institutions should ensure that policies, procedures, and controls are in place to detect promptly any data breach.

SECTION XI – EDUCATION AND TRAINING

639. An integral element of the fight against ML/TF/PF is the awareness of those charged with the responsibility of identifying and analyzing potential illicit transactions. A financial institution should, therefore, establish ongoing employee training programs.

640. The effectiveness of the procedures and recommendations contained in these Guidelines depends on the extent to which staff of financial institutions appreciate the serious nature of the background against which these Guidelines have been issued. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to cooperate fully and to provide a prompt report of any unusual or suspicious transactions without fear of reprisal.

641. Training should be targeted at all employees but added emphasis should be placed on the training of the Compliance Officer and the compliance and audit staff because of their critical role in sensitizing the broader staff complement of AML/CFT/CPF issues and ensuring compliance with policies and procedures.

11.1 Legal Obligations of Employees

642. Several offences under the MLTPA directly affect the employees of a financial institution:

i. The various offences of ML/TF/PF

ii. Failure to report knowledge, suspicion, or reasonable grounds for suspicion of ML/TF and

iii. Tipping-off and disclosure of information

643. These offences apply to all employees. They are not directed only to those who work directly with customers but apply equally to ‘back office’ and all other employees.

644. Senior management should ensure that employees receive regular and ongoing training on the legal requirements relating to ML/TF/PF.

11.2 Employee Knowledge of Higher Risks and Suspicious Activity

645. Financial institutions should ensure that relevant employees understand the financial institution's approach to risk assessment and risk mitigation. Training should be tailored to the AML/CFT/CPF policies, procedures and controls that relate to employees' specific job functions.

646. Financial institutions should ensure that relevant employees receive training on how to identify and deal with customers who present a higher risk of ML/TF/PF. Training should address the financial institution's risk tolerance for such customers and the specific risk mitigation measures the financial institution has developed, documented and implemented.

647. Financial institutions should also ensure that relevant employees receive training on the vulnerabilities the financial institution faces due to its products, services, delivery channels, transactions, and business relationships. Employees should understand and know how to apply the risk mitigation measures the financial institution has developed and documented with regard to specific combinations of customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions.

648. Employees should understand how ML/TF/PF operate and how these crimes might take place in connection with the financial institution. Financial institutions should consider providing employees with case studies and examples of ML/TF/PF related to the financial institution's business.

649. Employees should be aware of the financial institution's approach to assigning risk ratings to customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products, and transactions.

650. Employees should also understand any norms that the financial institution may establish for transactions and customer conduct and procedures for identifying and scrutinizing persons or activities that fall outside of those norms.

651. Financial institutions must train relevant employees to recognize unusual or suspicious transactions or conduct, and how to properly report knowledge, suspicion, and reasonable grounds for suspicion of ML/TF/PF.

652. Employees must understand the circumstances giving rise to unusual transactions or conduct and which may give rise to knowledge, suspicion, or reasonable grounds for suspicion of ML/TF, depend on the specific combination of customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products, and transactions in question.

11.3 Content and Scope of the Training Programme

653. A financial institution's overall training program should cover topics pertinent to its operations. It should provide relevant employees with training on how to recognize and handle transactions being carried out by persons who may be engaged in ML/TF/PF. Training should be general as well as

specific to the area in which the trainees operate. As staff members move between jobs, their training needs for AML/CFT/CPF may change. The timing of training programs should also be based on need and should be conducted accordingly, but not less than once per annum.

654. Training programs should, inter alia, incorporate references to:

i. Relevant ML, TF, and PF laws and regulations;

ii. Definitions and examples of laundering and terrorist financing schemes;

iii. How the institution can be used by launderers or terrorists;

iv. The vulnerabilities of the financial institution's products, services, delivery channels, transactions and business relationships;

v. The importance of adhering to CDD policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;

vi. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;

vii. The completion of UTR and STRs;

viii. Treatment of incomplete or declined transactions;

ix. The procedures to follow when working with law enforcement or the FIU on an investigation; and

x. The consequences to the financial institutions, its employees personally and its clients due to a breach of the legal requirements relating to ML/TF/PF.

655. A financial institution should therefore:

i. Develop an appropriately tailored training and awareness program consistent with its size, resources and type of operation to enable its employees to be aware of their responsibilities, the risks associated with ML/TF/PF, to understand how the institution might be used for such activities, to recognize and handle suspicious transactions and potential ML/TF/PF transactions and to be aware of new techniques and trends in ML/TF/PF;

ii. Differentiate between the terms "unusual" and "suspicious" transactions.

iii. Clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning CDD and suspicious transaction reporting;

iv. Formally document, as part of its anti-money laundering policy document, its approach to training, including the frequency, delivery channels, and content;

v. Ensure employees are made aware of their personal responsibilities and those of the financial institution at the start of their employment. These responsibilities should be documented in such a way as to enable employees to refer to them as necessary and when appropriate throughout their employment.

vi. Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the MLRO to whom they should report unusual or suspicious transactions;

vii. Obtain an acknowledgement from each staff member on the training received;

viii. Assess the effectiveness of training. Assessment methods include written or automated testing of staff on training received, use of evaluation forms by recipients of training, confirmation of delivery of training according to plan, and review of the contents of training;

ix. Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies to detect and deter ML and to counter TF and PF. Such documentation should include measures relating to identification, record keeping, unusual and suspicious transactions and internal reporting. These should complement rather than replace formal training programs.

x. Make arrangements for refresher training, at least annually, to remind employees of their responsibilities and to make them aware of any new developments in ML, TF, PF methods, trends and , legislation. Towards this end, a regular schedule of new and refresher programmes, appropriate to their risk profile should be established and maintained for the different types of training required for:

a. New hire orientation - General information on the background to ML/TF/PF, and the subsequent need for reporting of any suspicious transactions to the Compliance Officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority, within the first month of employment. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the financial institution for the reporting of suspicious transactions;

b. Operations staff - Members of staff who deal directly with the public (such as cashiers, foreign exchange operators and account opening personnel) are the first point of contact with potential money launderers. Their efforts are therefore vital to the organization's reporting system for such transactions. Tailored training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

All front-line staff should be made aware of the policy for dealing with occasional customers, particularly where large cash transactions, money transfers, negotiable instruments, certificates of deposit or letters of credit and other guarantees are involved, and of the need for extra vigilance in these cases;

Branch staff should be trained to recognize that criminal money may not only be paid in or drawn out across branch counters but may be transferred by other means. Staff should be encouraged to take note of credit and debit transactions from other sources, e.g., credit transfers, wire transfers and ATM transactions.

In addition to the above, account opening personnel should be provided with additional training in respect of the need to verify a customer's identity and on the business' own

account opening and customer verification procedures. They should be familiar with suspicious transaction reporting procedures as well;

c. **Supervisors** - A higher level of instruction covering all aspects of AML/CFT/CPF procedures should be provided to those with responsibility for supervising or managing staff. This is to include the offences and penalties in accordance with the MLTPA including but not limited to non-reporting, production and restraint orders, internal reporting procedures, verification of identity, records retention and disclosure of STRs;

d. **Compliance staff** - In-depth training concerning all aspects of the legislation and internal policies will be required for the Compliance Officer. The Compliance Officer will also require extensive initial and ongoing training on the validation, investigation and reporting of suspicious transactions and feedback arrangements and on new trends and patterns of criminal activity.

SECTION XII - PRE-EMPLOYMENT BACKGROUND SCREENING

656. Financial institution's AML/CFT/CPF policies and procedures must require relevant employees to be screened against high standards.

657. For the purposes of these Guidelines, the term 'employee' includes any person working for a financial institution, including persons working on a temporary or part-time basis, whether under a contract of employment, a contract for services or otherwise. A relevant employee is one who:

i. At any time in the course of their duties, has or may have access to any information that may be relevant in determining whether funds or assets are criminal property, or that a person is involved in ML, TF; or PF.

ii. At any time plays a role in implementing and monitoring compliance with AML/CFT/CPF requirements.

658. Where employees of a third-party carries out work on behalf of a financial institution under an outsourcing agreement, the financial institution should have procedures to satisfy itself as to the effectiveness of the screening procedures of the third party in ensuring employee competence and probity.

659. The ability to implement an effective AML/CFT/CPF program depends in part on the quality and integrity of staff, as an insider can pose the same ML threat as a customer. A financial institution should, therefore, undertake due diligence on prospective staff members with a view to determining whether criminal convictions exist. The senior management of a financial institution should:

i. Verify the applicant's identity;

ii. Develop a risk-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual staff member may warrant additional background screening, which should include verification of references, experience, education, and professional qualifications.

iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of departmental staff time. Internal policies and procedures should be in place (e.g., codes of conduct, ethics, conflicts of interest) for assessing staff; and

iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

660. To ensure that employees are fit and proper for their role, financial institutions should:

i. Request and verify appropriate references for the employee at the time of recruitment;

ii. Verify the employee's employment history, qualifications, and professional memberships;

iii. Request and verify the details of any regulatory action taken against the employee or any action taken by a professional body;

iv. Request and verify the details of any criminal convictions or the absence of any such convictions (e.g., by requesting a police report); and

v. Consult the most up-to-date lists of specified countries and persons against whom sanctions have been imposed by the UN, EU or other relevant body or jurisdiction on the grounds of suspected or known involvement in terrorist or other illegal activity.

661. Financial institutions should document or record electronically any situation where an employee has been hired despite the financial institution's inability to obtain all relevant information. In such cases, financial institutions should include the reasons why all relevant information was not obtained, an appropriate risk-based rationale for the exception and details regarding alternative screening methods undertaken.

SECTION XIII - APPENDICES

Appendix 1

Coverage of Entities

Although the MLTPA applies to a broad spectrum of persons and businesses, additional administrative requirements are placed on financial institutions. The MLTPA defines a financial institution as a bank or financial institution as defined in the Domestic Banks and Financial Institutions Act, or the International Banking Act. Accordingly, for the purposes of these Guidelines, a *financial institution* means:

i. Any person whose regular occupation or business is the carrying on of any of the below activity listed in the Second Schedule of the MLTPA which includes:

- Venture risk capital;
- Money or value transfer services;
- Issuing and administering means of payments (e.g., credit cards, travellers' cheques and bankers' drafts);
- Guarantees and commitments;
- Trading in money market instruments (e.g., cheques, bills, certificates of deposits, commercial paper etc.), foreign exchange, financial and commodity-based derivative instruments (e.g. futures, options, interest rate and foreign exchange instruments etc.), and transferable or negotiable instruments;
- Credit unions;
- Acceptance of deposits or other repayable funds from the public;
- Lending;
- Financial leasing;
- Credit and currency exchange;
- Pawning;
- Participating in securities issues and the provision of financial services related to such issues;
- Advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings;
- Portfolio Management;
- Safekeeping and administration of securities, cash, or liquid securities on behalf

of other persons;

- Investing, administering or managing funds for money on behalf of other persons;
- International (or offshore) banking.

ii. Banking business defined under the DBFIA as:

- Receiving money from the public through the acceptance of deposits which can be withdrawn on demand and used to on-lend;

iii. Financial business defined under the DBFIA as:

- Receiving funds from the public through obtaining loans, advances, extensions of credits, investments, sales of securities of any kind and re-lending or reinvesting of such funds in loans and advances to the public, shares or securities of any kind; or the business of a trust corporation or securities brokerage house;
- Financing house or finance company;
- Leasing corporation;
- Merchant bank or investment bank;
- Mortgage institutions;
- Collective investment;
- Credit card business;
- Financial services;
- Building societies;
- Safe custody services; and
- Other financial businesses;

iv. International banking business defined under the IBA as:

- Receiving, borrowing or taking up foreign money exclusively from non-residents for investing exclusively with non-residents and repayable subject to arrangement;
- Carrying on exclusively with non-residents such other activities as are customarily related or ancillary to international banking;

v. Any other activity defined by the Minister of Finance as such by an Order published in the Gazette amending the First Schedule the MLTPA.

Appendix 2

Useful Websites

IDENTIFICATION PROCEDURES

Information on the status of sanctions can be obtained from websites such as http://www.fco.gov.uk.

Other useful websites include:

http://www.un.org;

http://www.fbi.gov;

http://www.ustreas.gov;

http://www.bankofengland.co.uk;

http://www.osfi.bsif.gc.ca.

NPOS

For a list of all IRS recognized NPOs including charities, go to www.guidestar.org; and for a list of registered charities go to www.charity-commission.gov.uk. For various reasons, these bodies will not hold exhaustive lists.

POLITICALLY EXPOSED PERSONS

For information on the assessment of country risks see the Transparency International Corruption Perceptions Index at www.transparency.org.

For information about recent developments in response to PEPs risk, visit the Wolfsberg Group's website at www.wolfsberg-principles.com. In addition, a financial institution should be aware of recent guidance from the United States of America on enhanced scrutiny for transactions that may involve the proceeds of foreign official corruption. This can be found at www.federalreserve.gov.

HIGH RISK COUNTRIES

A source of relevant information is the FATF website at www.fatf-gafi.org. Other useful websites include: the Financial Crimes Enforcement Network (FinCEN) at www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov/ofac for information pertaining to US foreign policy and national security; and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

Appendix 3

Additional References

Names of Organizations	Website Addresses
Basel Committee on Banking Supervision • Core Principles for Effective Banking Supervision • Core Principles Methodology • Customer Due Diligence for Banks • Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering – December 1998 • Risk Management Principles for Electronic Banking	http://www.bis.org/bcbs/ http://www.bis.org/publ/bcbs30.pdf http://www.bis.org/publ/bcbs61.pdf http://www.bis.org/publ/bcbs85.htm#pgtop http://www.bis.org/publ/bcbsc137.pdf
Caribbean Financial Action Task Force (CFATF)	www.cfatf.org
Commonwealth Secretariat	http://www.thecommonwealth.org
Egmont Group for Financial Intelligence Units	http://www.egmontgroup.org
Federal Deposit Insurance Corporation • Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process	http://www.fdic.gov/
Financial Action Task Force (FATF)	http://www.fatf-gafi.org
Financial Stability Forum	http://www.fsforum.org
International Association of Insurance Supervisors	http://www.iaisweb.org
International Monetary Fund	www.imf.org
International Organisation of Securities Commission	http://www.iosco.org
Interpol (Interpol's involvement in the fight against international terrorism)	http://www.interpol.com/public/terrorism/default.asp
Organisation of American States – CICAD	http://www.cicad.oas.org
The Financial Crime Enforcement Network (FINCEN)	http://www.fincen.gov/af_main.html
The World Bank	http://www.worldbank.org
United Nations	http://www.un.org
United Nations – International Money Laundering Information Network	http://www.imolin.org
United Nations – Security Council Resolutions	http://www.un.org/documents/scres.htm
US Department of the Treasury, Comptroller of the Currency Administrator of National Banks (Money Laundering: A Banker's Guide to Avoiding Problems)	http://www.occ.treas.gov/launder/origc.htm
Wolfsberg Group	http://www.wolfsberg-principles.com/index.html

Appendix 4

Summary of Money Laundering and Terrorism Offences

AREA	DESCRIPTION OF OFFENCE	DESCRIPTION OF PENALTY	SECTION OF LEGISLATION
Money Laundering Offences	Engaging in money laundering directly or indirectly.	Summary conviction in the case of a natural person – fine of $50,000 minimum to $250,000 maximum or 5-10 years imprisonment or both. Summary conviction in the case of a legal person/entity - fine of $100,000 minimum to $500,000 maximum.	Section 4 MLTPA
	Attempting or aiding, abetting, counseling or procuring the commission of, or conspiring to commit money laundering.	Summary conviction in the case of a natural person – fine of $50,000 minimum to $250,000 maximum or 5-10 years imprisonment or both. Summary conviction in the case of a legal person/entity - fine of $100,000 minimum to $500,000 maximum.	Section 7 MLTPA
	Contravention or failure to comply with FIU directives to freeze funds connected with terrorism.	Summary conviction in the case of a natural person – fine of $50,000 minimum to $250,000 maximum or 5-10 years imprisonment or both. Summary conviction in the case of a legal person/entity - fine of $100,000 minimum to $500,000 maximum.	Section 12 MLTPA
	Failure, without reasonable excuse, to comply with all or any of the provisions of an injunction.	Fine in the sum and manner directed by the Court.	Section 35(2) MLTPA
	Failure to comply with any direction or instruction given by the FIU or a supervisory authority under this Act.	Upon summary conviction (unless a penalty is specifically provided for) – fine of $25,000 maximum or imprisonment for three years maximum or both.	Section 83 MLTPA
	Forming a business relationship or carrying on a one-off transaction from within Belize without maintaining proper identification and record-keeping procedures, appropriate internal controls to prevent money laundering and provide training to make employees aware of obligations under the law.	Upon summary conviction – fine of $10,000 maximum.	Section 4(2) MLP Regulations

AREA	DESCRIPTION OF OFFENCE	DESCRIPTION OF PENALTY	SECTION OF LEGISLATION
Reporting Obligations	Failure to make a report on a suspicious transaction to the FIU or willfully making a false or untrue report.	Fine of $50,000 maximum by FIU and possible suspension or revocation of licence by licensing authority.	Section 17(13) MLTPA
	Failure to provide a police officer or the FIU with information to prevent the commission of or the prosecution of a person who commits a terrorist act.	Conviction on indictment to a fine of $10,000 and to imprisonment for a term of two years.	Section 35A (4) (1)
	Failure to disclose to the FIU the possession or control of terrorist property or any information regarding a transaction or proposed transaction in respect of terrorist property required MLTPA section 5F.	Upon conviction, in the case of a natural person, - a fine not exceeding $5,000 or to imprisonment for a term not exceeding two years or both Upon conviction, in the case of a legal person, - a fine which shall not be less than $20,000 but which may extend to $50,000.	Section 5T
	Failure of a person who enters or leaves Belize with more than BZ$10,000 or equivalent foreign currency in cash or negotiable instruments without making a declaration or making a false declaration to the FIU or any other authorised officer.	Upon summary conviction – fine of $50,000 maximum.	Section 37 MLTPA
Other Obligations	Failure to keep transaction records with particulars as required by MLTPA Section 16 (1) for at least five years from the date the transaction was completed or termination of the business relationship, whichever is the later.	Fine of $5,000 maximum by the FIU.	Section 16(7) MLTPA
	Failure of financial institutions to verify, maintain and include originator information on outgoing electronic funds transfers and related outgoing messages.	Fine of $100,000 maximum by the FIU.	Section 19(5) MLTPA
	Failure to produce a document to the Police or an authorized officer of the FIU, as required by a production order; or producing or making available false or misleading material without indicating or providing any correct information.	Upon conviction, in the case of a natural person, – fine of $10,000 maximum or imprisonment for two years maximum or both. Upon conviction, in the case of a legal person or entity, - fine of $50,000 minimum to $100,000 maximum.	Section 25(1) MLTPA

Sanctions by Supervisory Authority	Breach of obligations related to identifying and verifying customer identity; other obligations of reporting entities; reporting suspicious transactions; appointing a Compliance Officer and establishing procedures and including originator information.	Imposition of one or more of the following by the supervisory or regulatory authority or competent disciplinary authority: Written warnings; order to comply with specific instructions; regular reporting on measures being taken; fine not exceeding $500,000; barring the convicted person from employment within the sector; replacing or restricting powers of managers, directors or controlling owners, including appointing an ad hoc administrator; possible suspension, restriction or withdrawal of licence.	Section 22(1) MLTPA
AREA	**DESCRIPTION OF OFFENCE**	**DESCRIPTION OF PENALTY**	**SECTION OF LEGISLATION**
Disclosure of Information	Divulging information (tipping-off) on an ongoing or pending money laundering, terrorism or proceeds of crime investigation, which is likely to prejudice the investigation.	Upon conviction – fine of $50,000 maximum or imprisonment of three years maximum or both.	Section 8(2) MLTPA
	Falsifying, concealing, destroying or otherwise disposing of information or permitting the falsification, concealment, destruction or disposal of any document or material relevant to a money laundering or proceeds of crime investigation or any order made in accordance with the MLTPA.	Upon conviction – fine of $100,000 maximum or imprisonment of five years maximum or both.	Section 9(2) MLTPA
	Willful contravention of a monitoring order or providing false or misleading information in purported compliance with the order.	Upon conviction, in the case of a natural person – fine of $5,000 maximum or imprisonment for two years maximum or both. Upon conviction, in the case of a body corporate – fine of $20,000 maximum.	Section 32(5) MLTPA
	Disclosing the existence of a monitoring order or operation of the order to any person except an officer or agent of the reporting entity to ensure compliance, a legal adviser for obtaining legal advice or representation or a police officer or authorised officer of the FIU authorised in writing to receive the information.	Upon conviction, in the case of a natural person – fine of $5,000 maximum or imprisonment for two years maximum or both. Upon conviction, in the case of a legal person or entity – fine not exceeding $20,000.	Section 33(4) MLTPA

Serious Crime Offences	Knowingly contravening a restraining order by disposing of or otherwise dealing with property that is subject to the restraining order.	Upon conviction, in the case of a natural person – fine of $2,000 minimum to $50,000 maximum or imprisonment for two years maximum or both. Upon conviction, in the case of a legal person or other entity – fine of $50,000 minimum to $100,000 maximum.	Section 45(1) MLTPA
	Where the Court is satisfied that property is tainted in respect of a serious crime of which a person has been convicted.	Upon application by the Director of Public Prosecution or the FIU – Court may order specified property to be forfeited.	Section 49(1) MLTPA
AREA	**DESCRIPTION OF OFFENCE**	**DESCRIPTION OF PENALTY**	**SECTION OF LEGISLATION**
Serious Crime Offences (continued)	Where the Court orders a person convicted of a serious crime to pay a fine instead of orders the forfeiture of tainted property.	In default of payment, Court shall impose imprisonment (to be served consecutively to any other form of imprisonment imposed) of: one year for amounts not exceeding $1,000 two years for amounts exceeding $1,000 but not exceeding $3,000 three years for amounts exceeding $3,000. Rules of remission of sentences of prisoners or release on parole shall not apply	Section 55 MLTPA
	Person convicted of a serious crime in Belize or elsewhere or of an offence under this Act.	Possible ineligibility to be licensed to carry on the business of a financial institution.	Section 36 MLTPA
Terrorist Financing Offences	Willfully providing or collecting funds or other property with the intention of using or in the knowledge that they are to be used, in whole or in part, to commit an act or omission, whether in Belize or elsewhere, to carry out an offence as defined in the listed counter terrorism conventions[5] or any other	Upon conviction, in the case of a natural person – to imprisonment of 10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum.	Section 68 MLTPA

[5] Counter Terrorism Conventions: Convention on Offences and certain Other Acts committed on Board Aircraft, Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, International Convention against the taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the suppression of Unlawful Acts against the Safety

	act; or to commit any act intended to cause death or serious bodily injury of a civilian or other person not taking an active part in hostilities in a situation of armed conflict when the purpose of such act is to intimidate a population or compel a government or international organization to perform or refrain from performing an act of any kind; by a terrorist or a terrorist organization.		
AREA	**DESCRIPTION OF OFFENCE**	**DESCRIPTION OF PENALTY**	**SECTION OF LEGISLATION**
Terrorist Financing Offences (continued)	Organizing, directing others to commit or attempting to or conspiring to commit, participating as an accomplice to a person committing or attempting to commit, aiding, abetting, facilitating, counseling or procuring the commission of a terrorist financing offence.	Upon conviction, in the case of a natural person – to imprisonment of 10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum	Section 68 MLTPA
	Soliciting, receiving, providing or possessing money or other property, entering into or becoming concerned in an arrangement where money or other property is made available or is to be made available for terrorism or a terrorist organisation.	Upon conviction, in the case of a natural person – to imprisonment of 10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum	Section 69 MLTPA
	Entering into or becoming concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property through concealment, removal from the jurisdiction or transfer to any other person.	Upon conviction, in the case of a natural person – to imprisonment of 10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum	Section 70(1) MLTPA
Terrorism Offences	Commission of a terrorist act by a person or body of persons.	Upon conviction, in the case of a natural person – to imprisonment of 10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum.	Sections 5 & 6 MLTPA
	Attempting or aiding, abetting, counseling or procuring the	Upon conviction, in the case of a natural person – to imprisonment of	Section 7 MLTPA

of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, Convention of the Marking of Plastic Explosives for the Purposes of Detention, the International Convention for the Suppression of Terrorists Bombings and the International Convention for the Suppression of the Financing of Terrorism.

	commission of or conspiring to commit terrorism.	10 years minimum to life. Upon conviction, in the case of a legal person/entity - $500,000 minimum to $1,000,000 maximum.	
	Tipping-off	Upon conviction, in the case of a natural person – to a fine of $50,000 maximum or imprisonment of three years maximum or both.	Section 8 MLTPA
	Falsifying, concealing, destroying or otherwise disposing of information or permitting the falsification, concealment, destruction or disposal of any document or material relevant to a terrorism investigation or any order made in accordance with the MLTPA.	Upon conviction – fine of $100,000 maximum or imprisonment of five years maximum or both.	Section 9 MLTPA
	Where the FIU has reasonable grounds to suspect that any cash is intended to be used for terrorism, belongs to or is held in trust for a terrorist organization or is or represents property obtained through acts of terrorism.	Possible seizure of cash.	Section 67 MLTPA

Appendix 5

Verification Examples

A. Natural Persons

- Confirm the date of birth from an official document (e.g., passport);
- Confirm the permanent address (e.g., utility bill, tax assessment, bank statement, letter from a public notary);
- Contact the customer e.g., by telephone, letter, email to confirm information supplied;
- Confirm the validity of the official documents provided through certification by an authorized person;
- Confirm the permanent and business residence through credit agencies, home visits;
- Obtain personal references from third parties and existing customers in writing;
- Contact issuers of references;
- Confirm employment;

B. Corporate Customers & Partnerships

- Review current financial information (preferably audited);
- Obtain statements of affairs, bank statements, confirmation of net worth from reputable financial advisers;
- Seek confirmation from a reputable service provider(s);
- Confirm that the company is in good standing;
- Undertake inquiries using public and private databases;
- Obtain prior banking and commercial references, in writing;
- Contact issuers of references;
- Onsite visitations;
- Contact the customer e.g., by telephone, letter, email to confirm information supplied;

C. Trusts and Fiduciary Clients

- Seek confirmation from a reputable service provider(s);
- Obtain prior bank references;
- Access public or private databases;

Appendix 6

Approved Persons for Certification of Customer Information

In keeping with the requirements on non-face-to-face customers, or where customers are unable to provide original documentation, a financial institution should only accept customer information that has been certified by a qualified practicing notary public.

i. The following original documents are acceptable methods for confirmation of the identity of local customers:

- Government-issued photo-bearing identification (e.g., passport, Social Security Card, Voter's ID orDriver's license)
- Armed forces ID card;
- Employer ID card;

ii. The following original documents are acceptable methods for confirmation of the current permanent address of local customers:

- Government-issued identification;
- Checking telephone directory;
- Recent utility bill;
- Tax bill;
- Letter from a financial institution subject to the MLTPA;
- Letter from the employer acknowledging address;
- Letter from a Judge or Magistrate of the Courts of Belize;
- Letter from an Alcalde acknowledging address;

Appendix 7

Confirmation of Customer Verification of Identity

Part A - Natural Persons

Full Name of Customer: (Mr./Mrs./Ms.)

.....

Known Aliases: .....

Identification: .....

Current Permanent Address: .....

Date of Birth:..... Nationality:.....

Country of Residence: .....

Specimen Customer Signature Attached: Yes □ No □

Part B - Corporate & Other Customers

Full Name of Customer**:** .....

Type of Entity: .....

Location & Domicile of Business: .....

Country of Incorporation:.....

Regulator / Registrar: .....

Names of Directors:.....

.....

Names of majority beneficial owners:.....

.....

Part C

We confirm that the customer is known to us.	Yes ☐	No ☐	
We confirm that the identity information is held by us.	Yes ☐	No ☐	
We confirm that the verification of the information meets the requirements of Belizean law and AML/CFT/CPF Guidelines.	Yes ☐	No ☐	
We confirm that the applicant is acting on his own behalf and not as a nominee, trustee or in a fiduciary capacity for any other person.	Yes ☐	No ☐	N/A ☐

Part D

Customer Group Name:.....

Relation with Customer:.....

Part E

Name & Position of Preparing Officer:.....
(Block Letters)

Signature & Date:.....

Name & Position of Authorizing Officer: .....
(Block Letters)

Signature & Date:.....

Appendix 8

Simplified Customer Due Diligence Requirements

Description	Lower-Value (Tier 1)	Low-Value (Tier 2)
Transaction Limits	<= BZ$1,400 per month	<= BZ$2,500 per month
Customer Type	Natural Person, Belizeans only	Natural Person
CDD Requirements	Basic customer information: • Full legal name • date and place of birth • residential address • source of funds, where necessary contact details.	Basic customer information along with: • anticipated account activity occupation • name of employer or information on the trade/activity where the customer is self-employed.
Verification of Customer Identity	Postponed	Government-issued photo-bearing identification
Record-Keeping Requirements	Obtain and maintain identification particulars	Obtain and maintain identification particulars
Non-Face-to-Face Processes	Allowed	Allowed
Point of Access to Products or Services	Branches and agents of regulated institutions / electronic platforms	
Geographic Reach	Domestic transactions only	

Appendix 9

Beneficial Ownership

The MLTPA defines a beneficial owner as the natural person who ultimately owns or controls a customer, the natural person on behalf of whom a transaction is conducted or the natural person who exercises ultimate control over a legal person or legal arrangement. In the case of a body corporate, any individual who -

1. in respect of a body, other than a company whose securities are listed on an appointed stock exchange, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

2. otherwise exercises control over the management of the body.

It is important to note that a beneficial ownership is not a title. It is the person who has the ultimate control of a legal entity. It may also be the person who receives the ultimate benefits from the operations of the entity. This guide provides circumstances by which each of the legal entities including partnerships and trust are to identify and verify the beneficial owners. This applies to Corporations, Partnerships and Trusts.

Corporations

Beneficial ownership can be determined for a corporation[9] based on the following:

1. **Shares** - A corporation is owned by a natural person by virtue of shares. In other words, a person can only be an owner of a corporation if he or she has shares. The shares can form in many classes and for many purposes. The most common is that everyone has shares which has the same powers for all shareholders. The shares can also be in different classes where one class of shares may have more privileges, rights or able to manage and control the operations of the corporation. The beneficial ownership requirements now require analysis of the actual class of shares and whether any of those affect the management and control of a corporation. If a shareholder has some additional rights or classes of shares through which he or she is able to control the operations and management of the corporation, that becomes an 'indirect control'.

2. **Power to appoint the Board Members** - The Articles of Association of a corporation provides means by which the Board of Directors of a corporation are to be appointed. Normally all the Directors have the same rights to choose the best persons who could look after the interest of the corporation as a whole. However, it can also be possible that due to the strength and the holding of majority capital shares a shareholder may have special rights for appointment of the Board of Directors.

3. **Power to appoint Senior Management Staff** - The operations of a corporation are dependent upon the work of the senior management staff. If one shareholder has certain rights contained in the shareholders Articles of Association by which he or she is able to take control on the appointment of Senior Management staff of the corporation.

4. **Administrative or contractual arrangement with legal entity or shareholders -** This is another means where a shareholder or person may have indirect control of a corporation. This is by entering into administrative or contractual arrangement with a legal entity or shareholders separately.

5. **Providing financial support to the corporation when needed -** This is another situation where a shareholder who has sufficient wealth will be able to manipulate the shareholding arrangements of a corporation. He would legally lend money to the corporation. When the corporation is not able to pay the money back, he would require the other shareholders to raise capital shares of a corporation so that he is able to acquire those shares as part of the corporation discharging his debt.

6. **Any other type of control -**There can be other forms of arrangements by which a beneficial owner may take control or management of the corporation.

Partnership

A partner who is duly registered or has ownership by virtue of the Partnership Agreement is a beneficial owner by virtue of a legal owner. However, it is important to know how a partnership can be indirectly or otherwise controlled. A partnership can be controlled indirectly or otherwise as follows:

1. **Power to make decisions -** A person who has absolute decision-making power or has voting rights in the operations and management of the partnership. This is when in a Partnership Agreement, the Partner may have a greater percentage of the shares or from the time when the Partnership is established, he has ensured to retain the decision making and management of the Partnership.

2. **Power to appoint partners** – A person who holds the power, directly or indirectly, to appoint or remove any partner of the partnership. A person only joins a Partnership if he or she is invited or may be through years of work in the Partnership. The rationale for taking more partners in a Partnership is not important for beneficial ownership. The requirement for indirect or direct control for the partnership for the purposes of beneficial ownership is when a particular partner or partners have the absolute authority to appoint or remove a partner. This is important because every partner in the partnership contributes to the decision making of the partnership. The removal of a partner would enable the remaining partners to make the decision which they intend to make. Equally, they may appoint an additional partner to outvote the remaining partners who may oppose a particular decision. By appointing a new partner, the partners who have control on the appointment or the removal of a partner would be able to make a decision which he or they intend to make.

3. **Entitled to assets** – the person is entitled to assets of the partnership in the event of dissolution of the partnership. This is an essential requirement in considering beneficial ownership in that if a partner has the final interest in the assets of the partnership, when it is dissolved, certainly it can be inferred that the decision making would be affected by this ultimate benefit. In that way he or she will also have indirect control of the management and operations of the partnership or its assets.

4. **Power to declare profits** – the person has the power or authority to declare or make decisions for profit sharing of the partnership. The establishment of partnership no doubt is all geared towards making profit. The partners enjoy the benefits of all the profits. If a partner controls on the declaration of the profits, certainly he has an indirect control on the operations of the partnership. Other partners may have to sometimes accede to the requests or demands of the partner who has such power. In that way the partner has indirect control of the partnership.

Trusts

The beneficial owners of trusts can be identified for the purposes of being registered as beneficial owners including:

1. **Trustee or similar position as trustee** - A trustee is normally provided for in the trust instrument. The trustee is the beneficial owner by virtue of having the management and control of the trust. In trusts, it is not unusual that on certain occasions in disputes, other persons meddle with the operations of the trust. Their decision can also affect the management and control of the trust. By acting in that manner, a person who may make decisions for the trust or take over the management and control of the trust. He or she will be regarded as a beneficial owner.

2. **Settlor** - A settlor establishes or creates a trust. Where settlor appoints trustees or other persons to have the management and control of the trust, in law those persons appointed should have the control and management of the trust. However, there would be circumstances where the settlor by writing or actions would be able to change the trust, terms and conditions or make decisions for the trust and required the trustees to implement such decisions. In the latter case, he or she will not be making a decision directly but the decision which he or she wants will be made through the people he or she appoints. If the settlor does not relinquish all his or her rights, power or authority and control over the trust he or she will at all times may have some right indirectly to manage and control the trust. He or she could also use the beneficiaries of the trust to take management and control of the trust. If the settlor retains any such powers or assumes an ostensible authority to manage and control the trust he or she will be a beneficial owner.

3. **Protector** - A protector for a trust is a person who is not the settlor, trustee or the beneficiary but an agent engaged as the third party to manage and control the trust or control the actions of the trustees. This could be power of attorneys, guardians appointed by beneficiaries or professional advisers. The protector is normally a person who is disinterested in the trust or as to who exercises the power over the terms of the trust. He or she actually performs the role of the trustee. The third party may represent a class of beneficiaries which will also have influence on the decision making on the management and control of the trust.

4. **Beneficiary or class of beneficiaries** - The beneficiaries in a trust also play a substantive role. Where the beneficiaries are able to control or direct the trustees in respect of the matters of trust, the beneficiaries will be treated as beneficial owners. This particularly happens where a class of beneficiaries who may have sufficient numbers for purposes of a trust to make decisions through voting or other democratic processes. In that way, beneficiaries can also coerce trustees

to make a particular decision. The decision-making process itself affects the management and control of the trust.

5. **Guardian** - a guardian holds power of attorney holders or any other person acting on behalf of the trustee, settlor, protector, beneficiaries or class of beneficiaries where the trustee, settlor, protector, beneficiaries or class of beneficiaries is not ascertainable.

6. **any other natural person exercising ultimate effective control** - a person exercising control over the trust including any other person who has under the instrument creating the trust or power to:

(i) amend the trust deed;
(ii) direct investment decision of the trust;
(iii) revoke the trust;
(iv) appoint or remove any of the trustee of the trust; or
(v) direct the distribution of assets or funds of the trust.

Obligation of Financial Institutions

It is a requirement of the legal entity to at all times maintain 'adequate, accurate and current beneficial ownership information'. Financial institutions are to ensure that customer due diligence information is sufficiently capable of identifying who the beneficial owner is. The information should be sufficient through which any person would be able to identify who is the person who has beneficial ownership control.

Customer due diligence information must be accurate information. The details of the beneficial owners must be in accordance with the requirements of the MLTPA and these Guidelines. If there is any change or any details are wrongly recorded, it must be corrected.

Customer due diligence information must also be current. The requirement for current information is that any changes or variations should be provided as soon as possible. Such information is to be provided by the beneficial owner or the entity within one (1) month.

In instances where the natural persons with controlling interest and persons exercising control through other means cannot be identified, identify the natural persons having the position of chief executive or a person of equivalent or similar position.

Appendix 10

Red Flags

There are a myriad of ways in which money laundering or terrorism financing may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention. Financial institutions are encouraged to refer to the FATF and Egmont Group for typology reports and sanitized cases on ML/TF schemes, respectively.

General

If the Client:

- Does not want correspondence sent to home address.
- Shows uncommon curiosity about internal systems, controls and policies.
- Over justifies or explains the transaction.
- Is involved in activity out-of-keeping for that individual or business.
- Produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Provides insufficient, false, or suspicious information, or information that is difficult or expensive to verify.

Economic Purpose

- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer's business.

If the Client:

- Starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past.
- Frequently exchanges small bills for large ones.
- Deposits small amounts of cash on different successive occasions in such a way that on each occasion the amount is not significant, but combined, total a very large amount. (i.e., "smurfing").
- Consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Stated occupation is not in keeping with the level or type of activity (e.g. a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Unusually large deposits or withdrawals of cash by an individual or a legal entity whose apparent business activities are normally carried out using cheques and other monetary instruments.

Deposit Activity

- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly exhibits significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

Cross-border Transactions

- Deposits followed within a short time by wire transfers to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
- Immediate conversion of funds transfers into monetary instruments in the name of third parties.
- Frequent sending and receiving of wire transfers, especially to or from countries considered high-risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family-run banks, shell banks or unknown banks.
- Large incoming or outgoing transfers, with instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities having no apparent business connection with client.
- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Increased use of safety deposit boxes. Increased activity by the person holding the boxes. The depositing and withdrawal of sealed packages.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated;
- Transactions are with persons in jurisdictions that do not have adequate systems in place to prevent money laundering/terrorist financing.

Corporate and Business Transactions

- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Unexplained transactions are repeated between personal and business accounts.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

Lending

- Customer suddenly repays a problem loan unexpectedly, without indication of the origin of the funds.
- Loans guaranteed by third parties with no apparent relation to the customer.
- Loans backed by assets, for which the source is unknown or the value has no relation to the situation of the customer.
- Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.
- Use of standby letters of credit to guarantee loans granted by foreign financial institutions, without any apparent economic justification.

Securities Dealers

- Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.

Accounts Under Investigation

- Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in a court or other competent national or foreign authority in connection with fraud, terrorist financing or money laundering.
- Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority with fraud, terrorist financing or money laundering.

Appendix 11

Declaration of Source of Funds / Source of Wealth

(Cross out the term that is not applicable)

Customer Name or Business:.....

Current Address: .....

Account Number:.....

Identification: .....

Amount of Transaction & Currency: .....

Description/Nature of Business Transaction:

Deposit ☐	Loan ☐	Currency Exchange ☐	Wire Transfer ☐
Credit/Debit Card ☐	ATM ☐	Trust Settlement/Distribution ☐	Investment ☐
Monetary Instrument ☐		Other (Specify) ☐	

Source of Funds / Wealth:

.....

.....

Supporting Evidence: .....

Customer Signature: .....

Date: .....

Transaction Approved? Yes ☐ No ☐

If No, state reason:.....

.....

....

OFFICER COMPLETING TRANSACTION
(Signature & Title)

AUTHORISING OFFICER
(Signature & Title)

Appendix 12

FINANCIAL INTELLIGENCE UNIT

Suspicious Transaction Report

SECTION 17(4)(b) OF THE MONEY LAUNDERING & TERRORISM (PREVENTION) ACT, 2008

SECTION 7(3) OF THE FINANCIAL INTELLIGENCE UNIT ACT, 2002

(Complete all applicable parts - See Instructions)

Part I	**Reporting Entity/Financial Institution Information**	**1**

1. Name of Reporting Entity/Financial Institution

2. Address of Reporting Entity/Financial Institution

3. Address of Branch Office(s) where activity occurred

4. Account number(s) affected, if any

a _____ Closed ☐ Yes ☐ No

b _____ ☐ Yes ☐ No

c _____ Closed ☐ Yes ☐ No

d _____ ☐ Yes ☐ No

Part II	**Suspect Information**	☐ Suspect Information Unavailable

5. Last Name or Name of Entity	6. First Name	7. Middle Name

8. Address

9. Phone Number – Residence	10. Phone Number – Work

11. Occupation/Type of Business	12. Date of Birth	13. Admission/Confession?
	_____/_____ /_____ MM DD YYYY	a ☐ Yes b ☐ No

14. Forms of Identification for Suspect:

a ☐ Driver's License b ☐ Passport c ☐ Social Security Card d ☐ Other

Number _____ Issuing Authority _____

15. Relationship to Reporting Entity/Financial Institution:

a ☐ Accountant c ☐ Attorney e ☐ Customer h ☐ Officer

b ☐ Agent d ☐ Borrower f ☐ Director i ☐ Shareholder

g ☐ Employee j ☐ Other _____

16. Is the relationship an insider relationship? a ☐ Yes b ☐ No If Yes specify: c ☐ Still employed at reporting entity/financial institution d ☐ Suspended e ☐ Terminated f ☐ Resigned	17. Date of Suspension, Termination, Resignation _____/_____ /_____ MM DD YYYY

Part III	**Suspicious Activity Information**	**2**

18. Date or date range of suspicious activity

From _____/_____ /_____ To _____/_____ /_____
MM DD YYYY MM DD YYYY

19. Total dollar amount involved in known or suspicious activity

20. Summary characterization of suspicious activity:

a	☐ Money Laundering	f	☐ Computer Intrusion	l	☐ Debit Card Fraud
b	☐ Bribery	g	☐ Consumer Loan Fraud	m	☐ Defalcation/Embezzlement
c	☐ Check Fraud	h	☐ Counterfeit Check	n	☐ False Statement
d	☐ Check Kiting	i	☐ Counterfeit Credit/Debit Card	o	☐ Misuse of Position
e	☐ Commercial Loan Fraud	j	☐ Counterfeit Instrument (other)	p	☐ Mortgage Loan Fraud
				q	☐ Mysterious Disappearance
				r	☐ Wire Transfer Fraud

s ☐ Other _____
(Type of Activity)

21. Amount of loss prior to recovery (if applicable)

22. Dollar amount of recovery (if applicable)

23. Has the suspicious activity had a material impact on, or otherwise affected, the financial soundness of the reporting entity/institution?

a ☐ Yes b ☐ No

24. Has any law enforcement agency already been advised by telephone, written communication, or otherwise? a ☐ Yes b ☐ No

Agency Name _____

25. Name of person(s) contacted at Law Enforcement Agency

26. Phone Number

Part IV	**Contact for Additional Information**

27. Last Name

28. First Name

29. Middle Initials

30. Title/Occupation

31. Phone Number

32. Date Prepared

_____/_____ /_____
MM DD YYYY

Part V	Suspicious Activity Information Explanation/Description	3

Explanation/description of known or suspected violation of law or suspicious activity.

This section of the report is **critical**. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood. Provide below a chronological and **complete** account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account. **If necessary, continue the narrative on a duplicate of this page.**

a **Describe** supporting documentation and retain for 5 years.
b **Explain** who benefited, financially or otherwise, from the transaction, how much, and how.
c **Retain** any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.
d **Retain** any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.
e **Retain** any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others.
f **Indicate** where the possible violation took place (e.g., main office, branch, other).
g **Indicate** whether the possible violation is an isolated incident or relates to other transactions.
h **Indicate** whether there is any related litigation; if so, specify.
i **Recommend** any further investigation that might assist law enforcement authorities.
j **Indicate** whether any information has been excluded from this report; if so, why?
k If you are correcting a previously filed report, describe the changes that are being made.

For Money Laundering reports, include the following additional information:

l **Indicate** whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, letter of credit, money order, traveler's checks, wire transfers sent or received, cash, etc.).
m **Indicate** any account number that may be involved or affected.

Suspicious Transaction Report
Instructions

Section 17(4)(b) of the Money Laundering and Terrorism (Prevention) Act (MLTPA), 2008, imposes a statutory obligation on all reporting entities/financial institutions and their staff to report suspicions of money laundering transactions to the Supervisory Authority, to wit the Financial Intelligence Unit (FIU).

Section 17(12) of the MLTPA exempts a reporting entity/financial institution and their employees, staff, directors, owners or other representatives as authorized by law, from criminal, civil, disciplinary and/or administrative liability, as the case may be, for complying with Section 17(4)(b) of the MLTPA or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication.
Reporting Entities/Financial institutions are required to file a Suspicious Transaction Report with the FIU on all complex, unusual or large business transactions, unusual pattern of transactions (whether completed or not) and insignificant but periodic transactions that have no apparent economic or lawful purpose.

In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the reporting entity/financial institution shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities in addition to filing a timely Suspicious Transaction Report with the FIU.

WHEN TO MAKE A REPORT:

1. All reporting entities/financial institutions operating in Belize, including any person whose regular occupation or business is, the carrying on of any activity listed in the First Schedule of the MLTPA and any other activity defined by the Minister of Finance as such by an Order published in the *Gazette* amending the First Schedule of the MLTPA.

    a. **Transactions that involve potential money laundering.** Any transaction (which for purposes of this subsection means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a entity/financial institution, by whatever means effected) conducted or attempted by, at or through the entity/financial institution and involving funds or other assets, if the reporting entity/financial institution knows, suspects, or has reason to suspect that:

        i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under law;

        ii. The transaction is designed to evade any regulations promulgated under the MLTPA; or

        iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the reporting entity/financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

    b. **Violations where a suspect can be identified.** Whenever the entity/financial institution detects any known or suspected criminal violation, or pattern of criminal violations, committed or attempted against the entity/financial institution or involving a transaction or transactions conducted through the entity/financial institution and involving funds or other assets, where the entity/financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the entity/financial institution was used to facilitate a criminal transaction, and the entity/financial institution has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing a Suspicious Transaction Report that the identified suspect or group of suspects has used an "alias," then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported.

    c. **Violations regardless of a potential suspect.** Whenever the entity/financial institution detects any known or suspected criminal violation, or pattern of criminal violations, committed or attempted against the entity/financial institution or involving a transaction or transactions conducted through the entity/financial institution and involving funds or other assets, where the entity/financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the entity/financial institution was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

    d. **Insider abuse.** Whenever the entity/financial institution detects any known or suspected criminal violation, or pattern of criminal violations, committed or attempted against the entity/financial institution or involving a transaction or transactions conducted through the entity/financial institution, where the entity/financial institution believes that it was either an actual or potential victim of a financial criminal violation, or a series of financial criminal violations, or that the entity/financial institution was used to facilitate a financial criminal transaction, and the entity/financial institution has a substantial basis

for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a financial criminal act regardless of the amount involved in the violation.

2. A reporting entity/financial institution is required to promptly file a Suspicious Transaction Report after the date of initial detection of facts that may constitute a basis for filing a Suspicious Transaction Report. If no suspect was identified on the date of detection of the incident requiring the filing, a reporting entity/financial institution may delay filing a Suspicious Transaction Report to identify a suspect. In no case shall reporting be delayed more than 3 calendar days after the date of initial detection of a reportable transaction.

3. A Suspicious Transaction Report does not need to be filed for those robberies and burglaries that are reported to law enforcement authorities, or for lost, missing, counterfeit, or stolen securities that are reported to law enforcement authorities.

HOW TO MAKE A REPORT:

1. Send each completed Suspicious Transaction Report to:

   Financial Intelligence Unit, c/o Central Bank Building, Gabourel Lane, PO Box 2197, Belize City, BELIZE

2. For items that do not apply or for which information is not available, leave blank.
3. Identify and retain a copy of the Suspicious Transaction Report and all original supporting documentation or business record equivalent for 5 years from the date of the Suspicious Transaction Report.
4. If more space is needed to report additional suspects, attach copies of page 1 to provide the additional information.

DEFINITIONS

A. **Reporting Entity/Financial Institution** – Any person whose regular occupation or business is the carrying on of any activity listed below:

1. Acceptance of deposits and other repayable funds from public.
2. Lending, including consumer credit, mortgage credit, factoring (with or without recourse) and financing of commercial transactions.
3. Financial leasing.
4. Transfer of money or value.
5. Money and currency changing (such as Casa de Cambios).
6. Pawning.
7. Issuing and administering means of payment (such as credit and debit cards, traveller's cheques, money orders, bankers draft and electronic money).
8. Issuing financial guarantees and commitments.
9. Trading for own account or for account of customers in money market instruments (such as cheques, bills, certificates of deposit, derivatives), foreign exchange, financial futures and options, exchange and interest rate instruments, transferable securities and commodity futures trading.
10. Credit unions.
11. Participation in securities issues and the provision of financial services related to such issues.
12. Advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings.
13. Portfolio management and advice whether individual or collective.
14. Safekeeping and administration of securities.
15. Safekeeping and administration of cash or liquid securities on behalf of other persons.
16. Otherwise investing, administering or managing funds or money on behalf of other persons.
17. Gambling houses.
18. Casinos.
19. Internet Casinos or Online Gaming.
20. Buying or selling of gold bullion.
21. Insurance business.
22. Venture risk capital.
23. Unit Trusts.
24. A trust or company services provider not otherwise covered by this schedule, which as a business, provides an of the following services to third parties:
    - Acting as a formation agent of legal persons;

- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust; and
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

25. International (or Offshore) banking business as defined in the International Banking Act.
26. Lawyers, notaries, other independent legal professionals, accountants, auditors and tax advisers, when they prepare for or carry out transactions for their clients concerning the following activities:
    - Buying and selling of real estate;
    - Managing of client money, securities or other assets;
    - Management of bank, savings or securities accounts;
    - Organization of contributions for the creation, operation or management of companies;
    - Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
27. Dealing in real estate when the persons dealing are involved in transactions concerning the buying and selling of real estate.
28. Dealing in precious metals and dealing in precious stones.
29. Dealing in vehicles.
30. Engaging in international financial services as defined in the International Financial Services Commission Act.

B. **Transaction** – A transaction shall include:
   a. opening of an account;
   b. any deposit, withdrawal, exchange or transfer of funds in any currency whether in cash or by cheque, payment order or other instrument or by electronic or other non physical means;
   c. the use of a safety deposit box or any other form of safe deposit;
   d. entering into any fiduciary relationship;
   e. any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation;]
   f. any payment made in respect of a lottery, bet or other game of chance;
   g. an act or combination of acts performed for or on behalf of a client in connection with purchasing, using or performing one or more services, or such other actions as may be prescribed by the Minister by Order published in the Gazette.