Anti-Money Laundering
and
Combating the Financing of Terrorism
(AML/CFT) Guidelines

for
Banks,
Financial Institutions,
Credit Unions
and
Money Transfer Services Providers

TABLE OF CONTENTS

INTRODUCTION

Money laundering is not a new phenomenon in the financial sector. The global trend has been geared towards continuously strengthening systems that are in place to deter illicit activities and their related offences. Hence, more emphasis is being applied to detecting attempts to launder money and finance terrorism. Given that the aforementioned 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 and Combating the Financing of Terrorism Guidelines (AML/CFT 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. As such, the Central Bank is hereby providing guidance to banks, financial institutions, credit unions and money transfer services providers that fall under its regulatory umbrella, with a view to strengthening the compliance functions of the relevant institutions.

These Guidelines hereby replace the previously issued Money Laundering (Prevention) Guidance Notes for Banks and Financial Institutions, 1998 to which Central Bank-regulated entities must abide.

SCOPE

These Guidelines are sector specific and must be viewed in collaboration with the MLTPA and accompanying Regulations. The Guidelines lay down the expectations of the Central Bank as regards the minimum standards for anti-money laundering/combating the financing of terrorism (AML/CFT) practices by all financial institutions. Towards this end, financial institutions should integrate AML/CFT 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 policies.

These Guidelines draw on the principles contained in the Revised Forty Recommendations and Special Nine Recommendations on Terrorist Financing, as developed by the Financial Action Task Force[1] (FATF). It encapsulates concepts from various papers on related topics as set out by the Basle Committee on Banking Supervision, as well as incorporates local AML/CFT legislation.

APPLICATION

Banks, financial institutions, credit unions and money transfer services providers should apply adequate resources in order to mitigate the risks involved in transacting the proceeds of illicit activities. All banks and financial institutions licensed under the Banks and Financial Institutions Act (BFIA) and International Banking Act (IBA), credit unions registered under the Credit Unions

[1] FATF is an inter-governmental body which sets standards, develops and promotes policies to combat money laundering and terrorist financing.

Act (CUA) and money transfer services providers registered under the Exchange Control Regulations are obligated to comply with these Guidelines, which contain both advisory and obligatory requirements. Advisory matters are expressed using the term "may". This allows banks and financial institutions to implement alternative but just as effective measures in the particular circumstances. On the other hand, institutions are not to divert from mandatory requirements which are expressed using the term "should".

These Guidelines apply to all entities in Belize that are licensed under the BFIA and IBA, credit unions registered under the CUA and money transfer services providers registered under the Exchange Control Regulations. These institutions are referred to as "financial institutions" throughout these Guidelines. Financial institutions should ensure that, at a minimum, the 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. For the purpose of these Guidelines, general references to money-laundering should be interpreted to include both money-laundering and/or terrorist financing.

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	-	All administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the Financial Intelligence Unit (FIU) and supervisors.
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 BFIA and IBA, credit unions registered under the CUA and money transfer services providers registered the Exchange Control Regulations. (See Appendix 1)
Immediate family	-	The parents, siblings, spouse, children and in-laws of the person who has been designated a PEP.
Intermediary	-	A financial institution, such as a bank, that acts as a conduit between suppliers of funds (depositors) and users of funds (borrowers).
Money Transfer 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.
Money transmission agent	-	A person carrying on money transfer services on behalf of a money transfer service provider.
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.
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 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 money laundering and terrorist financing.
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/CFT	-	Anti-Money Laundering/Combating the Financing of Terrorism

AML/CFT Guidelines	-	Anti-Money Laundering and Combating the Financing of Terrorism Guidelines
BFIA	-	Banks and Financial Institutions Act
CDD	-	Customer Due Diligence
Central Bank	-	Central Bank of Belize
CUA	-	Credit Unions Act
FATF	-	Financial Action Task Force
FIU	-	Financial Intelligence Unit
IBA	-	International Banking Act
KYC	-	Know Your Customer
MLRO	-	Money Laundering Reporting Officer
MLTPA	-	Money Laundering and Terrorism (Prevention) Act
NPO	-	Non-Profit Organization
PEP	-	Politically Exposed Persons
STR	-	Suspicious Transaction Report

SECTION I - BACKGROUND

1.1 Money Laundering Defined

2. Money laundering 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 money laundering is punishable, upon conviction, with a fine and/or imprisonment **(see Appendix 4)**.

1.2 Stages of Money Laundering

4. Money laundering 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 disposal of cash derived from criminal activity.

      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 includes 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, or a serious risk to public health or safety, or 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 money laundering and terrorist financing is that while money laundering seeks to legitimize money from illegal sources, terrorist financing 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. Terrorist financing 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 similar to those utilized by criminal organizations, especially when funds are from illegitimate sources. Regardless of the source, however, 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 FIU has powers to direct that accounts held on behalf of terrorists or terrorist organizations 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 Vulnerability of Banks and Financial Institutions to Money Laundering

13. Efforts to combat money laundering 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 money laundering 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.

14. The most common form of money laundering 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.

15. 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.

1.6 Tipping-Off

16. It is an offence under the MLTPA for a person who knows or suspects that an investigation into money laundering 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)**. Initial enquiries 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. Where it is known or suspected that an 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.

1.7 International Initiatives

17. Standard setters, such as the Basel Committee on Banking Supervision and FATF, provide guidance on measures which banks and financial institutions should apply as part of their AML/CFT programme. This internationally accepted framework includes the Forty Recommendations and the Special Nine Recommendations on Terrorist Financing, supported by subsequently issued papers covering a range of topics including:

i. Customer due diligence for banks;

ii. General guide to account opening and customer identification;

iii. Consolidated KYC risk management;

iv. Special recommendations on terrorist financing and the self assessment exercise;

v. Guidance for Financial Institutions in detecting terrorist financing and interpretative notes;

vi. Criminalizing the financing of terrorism and the associated money laundering;

vii. Freezing and confiscating terrorist assets;

viii. Alternative remittance;

ix. Wire transfers;

x. Non-profit organizations; and

xi. Cash couriers.

1.8 Legislative and Regulatory Framework

18. Belize's commitment to fight the harmful effects of money laundering, terrorist financing and their related offences is manifested in the following legislations and agreements aimed at suppressing serious crimes. They include:

i. Money Laundering (Prevention) Regulations, 1998;

ii. Prevention of Corruption Act, 2000 CAP 105;

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

iv. Financial Intelligence Unit Act, 2002 (No. 35 of 2002);

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

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

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

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

ix. Money Laundering and Terrorism (Prevention) Act, 2008 CAP 104;

1.9 Penalties for Non-Compliance

19. 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 legal framework. Upon summary conviction, penalties range from fines of BZ$1,000 minimum to BZ$1,000,000 maximum and/or imprisonment from two years to life. Penalties also include possible seizure of cash, sanctions imposed by the supervisory authority and possible suspension, restriction or revocation of licence. Administrative penalties range from BZ$5,000 to BZ$50,000, while fines may also be applied at the discretion of the Courts. A financial institution should therefore be vigilant and aspire to operate within the confines of the laws.

20. A summary of the money laundering and terrorism offences directly related to the MLTPA are set out in Appendix 4.

1.10 The Role of the Financial Intelligence Unit

21. The FIU is Competent Authority and the money laundering 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 information and cooperating with foreign FIUs;

iv. 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;

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

vi. 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;

vii. 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.

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

ix. 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(1)(k) of the MLTPA;

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

xi. 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.

22. The FIU's responsibilities may also include:

i. Providing instructions to a reporting entity to take certain steps, such as freezing of a person's funds and other financial assets to facilitate any investigation, prosecution or proceeding for a money laundering offence or for terrorist financing, in Belize or elsewhere;

ii. Conducting research into trends and developments in the area of money laundering and financing of terrorism. Research may also cover improved ways of detecting, preventing and deterring money laundering and terrorist financing.

iii. Educating the public and creating awareness on matters relating to money laundering and terrorist financing;

iv. Consulting with any relevant person, institution or organization in the exercise of its

powers or duties under paragraph 21(vii) 22(i), 22(ii) or 22(iii), 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.

23. 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 and/or the Police Department.

1.11 The Role of the Central Bank of Belize

24. 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 on-site examinations or using other means to supervise and regulate particular reporting entities to ensure compliance with the obligations set out in Sections 15 -19 of the MLTPA;

   a. By virtue of the BFIA, 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 particular 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 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 could be related to money laundering, terrorist financing 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 and select officers and controlling owners that breach obligations established under sections 15 - 19 of the MLTPA;

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

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

xi. Informing the FIU upon the discovery of facts likely to constitute indication of money laundering or terrorist financing.

25. Through periodic on-site examinations, the Central Bank, in its capacity as the supervisory and regulatory authority for financial institutions licensed or registered under the BFIA, IBA, CUA or Exchange Control Regulations, will assess a financial institution's AML/CFT 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 Section 36 of the BFIA or Section 45 of the IBA. Furthermore, the Central Bank may instruct a financial institution to file a suspicious transaction report where the situation necessitates, provided that the financial institution had not yet filed such a report.

26. Accessing relevant reports and working papers prepared in the external and internal audit process, to evaluate adherence to KYC standards.

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

28. The Central Bank should not be impeded by local bank secrecy laws from accessing information required to properly perform its functions to combat money laundering and terrorist financing. 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.

29. 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).

30. The Central Bank reserves the right to amend these Guidelines from time to time. In the interim, a financial institution should continuously update its AML/CFT programme as industry standards evolve.

31. 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 money laundering and terrorist financing.

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

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

33. The Board of Directors is ultimately responsible for the effectiveness of the financial institution's AML/CFT 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.

34. 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 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.

35. Directors should therefore demonstrate their commitment to an effective AML/CFT programme by:

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

represent;

ii. Approving AML/CFT 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 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. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems. (See Section on Compliance and Audit).

36. Senior management is responsible for the development of sound risk management programmes 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 money laundering and terrorist financing 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 ongoing 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 enquiries about the personal history of the potential employee and verifying appropriate references on the individual.

37. 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

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

39. Financial institutions should document a risk-based approach in their AML/CFT programmes. This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This should be evidenced by categorization of the customer base, products and services by risk rating (e.g. low, medium, high) and identification of assigned actions by risk types.

40. While each financial institution will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks. A financial institution should conduct periodic reviews (however, not more than two years apart) to determine whether any adjustment should be made to the risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

41. The risk rating framework should take into account customer acceptance and on-going monitoring policies and procedures that assist the financial institution in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk. A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve business relationships with such customers. The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason for such change.

42. All financial institutions should therefore design an AML/CFT framework that satisfies the

needs of their institution but should include at a minimum:

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. KYC documentation and due diligence information requirements appropriate for each risk category and risk factor; and

iv. Requirements for the approval of upgrading and downgrading of customer risk ratings.

43. A financial institution should establish a customer's profile taking into account, at a minimum:

i. The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);

ii. The nature and frequency of the activity;

iii. The complexity, volume and pattern of transactions;

iv. Type, status (whether dormant or active) and value of account;

v. Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);

vi. Type of product/service (e.g. whether private banking, one-off transaction, mortgage);

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

viii. Geographical origin of the customer;

ix. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);

x. Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;

xi. Unwillingness of the customer to cooperate with the financial institution's customer due diligence process for no apparent reason;

xii. Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

44. Accordingly, a financial institution may apply customer due diligence standards on a risk sensitive basis, consistent with these Guidelines, depending on the type of customer, business relationship or transaction. Reduced due diligence 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 money laundering or terrorist financing is high. It follows, then, that simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

45. In addition to "Red Flags" appended to these Guidelines, typologies of money laundering and terrorist financing schemes are available at websites such as www.fatf-gafi.org to assist in risk categorization.

46. A financial institution 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, a financial institution should periodically review their risk categories as typologies evolve on practices by money launderers and terrorists. These reviews should not be undertaken more than two years apart.

2.1 Prospective Customers

47. Prior to establishing a business relationship, a financial institution should assess the potential risk inherent in each new client relationship. This assessment should take into account 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. The financial institution should then decide whether or not to establish or continue with a relationship.

2.2 Existing Customers

48. A financial institution is required to risk rate all client relationships including those in existence prior to the implementation of these Guidelines. All risk ratings should be documented and should be in place for all customers within one year of the implementation of these Guidelines.

SECTION III – KNOW YOUR CUSTOMER

3.1 Customer Due Diligence

49. Customer due diligence is an essential element of the effort to prevent the financial system from being used to perpetrate money laundering and terrorist financing. 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.

50. A financial institution must avoid 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 Compliance Officer, other appropriate staff and competent authorities.

51. 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.

52. 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 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 (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 (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.

53. 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

[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.

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 certificate and driver's license) 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 Section on Identification Procedures.

54. For the purpose of these Guidelines, the financial institution should seek to identify the customer and all those who exercise control over the account/transaction. 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.

55. 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);

iii. The money laundering 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.

56. 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.

57. 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 a suspicious transaction report.

58. Where there is a suspicion that an asset is suspected to either stem from a criminal activity, or is linked or related to, or is to be used to finance terrorism or a transaction relates to money laundering or the financing of terrorism, 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 this is not possible, then the financial institution 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

59. 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.

60. Once a business relationship has been established, the financial institution should take reasonable steps to ensure that information collected in the customer due diligence 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.

61. 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.

62. 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.

63. 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

64. 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$15,000, 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$15,000 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$15,000, verification should be conducted as soon as practicable after the financial institution becomes aware of the foregoing circumstances;

v. 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; or

   b. 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; and

vi. 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.

vii. 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.

viii. 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

65. A financial institution should obtain relevant information on the identity of its customer and should seek to verify information on a risk basis, subjecting greater 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, or driver's license along with a passport or social security 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.

66. 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 along with a passport or social security card);

iii. Date and place of birth and nationality (indication should be made if dual citizenship is maintained);

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

v. Signature;

vi. Purpose of the account and the nature of the business relationship.

67. 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;

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

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

iii. Source of funds; and

iv. Any other information deemed appropriate and relevant.

68. 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.

69. 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

70. 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.

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

72. Both residence and nationality should 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.

73. 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.

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

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

76. 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 bearing the photograph and signature of the applicant (to be used along with a passport or social security card);

iv. Voter's card;

v. Social security card; or

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

77. 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

78. Where a customer's identity 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);

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

79. 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.

80. A financial institution may also as part of its own internal AML/CFT 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.

81. 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.

82. When an existing customer 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. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important 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

83. 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.

84. 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 senior staff member.

85. 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)**.

86. A certifier must be a qualified practicing notary public or attorney-at-law.

87. 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

88. To satisfy itself as to the identity of the corporate customer, the financial institution should obtain:

i. Name of corporate entity;

ii. Principal place of business and registered office;

iii. Mailing address;

iv. Contact telephone and fax numbers;

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

vi. 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;

vii. 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;

viii. Identity information on the natural persons with a controlling interest in the corporate entity. This information should extend, as far as practicable, to identifying those with a minimum of 10% 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. However, 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;

ix. Confirmation before a business relationship is established, by way of company search and/or other commercial enquiries 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;

89. 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 the Memorandum and 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 financial information or audited statements;

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

viii. 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;

ix. 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

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

90. 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.

91. 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.

92. 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. Enquiries 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.

93. 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.

94. 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.

95. 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.

96. When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering or terrorist financing activity, even though authorized signatories have not changed.

4.2.1 Powers of Attorney

97. 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

98. 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.

99. 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.

100. 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

101. Legal structures such as trusts and foundations and nominee 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 money laundering and terrorist financing through the use of 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

102. 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 or not these clients or customers are acting on their own behalf.

103. 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.

104. 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. In the case of a nominee relationship, obtain identification evidence for the beneficial owner(s).

105. 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.

106. 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.

107. 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.

108. 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 authorised signatories to the bank account should also be verified.

109. 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 enquiries.

110. 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.

111. 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.

112. 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.

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

114. 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

115. 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

116. 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.

117. 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

118. 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.

119. 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

120. Special consideration should be given to the following products and services, which may pose added risk:

4.4.1 Provision of Safe Custody and Safety Deposit Boxes

121. Where facilities to 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

122. A financial institution should have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing 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 particular 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 RELIANCE ON THIRD PARTIES TO CONDUCT KYC ON CUSTOMERS

123. 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 somehow has an interest in or is affected by it.

124. 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.

125. 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 BFIA, or a credit union. Examples of such circumstances are:

i. Where a financial institution is unable to readily determine whether or not 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.

126. 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.

127. 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.

4.5.1 Intermediaries

128. 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 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.

4.6 EXEMPTIONS AND CONCESSIONS

4.6.1 Financial Institutions

129. Verification of identity is not normally required when the facility holder is an eligible introducer (see Section on Introduced Business). A financial institution should satisfy itself that the financial institution does actually 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 standards of regulation.

130. 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.

4.6.2 Occasional Transactions

131. 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.

132. 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:

a. Encashment of cheques drawn on the financial institution;

b. Exchange of coins for cash;

c. Purchase of foreign currency for holiday travel; and

d. Transactions via money transfer services business.

133. Due diligence measures including identifying and verifying the identity of customers, should be undertaken on, inter alia on occasional transactions over BZ$15,000 or its equivalent in foreign currency, whether conducted in a single transaction or multiple operations that appear to be linked;

134. 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.

135. At a minimum, a financial institution should:

i. Identify and verify[3] 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.

136. 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$15,000 or the equivalent in any other currency, are exempt from full verification requirements.

137. 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$15,000 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$15,000 or its equivalent.

138. As per best practice, a time 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.

139. 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 enquiries should be made. If as a result of enquiries, the financial institution becomes aware of or suspects money laundering or the financing of terrorism the financial institution must take steps to verify the proposed client's identity. Where money laundering is known or suspected, the financial institution should make a suspicious transaction report regardless of the size of the transaction. Where terrorist financing is known or suspected, the financial institution should make a report to the FIU in accordance with Section 17 of the MLTPA.

4.6.3 Exempted Customers

140. 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);

[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.

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$15,000 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$15,000 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.

viii. The applicant for business is acquiring an equity interest in any type of collective investment scheme.

141. 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 money laundering or terrorist financing is known or suspected. If money laundering 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.

4.7 ENHANCED DUE DILIGENCE

142. A financial institution should apply enhanced CDD measures on a risk sensitive basis for such customers assessed as presenting a higher risk for money laundering or terrorist financing. 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.

143. 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.

144. 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 money

laundering or terrorist financing risk that the customer is assessed to present to the financial institution. A financial institution should hold a fuller set of information in respect of those customers assessed as carrying a higher money laundering or terrorist financing risk or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

145. 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.

146. 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 relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML/CFT measures;

v. Corporate customers able to issue bearer shares or bearer instruments.

4.7.1 Non-Profit Organizations

147. Non-Profit Organizations (NPOs) may pose specific risks of money laundering or terrorist financing 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.

148. 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 organisations, 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.

149. 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.

150. Where a facility holder is a non-profit organization, 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.

151. 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.

152. 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.

153. Where a non-profit organization 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.

154. A financial institution should refer to Appendix 2 for a list of relevant websites which

provide information on non-profits organizations and charities.

155. Whilst it is not practical to obtain documentary evidence of identity of all donors, a financial institution should undertake a basic "vetting" of all non-profit organizations established in other jurisdictions, in relation to known money laundering and terrorist activities. This includes a reasonable search of public information, verifying that the non-profit organization does not appear on any terrorist lists nor that it has any association with money laundering 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.

4.7.2 Non-Face-to-Face Customers

156. 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.

157. 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 money laundering and terrorist financing risk presented by the customer.

158. 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 standards of regulation.

159. 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. 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;

160. 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 customer due diligence standards; and

iii. Obtain any other information deemed appropriate.

161. 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.

162. 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 of 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.

163. Any subsequent change to the customer's name, address or employment details of which the financial institution becomes aware should be recorded and also 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 money laundering or terrorist financing prevention.

164. 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.

165. 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.

4.7.3 Introduced Business

166. 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.

167. 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.

168. 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;

iii. Immediately obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;

iv. Where copies of documentation are not obtained, a financial institution should take adequate steps to satisfy itself that copies of identification data and relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

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

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

vii. 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.

169. The Central Bank, as Supervisory Authority, may extend the status of eligible introducer to particular 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;

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

170. 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 169 (i-ii) above;

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

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

171. 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. The financial institution should however, retain copies of the identification records in accordance with the requirements in the MLTPA. A financial institution should obtain written confirmation from a group member confirming completion of verification. See Appendix 7.

172. 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 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.

173. 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 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.

4.7.4 Professional Service Providers

174. Professional service providers act as intermediaries between clients and the financial institution and 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.

175. Where pooled accounts are managed by:

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

b. 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 a minimum, equivalent due diligence standards as set out in these Guidelines and has systems and controls to allocate the assets to the relevant beneficiaries.

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

4.7.5 Politically Exposed Persons

177. The MLTPA defines PEPs as individuals in Belize or in a foreign country entrusted with public functions, their family members or close associates. These functions include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials including family members or close associates of the politically exposed person. For the purposes of these Guidelines, once persons are identified as PEPs they are always to be considered as PEPs.

178. 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 should 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 on-going 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; and

iv. Require senior management or the board 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 or not 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.

179. In addition to the identity 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 having transaction authority over the account; and

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

180. In particular, 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 so as 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.

181. 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 (in particular from high risk countries) who are seeking to establish relationships.

182. 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.

4.7.6 High-Risk Countries

183. 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.

184. 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.

4.7.7 Bearer Shares

185. Bearer shares can provide a significant level of anonymity, which can be abused by those seeking to use companies for criminal intent. 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.

186. 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 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.

4.7.8 Correspondent Banking

187. 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.

188. The decision to approve a respondent relationship should depend inter alia on the financial institution's assessment of the counterpart's money laundering and terrorist financing prevention and detection systems and controls, and the quality of bank supervision and regulation in the counterpart's country.

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

190. 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.

191. 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.

192. A financial institution should obtain the following on the respondent 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 and determine from publicly available information the reputation of the respondent);

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

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

v. Assessment of the quality of bank supervision and regulation in the respondent's country, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; and

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

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

194. 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 standards of regulations, additional due diligence should be carried out.

195. 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 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.

196. 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.

197. 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.

198. 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.

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

200. 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.

201. 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.

202. 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.

203. 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 programme in place; and

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

SECTION V - ELECTRONIC PAYMENTS TRANSFERS

5.1 Wire/Funds Transfers

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

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

5.1.1 Pre-Conditions for Making Funds Transfers – Verification of Identity of Payers

205. A financial institution that initiates wire transfers on behalf of payers ("Originating financial institutions") must ensure that the payer information conveyed in the payment message or instruction is accurate and has been verified.

206. 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.

207. Before initiating one-off wire transfers on the instructions of non-account holding customers, the originating financial institution must verify the identity and address (or a permitted alternative to address) of the payer.

208. 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 money laundering or terrorist financing.

5.1.2 Cross-Border Wire Transfers – Complete Payer Information

209. Except as permitted below, complete payer information must accompany all wire transfers of BZ$2,000 or more where the beneficiary financial institution (i.e. the financial institution that receives a funds transfer on behalf of a payee) is located in a jurisdiction outside Belize. Complete payer information consists of the payer's:

i. Name;

ii. Account number, or if no account exists, a unique identifier or transaction number; and

iii. Address, or date and place of birth or national identity number, or customer identification number.

210. 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 a payer's name where, dependent upon the size of the field, it provides the name of one or more account holders.

211. 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 payer. 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 payer to the wire transfer.

212. Only the address of a payer may be substituted with the payer's date and place of birth, or national identity number or customer identification number. A national identity number may be used for payers resident in countries that issue such numbers. However, for payers 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 a payer, 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.

213. Payers 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 payee) demands the payer's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the payer's consent or under judicial compulsion should the address be additionally provided.

5.1.3 Domestic Wire Transfers – Reduced Payer Information

214. Where the originating and beneficiary financial institutions are both located within Belize, wire transfers need be accompanied only by the payer's account number or a unique identifier or a transaction number which permits the transaction to be traced back to the payer. However, if requested by the beneficiary financial institution, complete payer information must be provided by the originating financial institution within three business days of such request.

5.1.4 Batch File Transfers

215. A batch file transfer contains several individual transfers from a single payer bundled together for transmission to beneficiaries outside Belize. For batch file transfers of BZ$2,000 or more, reduced payer information requirement applies. Individual transfers within the batch need carry only the payer's account number or a unique identifier or transaction number, provided that the batch file itself contains complete payer information. In general, only routine transactions should be batched.

5.1.5 Wire Transfers via Intermediaries

216. 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 payer which accompanies a wire transfer is retained with the transfer throughout the payment chain.

5.1.6 Technical Limitations

217. It is preferable for payments to be forwarded through a system which is capable of carrying all the required information. However, where an intermediary financial institution is technically unable to transmit complete payer information, it may nevertheless use a system with technical limitations provided that:

i. If it is aware that the payer information is missing or incomplete, it must concurrently advise the beneficiary financial institution of that fact by an agreed form of communication, whether within a payment or messaging system or otherwise; and

ii. It retains records of any information received with the funds transfer for five years from receipt of the information, whether or not the information is complete. If requested to do so by the beneficiary financial institution, the intermediary financial institution must provide the payer information received with the funds transfer within three business days of receiving the request.

5.1.7 Minimum Standards

218. The above information requirements are minimum standards. A financial institution may elect to supply complete payer 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.

5.2 Record Keeping Requirements

219. A financial institution should maintain all necessary records on transactions, identification data, account files and business correspondence for all wire transfers 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.

220. The particulars of the wire transfer to be recorded must be of sufficient detail so as 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 payer (including the payer's identity verification documentation) must be retained by the originating financial institution for a period of five years from execution of the transfer.

221. 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

222. A beneficiary financial institution should adopt risk-based procedures to detect whether required information is missing from wire transfers received and to determine whether the

absence of required information should give rise to an STR being made to the FIU.

223. It is expected that payer information requirements will be met by a combination of the following:

i. SWIFT payments on which mandatory payer 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 payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system.

ii. A beneficiary financial institution should therefore subject incoming wire transfers to an appropriate level of post event random sampling to detect non-compliant payments. This sampling should be risk-based. For example:

a. The sampling could normally be restricted to payments emanating from originating financial institutions outside Belize where the complete payer information requirement applies;

b. The sampling could be weighted towards those jurisdictions deemed high risk under a financial institution's own country risk assessment;

c. The sampling could be focused more heavily on transfers from those originating financial institutions who are identified by such sampling as having previously failed to comply with the relevant information requirements;

d. Other specific measures might be considered, for example, checking at the point of payment delivery, that payer information is complete and meaningful on all transfers that are collected in cash by payees on a "pay on application and identification" basis. It should be noted that none of the above requirements obviate the obligation to report suspicious transactions.

224. If a beneficiary financial institution becomes aware in the course of processing a payment that it contains meaningless or incomplete information, it should either reject the transfer or ask for complete payer information.

225. Where an originating financial institution is identified as having regularly failed to comply with the payer 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.

226. When querying incomplete payments, financial institutions should bear in mind that some

countries may have framed their own regulations to incorporate a threshold below which the provision of complete payer information on outgoing payments is not required. However, this does not preclude a beneficiary financial institution from calling for the complete payer information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether or how far to press the point.

5.4 Exemptions

227. The following payment types are exempt:

i. Transfers where the payer withdraws cash from his or her own account;

ii. Transfers by credit or debit card so long as the payee 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 payer) accompanies all transfers;

iii. Direct debits from accounts authorized between two parties so long as a unique identifier, allowing the payment to be traced back to the payer, accompanies all transfers;

iv. Transfers to public authorities for the payment of fines, penalties, duties or other taxes within Belize; and

v. Transfers where both the payer and payee are financial institutions acting on their own behalf.

5.4.1 Card Transactions

228. 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 payer, accompanies the movement of the funds. The 16-digit Card PAN number serves this function.

229. Complete payer information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a payee's beneficiary financial institution located in Belize.

5.5 Offences and Fines

230. A financial institution that fails to comply with these provisions commits an offence and shall be liable to a fine not exceeding BZ$10,000 by the FIU, as per Section 19 of the MLTPA.

231. As per Section 19(6) of the MLTPA, a financial institution aggrieved by the decision of the FIU, as it relates to the above fine, may appeal to the Supreme Court under the provisions of Part X of the Supreme Court of Judicature Act. For this purpose, the FIU shall be deemed to be an inferior court. An appeal shall not by itself result in the suspension of the decision under appeal, but the appellant may, within the prescribed time for filing an

appeal, apply to the Supreme Court for stay of execution of the order appealed from, pending the determination of the appeal.

5.6 Reduced Customer Due Diligence

232. 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. Such circumstances include:

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

   a. An entity regulated by the Central Bank under the BFIA 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;

   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 business persons provided that they are subject to requirements to combat money laundering and terrorist financing 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.

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

234. Reduced CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

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

236. 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.

5.7 Retrospective Due Diligence

237. 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.

238. 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.

5.8 ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

239. 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.

5.8.1 Monitoring

240. 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. The purpose of this monitoring is for a financial institution to be vigilant to note any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts.

241. 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 risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity.

242. 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 on-site visits, interviews with the business' management, or closer reviews of transactional activity.

243. It is recognized that the most effective method of monitoring accounts or business relationships is achieved through a combination of computerized and human manual solutions. A corporate compliance culture and properly trained, vigilant staff through their day-to-day dealing with customers will form an effective monitoring method. Computerized approaches may include the setting of "floor levels" for monitoring by amount.

244. A financial institution should invest in computer systems specifically designed to assist the detection of money laundering and other crimes. It is recognized however that this 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.

5.8.2 "Hold Mail" Accounts

245. "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.

246. 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.

247. 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.

248. 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.

249. "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 VI – MONEY TRANSFER SERVICES PROVIDERS

250. The following guidance applies to money transfer services providers and their agents, which conduct money transmission business in Belize. Persons who wish to provide a money transfer or value transfer service must first apply for approval to receive a licence from the Central Bank. This licence must be renewed annually, subject to review of operations of agents and sub-agents to ascertain compliance with all regulations and conditions governing money transfer services requirements, including those to combat money laundering and terrorist financing.

251. At the time of the request for the annual renewal of licence, each licensed money transfer services provider should make available to the Central Bank, as Supervisory Authority, a list of their agents and sub-agents.

252. It is the responsibility of each money transfer services provider to have policies in place to prevent money laundering and terrorist financing in line with the FATF Forty Recommendations. Such policies should include provisions for:

i. Internal systems of controls, policies and procedures;

ii. CDD procedures;

iii. A risk-based framework;

iv. A records management system; and

v. Education and training of employees in recognizing and reporting suspicious transactions.

6.1 Vulnerability of Money Transfer Services Providers to Money Laundering and Terrorist Financing

253. Fleeting relationships with customers make money transfer services providers vulnerable to money laundering and the financing of terrorism. Whereas a person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, a person does not have that type of relationship with the money transfer services providers and can repeatedly use different ones to transact business. These entities are particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the world.

254. While the international remittance system is typically used to repatriate earnings, it can also be used to transmit the illegal proceeds of criminal activities and funds used to finance terrorism. The rapid movement of funds across multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer information that should accompany wire transfers to mitigate this risk.

255. Apart from money transmission, cheque cashing is another important segment of the business for some money transfer services providers. These entities should be aware that endorsed third party cheques from overseas are a money laundering risk. Even where a Belize dollar cheque, endorsed by a third party, is presented for cashing, the money transfer services provider should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large cheques originating from unknown individuals present a greater money laundering risk compared to small cheques originating from well-established businesses.

6.2 Identification Documentation

256. Proper identification documentation is required for **all** money transmissions. The requirement for specific pieces of payer information that are to accompany each wire transfer applies to money transmissions. Money transfer services providers must therefore request and obtain identification documentation for money transmissions in line with the payer information requirements as noted under the section “Electronics Payments Transfers” in these Guidelines.

257. Given the fleeting nature of the customer relationship, money transfer services providers should obtain identification information where the customer, product or geography is deemed to be high risk.

258. Customer identification information should be obtained prior to a transaction being carried out. If identification information is not obtained, the transaction should not proceed.

259. For further guidance on customer identification and record keeping requirements, money transfer services providers should refer to those particular sections in these Guidelines.

6.3 Transaction Monitoring

260. Because of the large number of customers involved and the relatively small amounts transacted, it is imperative for money transfer services providers to have adequate systems in place to collate relevant information and monitor customers' activities. In the money transfer services provider, the amount of information collected may be broadened to include details of the recipient of the funds. This information will assist money transfer services provider to determine whether there is any risk that the customer is utilizing multiple recipients to facilitate money laundering or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

6.4 Indicators of the Misuse of Money Transfer Services Providers

261. The following activity may be suspicious and indicate money laundering or other illegal activity through the misuse of money transfer services providers:

i. Transactions which do not make economic sense – these include transactions which:

   a. Are incompatible with the financial institution's knowledge and experience of the customer in question or with the purpose of the relevant business transaction;

   b. A customer or group of customers attempt to hide the size of a large cash transaction by breaking it into multiple, smaller transactions by, for example, conducting the smaller transactions at different times on the same day or with different cashiers on the same day or on different days or at different branches/offices of the same money transfer services provider.

   c. Cannot be reconciled with the usual activities of the customer;

   d. A customer sends to or receives money transfers from persons in other countries without an apparent business reason or gives a reason inconsistent with the customer's business.

   e. A customer sends to or receives money transfers from persons in other countries when the nature of the business would not normally involve international transfers.

ii. Transactions involving large amounts of cash – these include transactions in which:

   a. Frequent large cash amounts do not appear to be justified by the customer's business activity;

   b. Large and regular payments that cannot be identified as bona fide transactions, are sent to countries associated with the production, processing or marketing of narcotics or other illegal drugs;

   c. Cash payments are remitted to a single account by a large number of different persons without an adequate explanation.

iii. Other types of transactions and activity – this includes but is not limited to transactions in which:

   a. The volume and activity is not commensurate with the customer's known profile

(e.g. age, occupation and/or income);

b. Countries or entities are reported to be associated with terrorist activities or with persons that have been designated as terrorists;

c. Multiple transactions and multiple recipients, including structuring of transactions are used to avoid identification or enhanced due diligence threshold requirements;

d. A business customer is reluctant to provide complete information regarding the type of business, the purpose of the transaction or any other information requested by the money transfer services provider.

SECTION VII - UNUSUAL & SUSPICIOUS TRANSACTIONS

262. Suspicious transactions are financial transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism 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.

263. 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.

264. 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.

265. 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 competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors for at least five years.

266. A financial institution should refer to established websites for entities such as FATF, FinCEN, US Treasury, OFAC, Transparency International and other recommended websites, as highlighted in Appendix 2, for country advisories and information on countries vulnerable to corruption. This information should be regarded in conjunction with the notices forwarded by the FIU.

267. Where a country continues not to apply or insufficiently applies the FATF Recommendations, appropriate counter-measures 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 these countries;

ii. Enhanced 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 systems;

iv. Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering; and

v. Limiting business relationships or financial transactions with the identified country or persons in that country.

268. A financial institution should develop procedures to assist in the identification of 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, on a solo, consolidated and group-wide basis, transactions undertaken throughout the course of the business relationship and 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 give rise to multiple limits and/or aggregate limits on a consolidated basis.

269. A financial institution should not grant blanket reporting exemptions and should:

i. Clearly document their policy for the granting of such exemptions including the qualifying criteria for exemption, officers responsible for preparing and authorizing exemptions, the basis for establishing threshold limits, review of exempt customers and procedures for processing transactions.

ii. Maintain authorized exempt lists showing threshold limits established for each qualifying customer; and

iii. Monitor currency exchanges and international wire transfers.

270. For the purposes of these Guidelines, a transaction includes an attempted or aborted transaction.

7.1 Internal Reporting Procedures

271. 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 9 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;

ii. Develop written policies, procedures and processes to provide guidance on the reporting chain and the procedures to follow when identifying and researching unusual transactions and reporting suspicious activities. Investigation of suspicions should be prompt;

iii. 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);

iv. Require its staff to document in writing their suspicion about a transaction; and

v. Require documentation of internal enquiries.

272. 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 enquiries should be made to ascertain whether the business relationship is being used for money laundering or terrorist financing purposes. A financial institution should record the findings of their enquiries in writing.

273. Where a financial institution conducts enquiries and obtains a satisfactory explanation for the unusual transaction or pattern of transaction, 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.

274. Where a financial institution conducts enquiries 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.

275. 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 Money Laundering Reporting Officer (MLRO) so that an informed overview of the situation can be maintained.

7.2 External Reporting

276. The national reception point for disclosure of STRs is the FIU. Reports should be in the format determined by the FIU (**See Appendix 10**). 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.

277. 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.

278. 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 money laundering or terrorist financing offence, terrorist act or suspected to be the proceeds of crime.

279. As per Section 76 (6) of the MLTPA the FIU may direct financial institutions to freeze funds and other financial assets or economic resources of any person, to comply or give effect to a resolution of the Security Council of the United Nations adopted under Chapter VII of the United Nations Charter, provided that if the Security Council takes a subsequent decision which has the effect of postponing, suspending or canceling the operation of such resolution (wholly or partly), any order by the FIU pursuant to that resolution shall cease to have effect or shall be postponed or suspended in whole or in part, in accordance with that decision, as the case may be. "The UN list of persons connected to terrorism may be accessed at www.un.org[5].

280. 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.

281. 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 was 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.

282. 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.

[5] http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm

283. 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 - COMPLIANCE AND AUDIT

284. 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 money laundering or terrorist financing. 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 of this officer as per Section 18(3) of the MLTPA.

285. A financial institution may also appoint a MLRO to supervise the Compliance Officer.

286. All financial institutions should designate a suitably qualified person with the appropriate level of authority, seniority and independence as Compliance Officer. The Compliance Officer should be independent of the receipt, transfer or payment of funds or management of customer assets and should have timely and uninhibited access to customer identification, transaction records and other relevant information. The powers and reporting structure of the officer should be conducive to the effective and independent exercise of duties.

287. 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.

288. All financial institutions are required to notify the Central Bank of the name of the Compliance Officer and MLRO. This notification should include a statement that the Compliance Officer and MLRO are fit and proper persons;

289. A financial institution is to notify the Central Bank where there are any changes to the designations of the Compliance Officer and/or Money Laundering Reporting Officer;

290. The Compliance Officer should:

i. Undertake responsibility for developing compliance policies;

ii. Develop a programme to communicate policies and procedures within the entity;

iii. Monitor compliance by staff with the financial institution's internal AML programme and any relevant law relating to AML/CFT;

iv. 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 money laundering or terrorist financing;

v. 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);

vi. Monitor the accounts of persons for whom a suspicious report has been made;

vii. Establish and maintain on-going awareness and training programmes for staff at all levels and establish standards for the frequency and means of training;

viii. 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 money laundering and the financing of terrorism;

ix. Review compliance policies and procedures to reflect changes in legislation or international developments;

x. Participate in the approval process for high-risk business lines and new products, including those involving new technologies; and

xi. Act as liaison and be available to discuss with the Bank or the FIU matters pertaining to the AML/CFT function.

291. The internal audit department should carry out reviews to test and evaluate how effectively compliance policies 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.

292. 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 discharged.

293. 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 Group Internal Audit may perform the internal audit services. Where this is not possible, a financial institution may, subject to the Bank'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 issues.

294. The MLRO and Compliance Officer are expected to act honestly and reasonably and to make determinations in good faith.

SECTION IX - RECORD-KEEPING

295. 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.

9.1 Transaction Records

296. 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.

297. 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 on-going investigation relating to a transaction or client.

298. 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.

9.2 Verification of Identity Records

299. 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.

300. 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.

301. 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 later.

302. 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.

303. 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.

304. 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.

305. 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.

306. 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.

307. 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.

308. 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:

9.3 Customer Records

309. In order to comply with Section 16 (1) of the MLTPA, a financial institution should retain:

i. Copies or records of customer identification, including those obtained through the conduct of enhanced due diligence;

ii. Account files, account statements and business correspondence; and

iii. All business transaction records.

9.4 Internal and External Records

310. A financial institution should maintain records related to unusual and suspicious transaction reports. 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.

9.5 Training Records

311. In order to provide evidence of compliance with Section 4(1) (b) and (c) of the MLP Regulations, at a minimum, a financial institution should maintain the following information:

i. Details and contents of the training programme 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 money laundering and terrorist financing requirements; and

v. An ongoing training plan.

SECTION X – EDUCATION AND TRAINING

312. An integral element of the fight against money laundering and the financing of terrorism 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 programmes.

313. The effectiveness of the procedures and recommendations contained in these Guidelines depend on the extent to which staff of financial institutions appreciates 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.

314. 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 issues and ensuring compliance with policy and procedures.

10.1 Content and Scope of the Training Programme

315. A financial institution's overall training programme should cover topics pertinent to its operations. It should provide to the relevant employees training on the recognition and handling of transactions carried out by persons who may be engaged in money laundering or terrorist financing. 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 may change. The timing of training programmes should also be based on need and should be conducted accordingly, but not less than once per annum.

316. Training programmes should, inter alia, incorporate references to:

i. Relevant money laundering and terrorism financing 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 importance of adhering to CDD policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;

v. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;

vi. The completion of unusual and suspicious transaction reports;

vii. Treatment of incomplete or declined transactions; and

viii. The procedures to follow when working with law enforcement or the FIU on an investigation.

317. A financial institution should therefore:

i. Develop an appropriately tailored training and awareness programme consistent with its size, resources and type of operation to enable its employees to be aware of their responsibilities, the risks associated with money laundering and terrorist financing, to understand how the institution might be used for such activities, to recognize and handle suspicious transactions and potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;

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 customer due diligence 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 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;

vi. Obtain an acknowledgement from each staff member on the training received;

vii. 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;

viii. Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies to detect and deter money laundering and to counter the financing of terrorism. 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 programmes.

ix. Make arrangements for refresher training, at least annually, to remind employees of their responsibilities and to make them aware of any new developments in money laundering and anti-terrorism 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 money laundering and terrorist financing, 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 and their efforts are therefore vital to the organization's reporting system for such transactions. 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 business 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 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 suspicious transaction reports;

e. **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 on-going training on the validation, investigation and reporting of suspicious transactions and feedback arrangements and on new trends and patterns of criminal activity.

SECTION XI - PRE-EMPLOYMENT BACKGROUND SCREENING

318. The ability to implement an effective AML/CFT programme depends in part on the quality and integrity of staff, as an insider can pose the same money laundering 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 over a period of 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.

SECTION XII - 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. In defining the term financial institution, Section 2 (1) of the MLTPA makes a circular reference to the 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 First 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;

ii. Banking business defined under the BFIA 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 BFIA 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.

NON-PROFIT ORGANIZATIONS

For a list of all IRS recognized non-profit organizations 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 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 $10,000 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 from $5,000 minimum to $20,000 maximum; 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 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 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 of $20,000 minimum to $50,000 maximum.	Section 33(1) 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[6] or any other 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.	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

6 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 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.

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 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 commission of or conspiring to commit terrorism.	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 7 MLTPA
	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. birth certificate);
- 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 enquiries 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 or attorney-at-law.

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, Driver's license along with a social security card or passport)
- 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 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 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

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 money laundering and terrorist financing 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 9

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 AUTHORISING OFFICER

(Signature & Title) (Signature & Title)

Appendix 10

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.