CENTRAL BANK OF
TRINIDAD & TOBAGO

GUIDELINE ON
ANTI-MONEY LAUNDERING AND THE COMBATING OF TERRORIST FINANCING

October 2011

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The revised Guideline on Anti-Money Laundering (AML) and the Combating of the Terrorist Financing (CTF) (the Guideline) seeks to provide institutions regulated by the Central Bank of Trinidad and Tobago (the Central Bank) with guidance as to what is required to implement adequate AML/ CTF compliance frameworks within their institutions. This Guideline therefore replaces the Central Bank's 2005 Guideline on AML/ CTF.

1.2 The global threat of money laundering and the financing of terrorism have led financial sector regulators and financial institutions to strengthen their vigilance in support of the efforts of governments to more easily detect attempts to launder money and finance terrorism and to minimise the possibility that their jurisdictions or institutions become involved in such activities. Effective enforcement of policies to deter money laundering and the financing of terrorism should, *inter alia*, enhance the integrity of the financial system and reduce incentives for the commission of crime within a jurisdiction.

1.3 Financial institutions are attractive conduits for money launderers and persons wishing to finance terrorism since the services offered can be easily utilised to conceal the true origin of money. It is the duty of each financial institution to ensure that preventative measures are in place to deter such activity.

1.4 Money laundering (ML) and terrorist financing (TF) prevention should not be viewed in isolation from an institution's other business systems and needs, but as part of the institution's overall risk management strategies. Consequently, it is imperative that the board and senior management of financial institutions ensure that the policies, procedures, systems and processes that are put in place to prevent ML and TF are risk-based and commensurate with the size, complexity and risks of their financial institution.

2. PURPOSE OF THE GUIDELINE

2.1 The objective of this Guideline is to assist financial institutions with the following:-

a) complying with legislative and regulatory requirements contained in the following AML/ CTF laws:-

i. Proceeds of Crime Act Chap 11:27 (POCA),

ii. The Financial Obligations Regulations 2010 (FOR),

iii. The Anti-Terrorism Act Chap 12:07 (ATA);

iv. The Financial Obligations (Financing of Terrorism) Regulations, 2011 (The Financing of Terrorism Regulations);

v. The Financial Intelligence Unit of Trinidad and Tobago Act 2009 as amended in 2011 (FIUTTA); and

vi. The Financial Intelligence Unit Regulations, 2011 (The FIU Regulations);

b) implementing effective procedures and controls to manage AML/ CTF risks; and

c) establishing adequate AML/ CTF compliance programmes.

2.2 It is critical that financial institutions implement effective controls for ML and TF risks. A financial institution's compliance programme, in addition to meeting statutory criteria, should be adapted to reflect the nature, scope, complexity and risk profile of the institution. Financial institutions are therefore expected to consider the contents of this Guideline when implementing their AML/CTF programmes.

2.3 This Guideline therefore sets out the expectations of the Central Bank in relation to the minimum standards for AML/ CTF practices by all financial institutions and, together with the POCA, FOR and ATA, will form an integral part of the framework used by the Central Bank in assessing the adequacy and effectiveness of the implementation of institutional AML/CTF frameworks.

3. MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1 Money Laundering

3.1.1 Money laundering is the process by which the direct or indirect benefits of crime are channeled through financial institutions to conceal the true origin and ownership of the proceeds of criminal activities. If successfully undertaken, it allows them to maintain control over those proceeds but the money can lose its criminal identity and appear to be legitimately derived.

3.1.2 The ability to launder the proceeds of criminal activity through the financial system is vital to the success of criminal operations. If they are to benefit from the proceeds of their activities, those involved need to exploit the facilities of the world's financial institutions. The increased integration of the world's financial systems and the removal of barriers to the free movement of capital, have enhanced the ease with which proceeds of crime can be laundered and have complicated the tracing process.

3.1.3 There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. cars or jewellery) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, in the case of drug trafficking and other specified offences enforceable under POCA[1], the proceeds usually take the form of cash which needs to enter the financial system.

1 Specified offences are defined in POCA.

3.2 Stages of Money Laundering

3.2.1 Despite the variety of methods employed, money laundering is generally accomplished in three stages, which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. These stages are placement, layering and integration:-

a) **Placement**: refers to the placing of "dirty money" or unlawful cash proceeds into the financial system without arousing suspicion for example via deposits, purchases of cheques or money orders.

b) **Layering**: refers to the movement of the money, often in a series of complex transactions crossing multiple jurisdictions designed to disguise the audit trail and provide the appearance of legitimacy. These transactions may include purchasing investment instruments, insurance contracts, wire transfers, money orders and letters of credit.

c) **Integration**: refers to the attempt to legitimize wealth derived from criminal activity. The illicit funds re-enter the legitimate economy by way of investment in real estate, luxury assets and business ventures, until the laundered funds are eventually disbursed back to the criminal.

3.2.2 Efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have, therefore, to a large extent concentrated on the deposit taking procedures of financial institutions, i.e., the placement stage. However, there are many crimes where cash is not involved. *Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their AML procedures with due regard to that risk.*

3.2.3 The most common form of money laundering that a financial institution will encounter on a daily basis, in respect of their mainstream banking business, takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value. Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions. Additionally, financial institutions as providers of a wide range of services are susceptible to being used in the layering and integration stages of money laundering. Mortgage and other loan accounts may be used as part of this process to create complex layers of transactions. *A financial institution's AML programme should seek to ensure that appropriate methods exist for identifying and reporting money laundering at each of the three stages.*

3.3 Terrorist Financing

3.3.1 Terrorism is the unlawful threat of action designed to compel the government or an international organization or intimidate the public or a section of the public for the purpose of advancing a political,

religious or ideological belief or cause. These actions include violence against a person, endangering a person's life, damage to property, threats to national security or public health and safety, or serious interference with or disruption to an electronic system. In contrast, financial gain is the main objective of financial crimes like money laundering. Nonetheless, terrorists[2] and terrorist organisations[3], must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts[4].

3.3.2 Terrorist financing may involve amounts that are not always large, and the associated transactions may not necessarily be complex. However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organization in laundering the funds. Where the funds are derived from legitimate sources, terrorist organisations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organisation and the funds.

3.3.3 Some of the particular methods detected with respect to various terrorist groups include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers.

3.3.4 A financial institution can be guilty of aiding terrorist financing if it carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used for, terrorist activity. An institution may be guilty of aiding terrorist financing whether the assets involved in the transaction are proceeds of criminal activity or are derived from lawful activity but intended for use in support of terrorism.

3.3.5 Generally, it is difficult for financial institutions to detect terrorist financing. Indeed, the only time that financial institutions might clearly identify terrorist financing as distinct from other criminal misuse of the financial system is when a known terrorist or terrorist organisation has opened an account. Financial institutions are however, in a position to detect suspicious transactions that, if reported, may later prove to be related to terrorist financing. *For this reason, financial institutions do not need to determine the legality of the source or destination of funds but should ascertain whether transactions are unusual or suspicious* or otherwise indicative of criminal or terrorist activity[5]. It is the competent enforcement authority or the financial intelligence unit (FIU) then that is in a position to determine whether the transaction relates to a particular type of criminal or terrorist activity and decide on a course of action.

2 Refer to Anti-Terrorism (Amendment) Act #2 of 2010 section 5(e)
3 Refer to Anti-Terrrorism (Amendment) Act, # 2 of 2010 section 5(e)
4 Refer to Anti-Terrrorism (Amendment) Act, #2 of 2010 section 5(d)
5 Refer to FATF Guidance for Financial Institutions on Detecting Terrorist Financing.

For this reason, financial institutions do not necessarily need to determine the legality of the source or destination of the funds.

Sources of Terrorist Financing

3.3.6 Terrorist financing usually comes for two primary sources. The first source is the financial support provided by States or organizations with large enough infrastructures to collect and make funds available to the terrorist organization. This so-called State-sponsored terrorism has declined, and has been replaced by other types of funding. An individual with sufficient financial means may also provide substantial funding to terrorist groups, e.g. Osama bin Laden is thought to have contributed significant amounts of his personal wealth to the Al-Qaeda terrorist network.

3.3.7 The second major source of funding for terrorism may come from "revenue generating" criminal activities like kidnapping or extortion. However, terrorist groups may engage in large-scale smuggling, various types of fraud (e.g. through credit cards or charities), thefts and robberies, and narcotics trafficking.

3.3.8 Unlike money laundering, funding for terrorist groups may come from legitimate sources. This funding from legal sources is a key difference between terrorist groups and traditional criminal organisations. For example, community solicitation and fundraising appeals are one very effective means of raising funds to support terrorism. Oftentimes, such fundraising is carried out in the name of organizations having the status of a charitable or relief organization and in many cases, the charities to which donations are given are in fact legitimate in that they do engage in the work they purport to carry out. Most of the members of the organization however, have no knowledge that a portion of the funds raised by the charity is being diverted to terrorist causes.

4. APPLICABILITY OF THE GUIDELINE

4.1 This Guideline applies to:-

a) Financial institutions licensed under the Financial Institutions Act, 2008 (the FIA) to carry on the "business of banking" or "business of a financial nature";

b) Insurance companies and intermediaries (e.g. salesmen, agents and brokers) registered under the Insurance Act Chapter 84:01 (the IA) to carry on the business of insurance;

c) Authorized dealers (i.e. cambios and bureaus de change) registered under the Exchange Control Act; and

d) Companies engaged in money transmission or remittance business under the Central Bank Act Chapter 79:02. This would also include agents of money remitters.

4.2 Hereinafter in this Guideline, these institutions will be collectively referred to as financial institutions. Appendices to this Guideline deal with special issues that should be considered by each category of financial institution considered in 4.1.

4.3 With respect to 4.1 (b), the Central Bank expects insurance companies to extend their AML/ CTF compliance programmes to their salesmen and agents. Brokers on the other hand as introducers of business to insurance companies must implement their own AML/ CTF compliance programmes.

4.4 Financial institutions should ensure that, at a minimum, this Guideline is also implemented in their branches and subsidiaries abroad. Where the local applicable laws and regulations prohibit the implementation of this Guideline, the Central Bank must be notified.

4.4.1 Financial institutions are required to assess the AML/ CTF regime existing in any jurisdiction in which its branches and/or subsidiaries operate. Where the branch operates in an overseas jurisdiction and the AML/ CTF laws and requirements in that jurisdiction exceed the standards required by Trinidad and Tobago laws, the branch should adhere to the requirements in the overseas jurisdiction.

4.4.2 Where the Trinidad and Tobago AML/CTF requirements exceed those in the host jurisdiction, subsidiaries and branches of the financial institution in those jurisdications should apply the higher standard to the extent that the host jurisdiction laws and regulations permit.

4.4.3 Financial institutions with non-deposit-taking subsidiaries, must take steps to ensure that there is access to information regarding the operations, and activities of these subsidiaries in order to ensure that such subsidiaries are compliant with the AML/CTF laws, regulations, and guidelines. Both 4.4.2 and 4.4.3 should form part of the group risk management strategy.

5. THE LEGISLATIVE AND REGULATORY FRAMEWORK

5.1 Section 2.1(a) of this Guideline names the relevant AML/ CTF legislation that applies to all regulated financial institutions. The general obligations created under the specific legislation are as follows:-

5.1.1 The **POCA** requires financial institutions to:-

a) document, establish and maintain a compliance programme;

b) appoint a Compliance Officer;

c) pay attention to and report if suspicious, business transactions which are large, unusual, complex as well as transactions which have no apparent economic or visible lawful purpose those undertaken with persons and transactions with financial institutions in or from other countries which do not or insufficiently comply with the recommendations of the Financial Action Task Force;

d) report all complex, unusual or large transactions which have no apparent economic or visible lawful purpose to the Finance Intelligence Unit of Trinidad and Tobago (the FIU); and

e) make a suspicious transactions or a suspicious activity report to the FIU.

5.1.2 The **FOR** was made pursuant to section 56 of POCA and contains *inter alia* statutory obligations relating to the Compliance Officer, compliance programme, identification of customers, trusts, record keeping, training, anonymous accounts, shell banks, politically exposed persons, correspondent banking and wire transfers.

In addition, the FOR specifically names the Central Bank as the Supervisory Authority[6] for the financial institutions that it regulates and allows the Central Bank to take regulatory measures prescribed in the legislation governing particular financial institutions to ensure compliance with AML/CTF requirements. The regulatory measures which may be takesn are the enforcement actions allowed in the legislation governing particular financial institutions including the FIA and IA.

5.1.3 The **ATA** criminalizes terrorism and provides for the detection, prosecution, conviction and punishment of terrorist activities and the confiscation, forfeiture and seizure of terrorists' assets. It introduced a quarterly reporting regime as regards possession or control of terrorist property as well as a suspicious transaction reporting where there are reasonable grounds to suspect that a transaction is related to the commission of a terrorist act.

5.1.4 The **FIUTTA** establishes the Financial Intelligence Unit of Trinidad and Tobago, for the implementation of the anti-money laundering policies of the Financial Action Task Force. It also *inter alia* requires a financial institution to follow the Guidelines issued by the Central Bank in determining what is a suspicious transaction or suspicious activity. Further, a financial institution may seek the approval of the FIU to complete a suspicious transaction where:-

a) a transaction or activity appears to be suspicious; or

b) a suspicious transaction or suspicious activity report has been submitted in respect of a customer or another person, who attempts a subsequent transaction.

6 Other named Supervisory Authorities are the Trinidad and Tobago Securities and Exchange Commission (TTSEC) for securities businesses and the Financial Intelligence Unit (FIU) for listed businesses and other financial institutions not regulated by the Central Bank or the TTSEC.

The procedures to be followed where such circumstances arise will be detailed by the FIU.

5.1.5 The **FIU Regulations** were made by the Minister of Finance pursuant to section 27 of the FIUTTA and stipulates *among other things*, the manner in which:-

a) the SAR is to be submitted to the FIU;

b) the FIU may request financial information from a financial institution or listed business;

c) the FIU is to store financial information received from financial institutions or listed businesses; and

d) the FIU may disseminate and share information with other local and foreign authorities.

5.1.6 The **Financing of Terrorism Regulations** were made by the Minister of National Security under section 41 of the Anti-Terrorism Act. The Regulations seeks to extend the obligations imposed on financial institutions and listed business under the FOR to terrorist financing as well.

6. THE ROLE OF THE CENTRAL BANK AS SUPERVISORY AUTHORITY

6.1 The FOR has named the Central Bank as the Supervisory Authority for those financial institutions (or persons) over which it is the primary Regulator. The primary responsibilities of the Central Bank as a Supervisory Authority include:-

a) reviewing the compliance programme of all financial institutions during on-site examinations to determine its adequacy and assess its compliance with applicable laws and guidelines;

b) approving the compliance officer as fit and proper;

c) issuing guidelines as appropriate to aid compliance with AML/ CTF requirements;

d) receiving an external audit report from the financial institution's auditors on an annual basis that evaluates the adequacy of the financial institution's compliance programme in accordance with relevant laws and guidelines;

e) taking regulatory action against those institutions and persons regulated by it which fail to adequately comply with statutory AML/ CTF statutory obligations and Guidelines issued by the Central Bank; and

f) sharing information with the FIU as required for the purposes of AML/ CTF. This includes disclosing information to the FIU as soon as is reasonably practicable where it has knowledge or has reasonable grounds for believing that a financial institution may have been engaged in money laundering[7] or terrorist financing.

7 Refer to the FOR Regulation 41 (1).

6.2 The type of regulatory action taken by the Central Bank will depend on the institution's level of non-compliance with AML/ CTF statutory obligations and Guidelines issued by the Central Bank and the potential risk to the institution's operations. Regulatory actions that could be taken by the Central Bank include the issue of warning letters, compliance directions or other injunctive or equitable relief, restriction of activities and revocation of a licence.

7. DEVELOPING A RISK BASED FRAMEWORK

7.1 The Financial Action Task Force ("FATF"), in its revised Forty plus Nine Special (40 + 9) Recommendations on AML/ CTF, recommended that financial institutions adopt a *risk based approach* to customer due diligence. Such an approach would provide financial institutions with the discretion to determine the appropriate level of information and documentation required to verify customer identity based on the nature and degree of risk inherent in the customer relationship.

7.2 Each financial institution should develop and implement a risk rating framework appropriate for the type of products offered by the institution, and capable of assessing the level of potential risk each client relationship poses to the institution. As part of the on-going onsite examination program, the Central Bank will assess the adequacy of the institution's risk rating policies, processes and procedures, in light of the type of business conducted, as well as the extent of compliance with legislative requirements.

7.3 The risk rating framework should include:

a) Segregation of client relationships by risk categories (such as high, moderate or low);

b) 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 and volume of transactions, type of transactions, cash transactions, adherence to client activity profile);

c) The know your customer (KYC) documentation and due diligence information requirements appropriate for each risk category and risk factor; and

d) A process for the approval of the downgrading/ upgrading of risk ratings.

7.4 The risk rating framework should provide for the periodic review of the customer relationship to allow the institution to determine whether any adjustment should be made to the risk rating. The review of the risk rating for high risk customers must be undertaken more frequently than for other customers, and where appropriate, a determination should be made by senior management as to whether the relationship should be discontinued. All decisions regarding discontinuation of business with high risk customers should be documented.

7.5 The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason(s) for such change. In determining the risk profile of any customer, institutions should take into account the following risk criteria:

a) the geographical origin of the customer;

b) the geographical sphere of the customer's business activities including the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with certain high risk jurisdictions, or those known to the institution to lack proper standards in the prevention of money laundering, countering the financing of terrorism or in the customer due diligence process;

c) the nature of the customer's business, which may be particularly susceptible to money laundering or terrorist financing risk, such as casinos that handle large amounts of cash;

d) the nature and frequency of activity. This should include the pattern of account activity given the institution's information on the customer;

e) the type of customer, i.e. whether a trust or politically exposed persons ("PEPs");

f) the type, value and complexity of the facility;

g) the unwillingness of the customer to cooperate with the institution's customer due diligence process for no apparent reason;

h) for a corporate customer, an unduly complex structure of ownership for no apparent reason;

i) whether there is any form of delegated authority in place (e.g. power of attorney);

j) the product or service used by the customer;

k) situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered;

l) whether an account/business relationship is dormant; and

m) any other information that raises suspicion of the customer being connected to money laundering or terrorist financing.

8. KEY ELEMENTS OF A COMPLIANCE PROGRAMME

8.1 Financial institutions have a statutory obligation to implement robust compliance programmes to prevent money laundering and terrorist financing. The minimum elements of a compliance programme are outlined in Regulation 7(1) (a) to (h) of the FOR and include the development of policies, procedures and control to allow for *inter alia* proper customer identification and verification, filing of suspicious activity reports (SARs), internal and external audit, record keeping, and training.

8.2 Financial institutions' compliance programmes must be risk-based and appropriate for the size, complexity and risk of the institution. This means that it is expected that where possible financial institutions will consider, adopt and adapt the requirements to appropriately reflect the AML/CTF vulnerabilities identified by the institutions in terms of its clients, products, markets etc.

9. CUSTOMER DUE DILIGENCE AND IDENTIFICATION PROCEDURES

9.1 Regulation 11(1) of the FOR outlines the circumstances under which a financial institution should conduct customer due diligence (CDD) including the verification of customer identity. Such instances include:-

a) when establishing a business relationship;

b) for one-off transactions or occasional transactions of value TT$90,000 or more;

c) for two or more one-off transactions which together total TT$90,000 or more and which appear to be linked;

d) for one-off wire transfers of TT$6,000 or more; and

e) for two or more one-off wire transfers which appear linked and which in total amount to TT$6,000 or more.

9.2 Notwithstanding the thresholds established in law, financial institutions may establish lower reporting thresholds that are commensurate with the size of transactions that are typically conducted at the institution.

9.3 The verification of the source of funds is not normally required in the case of:

a) a one- off transaction or occasional transaction of less than TT$90,000, or TT$6,000[8] in the case of a one-off wire transfer;

b) two or more one-off transactions which appear to be linked but which together total less than TT$90,000; or

c) two or more one-off wire transfers which appear linked but which total less than TT$6,000.

Irrespective of the size of the transaction however, any suspicions of money laundering or terrorist financing must be reported to the FIU.

9.4 Financial institutions should assess the potential risk inherent in each new client relationship prior to establishing a business relationship. This assessment should take account of whether and to what extent a customer may expose the institution to risk, and of the product or facility to be used by the customer. Based

8 A money remittance company which typically engages in wire transfer will be expected to use the TT$6,000 threshold or such lower threshold as the company has established based on the usual value of business transactions conducted.

on this assessment, the institution should decide whether or not to establish, or continue, a relationship with the customer.

9.5 Prior to establishing a business relationship, the onus is on the financial institution to verify the customer's identity. The customer's physical identity should be verified using at least one form of picture identification[9], which may be a valid passport, national identification card or driver's license. Additional picture identification may be requested by the financial institution as part of its enhanced due diligence efforts.

9.5.1 When commencing a business relationship, institutions 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 required will depend on the applicant and the nature of the applicant's business. Documentation confirming the nature of the applicant's business (e.g. audited financial statements) or the applicant's occupation (e.g. job letter or last pay slip) should also include the origin or source of funds to be used during the relationship.

9.5.2 Once a business relationship has been established, reasonable steps should be taken by the institution to ensure that due diligence information is kept up to date. For example, financial institutions should update customer records as appropriate or at least upon occurrence of a material change to the business relationship (e.g. change of employment, marital status, address etc.). In addition, it is recommended that records for high risk customers are updated at least annually.

9.5.3. When considering whether to enter into a business relationship, reasonable measures 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, in the case of a representative applicant, trustee or nominee.

9.5.4 Where a prospective client fails or is unable to provide adequate evidence of identity or in circumstances in which the institution is not satisfied that the transaction for which it is or may be involved is legitimate, an explanation should be sought and a decision made by the Compliance Officer as to whether:-

a) it is appropriate to proceed with the business relationship; or

b) the other measures that should be taken to verify the client's identity; and

c) whether or not a report to the FIU should be made.

9.5.5 The identification requirements for establishing a relationship with an individual or a business client are outlined in Regulations 15 and 16, respectively of the FOR.

9 Refer to the FOR, Regulation 15(2).

9.6 Financial institutions are also prohibited from opening anonymous accounts or accounts in fictitious names[10]. Where a financial institution is unable to verify the true identify of a prospective client or beneficial owner, the financial institution is prohibited from establishing the business relationship, or if already established must immediately terminate the business relationship.

9.7 Customer Due Diligence (CDD) for Insurance Companies

9.7.1 An insurance company shall pay particular attention to the CDD provisions contained in Part IV of the FOR and streamline its compliance programme to ensure compliance with that Part. Appendix II also provides guidance to insurers as to what may constitute a suspicious transaction or activity in respect of insurance business. It also provides guidance on high risk and low risk insurance products.

10. VERIFICATION OF CUSTOMER IDENTITY

A financial institution must implement adequate policies and procedures to verify the identity of an individual or business customer in accordance with Regulations 15, 16, 18 and 19 of the FOR.

10.1 Individual Customers

For an individual customer, the financial institution should consider obtaining and verifying the permanent address of a prospective customer by either: -

a) checking the Register of Electors;

b) requesting a recent utility bill, tax assessment or bank statement[11] containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);

c) checking the telephone directory; or

d) conducting a home visit.

The information obtained should demonstrate that a person of that name exists at the address given, and that the account holder is that person. Where the utility bill is not in the client's name, the financial institution should request additional information to confirm the customer's address such as obtaining a letter from the landlord or a copy of the lease agreement and a recent receipt.

10 Refer to the FOR, Regulation19(1).

11 This assumes that the bank has undertaken the necessary due diligence to confirm the customer's identity. Where the financial institution is in doubt, the financial institution should request other evidence of proof of identity.

Both residence and nationality should be established to ensure that the account holder is not from a high risk country or jurisdiction 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.

Identification documents, either originals or certified copies, should be pre-signed and bear a discernable photograph of the applicant. Where prospective customers provide documents with which an institution is unfamiliar, either because of origin, format or language, the 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. In addition, where original documents are not available, the financial institution should only accept copies of documents that have been appropriately certified.

Where a financial institution has obtained identification records of the customer, enhanced due diligence is required if:-

a) during the course of the business relationship the institution has reason to doubt the identity of the customer; and

b) there is a material change in the way a relationship is operated.

With regards to b), examples of a material change include:

a) a significant transaction (relative to a relationship);

b) a transaction which is inconsistent with previous activity;

c) a new product or account being established within an existing relationship;

d) a change in an existing relationship which increases a risk profile; and

e) the assignment or transfer of ownership of any product or account.

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 among 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.

In the case of students or other young people, the financial institution may consider verification using the home address of parent(s), or by making enquiries of the applicant's school or university.

Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

Institutions should consider taking appropriate steps to verify the name and address of applicants by one or more methods, e.g.:

a) obtaining a reference from a "respected professional[12]" who knows the applicant;

b) checking a local telephone directory;

c) requesting sight of an original, recent land and building tax assessment, inland revenue statement, utility bill, bank or credit union statement; or

d) visiting the home of the applicant where possible.

Where a proposed account holder's address is temporary accommodation, for example an expatriate on a short term overseas contract, institutions should adopt flexible procedures to obtain verification under other categories, such as copy of contract of employment, or banker's or employer's written confirmation.

10.1.1 Certification of Identification Documents

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

In the case of natural persons, face-to-face customers must, where possible, produce original documents bearing a photograph, and copies should be taken, retained and certified by the staff member. The staff member must endorse the copies and note that the original document had been seen.

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[13] as being a true copy of the original document and that the photo is a true likeness of the account holder.

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

12 For example lawyers, accountants, teachers, directors or managers of a regulated institution, the police above the rank of sergeant, and ministers of religion or doctors.

13 A certifier must be a suitable person. Examples of a suitable certifier include a justice of the peace, notary public, police officer above the rank of sergeant and commissioner of affidavits.

10.2 Corporate or Business Customers

For corporate or business customers, the financial institution shall apply the requirements in Regulations 15 and 16 of the FOR with appropriate adaptation. The information obtained from the corporate entity should facilitate the identification of:-

a) The correct name of the corporate entity;

b) The address of its principal place of business and registered office;

c) The mailing address;

d) Telephone contact and fax numbers;

e) A description of the type and nature of business including the date of commencement of the business and the products and services offered; and

f) Purpose of the account, source of funds and the estimated account activity, including an indication of the expected transaction volume of the account and balance ranges in the case of current and deposit accounts.

10.2.1 Companies may sometimes form part of complex organisational structures which also involve trusts and foundations. Consequently, the legal existence of the corporate entity should be verified and the financial institution should ensure that any person purporting to act on behalf of the corporate entity is authorized to do so. The financial institution should 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. As such the following information should be requested:-

a) The beneficial owners[14] of the entity. However, if the company is publicly listed on a recognised stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required; and

b) The directors and officers who exercise effective control over the business and are in a position to override internal procedures/ control mechanisms and, in the case of bank accounts, the signatories to the account.

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

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

14 Refer to the FOR Regulation 12 (5) – A beneficial owner is the person who ultimately owns and controls an account, or who exercises ultimate control over a legal person or legal arrangement and "legal arrangement" includes an express trust.

10.2.2 Financial institutions should make enquiries to confirm that the company exists for a legitimate trading or economic purpose, for example, where appropriate visit the business/company to ensure that there is an actual physical presence. If there are any 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.

10.2.3 In addition, the institution may obtain any other information deemed appropriate. For example, an institution may also request the financial statements of parent or affiliate companies, or seek evidence that the entity is not in the process of being dissolved or wound-up. It should request this information, particularly for non-resident companies, where the corporate customer has no known track record or it relies on established affiliates for funding.

10.3 Powers Of Attorney

Regarding 10.2.1 (c) above, the authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates must be verified.

10.4 Partnership/Unincorporated Business

In the case of a partnership, each partner should be identified as well as the immediate family members with ownership control. In addition to providing the identification documentation for partners/controllers and authorised signatories, where a formal partnership arrangement exists, there should be a mandate from the partnership authorising the opening of an account. Evidence of the trading address of the business or partnership should also be obtained and a copy of the latest report and accounts (audited where applicable). An explanation of the nature of the business or partnership should be ascertained to ensure that it has a legitimate purpose.

11. ONGOING DUE DILIGENCE

11.1 Financial institutions are expected to have systems and controls in place to monitor on an ongoing basis the relevant 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 ongoing due diligence and the continuous review and monitoring of transactions. This will generally mean more frequent or intensive monitoring. The purpose of this monitoring is for financial institutions to be vigilant for any significant changes or inconsistencies in the pattern of transactions and to maintain up to date records[15]. Inconsistency is

15 Refer to the FOR Regulation 12.

measured against the stated original purpose of the accounts. Financial institutions should consider monitoring by: -

a) transaction type;

b) frequency;

c) amount;

d) geographical origin/ destination;

e) account signatories.

11.2 An effective monitoring regime comprises a corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers. The most effective method for the monitoring of accounts is achieved through a combination of computerised and human manual solutions. Computerised approaches may include the setting of “floor levels" for monitoring by amount. Whilst some financial institutions may wish to invest in expert computer systems specifically designed to assist with the detection of fraud and money laundering, it is recognized that this may not be a practical option for many financial institutions because of cost, the nature of their business, or difficulties of systems integration, in such circumstances institutions will need to ensure they have alternative systems in place.

11.3 Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity or adequacy of that information, such as. when a document evidencing identification expires.

12. ENHANCED DUE DILIGENCE

12.1 Financial institutions should apply enhanced CDD measures on a risk sensitive basis for such categories of customer, business relations or transactions as the financial institution may assess to present a higher risk for money laundering or terrorist financing. As a part of this, a financial institution may conclude, under its risk based approach, 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. As a result, the standard evidence of identity is insufficient in relation to the ML or TF risk, and that it must obtain additional information about a particular customer. The extent of additional information sought, and of any monitoring carried out in respect of any particular customer, or class/category of customer, will depend on the ML or TF risk that the customer, or class/category of customer, is assessed to present to the financial institution.

12.2 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. A fuller set of

information should be retained in respect of those customers, or class/category of customers, assessed as carrying a higher ML or TF risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes. 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.

12.3 High Risk Customers

12.3.1 High-risk customers should be approved by senior management and stringent documentation, verification and transaction monitoring procedures should be established. High risk customers should be subject to enhanced due diligence which should be undertaken at greater frequency than that applied for low risk customers. Enhanced due diligence should consider:-

a) an evaluation of the principals;

b) a review of current financial statements;

c) verification of the source of funds;

d) verification of source of wealth;

e) the conduct of reference checks; and

f) checks of electronic databases.

12.3.2 Examples of high risk customers that require enhanced due diligence include trust accounts, foundations, executorships accounts, non-profit organizations (NPOs), non face to face customers, introduced business, companies within a conglomerate, professional service providers, private banking customers and politically exposed persons (PEPs).

12.3.2 (i.) Trust accounts

Legal structures such as trusts and foundations, nominee and fiduciary accounts can be used by criminals who wish to mask the origin of funds. The principal means of preventing ML or TF through the use of such legal structures is to verify the identity of the provider of funds, such as the settlor and also those who have control over the funds, i.e. trustees, advisors, and any controllers who have the power to remove the trustees/advisors etc. In some instances, the settlor may also be a sole trustee or a co-trustee of the trust, in which case, identification documentation should be obtained for the settlor.

Institutions 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.

Where an applicant for business is a trustee, nominee or fiduciary customer, the financial institution must obtain:-

a) Evidence of the appointment of the trustee by means of a certified copy of the Deed of Trust;

b) The nature and purpose of the trust; and

c) Verification of the identity of the trustee[16].

The financial institution should also obtain the following:

a) name of trust[17];

b) source of funds;

c) country of establishment;

d) identity of the trustee(s), settlor(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;

e) identity of person(s) with powers to add beneficiaries, where applicable;

f) identity of the person providing the funds, if not the ultimate settler;

g) identity of the settlor(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:

   i. dispose of, advance, lend, invest, pay or apply trust property;

   ii. vary the trust;

   iii. add or remove a person as a beneficiary or to or from a class of beneficiaries;

   iv. appoint or remove trustees; and

   v. direct, withhold consent to or veto the exercise of a power such as is mentioned in subparagraph (i), (ii), (iii) or (iv): and

h) in the case of a nominee relationship, the identity of the beneficial owner(s).

Institutions are required to verify the identity of any ultimate beneficiary of a legal structure. Depending on the type or nature of the trust, it may be impractical to obtain all of the above at the onset of the relationship e.g. in the case of unborn beneficiaries. In such cases, discretion should be exercised. In all circumstances however, there should be verification of beneficiaries before the first distribution of assets. Further, verification of

16 Refer to FOR, Regulation 17.

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

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.

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.

Financial institutions are required to inform the Central Bank when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of this guideline. The Central Bank will not approve the opening of such an account but will expect the financial institution to conduct enhanced due diligence.

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

Where a corporate trustee acts jointly with a co-trustee, the identity of any non-regulated co-trustees should be verified.

Verification should be made to ensure that any bank account on which the trustees have drawn funds is in their names, and the identities of any additional authorized signatories to the bank account should also be verified.

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 requires further enquiries.

Institutions 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), institutions should endeavour so 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 institutions are encouraged to take this into account while pursuing necessary or appropriate inquiries.

There are a number of commercial structures in which a trust may feature as the legal owner, such as in debt repackaging arrangements. In such cases where the traditional relationship between the settlor and beneficiary is absent, institutions should demonstrate that they understand the commercial rationale for the arrangement and have verified the identity of the various counterparties.

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.

12.3.2 (ii.) Foundations

A foundation (also a charitable foundation) is a legal characterization of a nonprofit organization (NPO) that will typically either donate funds and support to other organizations, or provide the source of funding for its own charitable purposes. A private foundation is a legal entity set up by an individual, a family or group of individuals for a purpose such as philanthropy. Unlike a charitable foundation, a private foundation does not generally solicit funds from the public. In the case of foundations, financial institutions should obtain information on:-

a) The foundation's charter;

b) The 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;

c) The source of funds. In cases where a person other than the founder provides funds for the foundation, institutions should verify the identity of that third party providing the funds for the foundation and/or for whom a founder may be acting;

d) The identification evidence for the founder(s) and for officers and council members of a foundation as may be signatories for the account(s) of the foundation; and

e) The identification evidence should also be obtained for all vested beneficiaries of the foundation.

12.3.2. (iii.) Executorships Accounts

Where a business relationship is entered into for the purpose of winding up the estate of a deceased person, the identity of the executor(s)/ administrator(s) of the estate should be verified. 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 without verification of their identity.

12.3.2. (iv) Non-profit organizations (NPOs)

NPOs differ in size, income, structure, legal status, membership and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes or for carrying out other types of "good works". NPOs can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support.

While terrorist financing may occur through small, non-complex transactions, enhanced due diligence may not be necessary for all clients that are small organizations dealing with insignificant donations for redistribution among members. Institutions should therefore, determine the risk level of activities in which the NPO is engaged.

To assess the risk, a financial institution should consider:

a) The evidence of registration under applicable laws of the home and local operation;

b) The purpose, ideology or philosophy of the NPO;

c) The geographic areas served (including headquarters and operational areas);

d) organizational structure;

e) The NPO's donor and volunteer base;

f) Funding and disbursement criteria (including basic beneficiary information);

g) Record keeping requirements;

h) Affiliation with other NPOs, Governments or groups;

i) Identity of all signatories to the account; and

j) Identity of board members and trustees, where applicable.

As part of the verification process, financial institutions should carry out due diligence against publicly available terrorist lists and monitor on an ongoing basis whether funds are being sent to high-risk countries.

Where a non-profit association is registered in an overseas jurisdiction, it may be useful 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. Institutions should satisfy

themselves as to the legitimacy of the organization[18] by, for example, requesting a copy of the constitution.

Whilst it is not practical to obtain documentary evidence of identity of all donors, institutions, where possible financial institutions should undertake a basic level of due diligence of a foreign NPO's donors in relation to known money laundering and terrorist activities.

12.3.2. (v.) Non-face to face customers

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. The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities.

The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering, and fraud. It is recognized that on-line transactions and services are convenient. However, it is not appropriate that institutions should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. Initial application forms could be completed on-line and then followed up with appropriate identification checks.

Financial institutions are required to pay special attention to any money laundering patterns that may arise from new or developing technology that might favour anonymity; and be used to facilitate money laundering, and financial institutions must take appropriate measures to treat with such patterns[19].

There should be policies in place or measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Institutions offering Internet-based and/or telephone products and services should ensure that they have reliable and secure methods to verify the identity of their customers.

18 For example, www.guidestar.org provides a list of all IRS recognized nonprofit organizations including charities; and www.charity-commission.gov.uk provides a list of registered charities.

19 Refer to the FOR, Regulation 23.

Policies and procedures should address non face-to-face transactions which have an inherent risk of forgery and fraud. Financial institutions 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. The level of verification used should be appropriate to the risks associated with the particular product or service.

Additionally, institutions should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks. To assist in the identification and verification of non-face-to-face customers, financial institutions should:

a) Ensure that documents presented are certified by the relevant and appropriate authority;

b) Require customers to submit additional documents to complement those which are required for face-to-face customers to verify identity;

c) Make face to face contact with the customer;

d) Require the first payment be made through a financial institution which has similar customer due diligence standards;

e) Make independent contact with the customer, for example by telephone on a listed business or other number;

f) Carry out employment checks (where applicable) with the customer's consent through a job letter; and

g) Obtain any other information if deemed appropriate.

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.

12.3.2. (vi.) Introduced business

A financial institution may rely on other regulated third parties[20] to introduce new business in whole or in part. Nevertheless, the ultimate responsibility remains with the

20 In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group or in some cases from another financial institution. It may also occur in business relationships between insurance companies and insurance agents / brokers.

financial institution for customer identification and verification that the documentary evidence of the introducer that is being relied upon, is satisfactory for these purposes.

Financial institutions should therefore:

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

b) Satisfy itself that the regulated entity or introducer has in place KYC/ CDD practices at least equivalent to those required by Trinidad and Tobago law and the financial institution;

c) Obtain copies of the due diligence documentation provided to the introducer within a reasonable time frame subsequent to the commencement of the business relationship; and

d) 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 and where an introducer fails to provide the requisite customer identification and verification documents.

A foreign financial institution may act as an introducer if:

a) It is an entity regulated by a regulatory or supervisory body equivalent to the Central Bank or the TTSEC;

b) It is based in a country subject to equivalent or higher AML/ CTF standards of regulation; and

c) There are no obstacles which would prevent the financial institution from obtaining the original documentation.

Reliance on an eligible introducer should be approved by senior management and the decision as to whether normal due diligence procedures are followed should be part of the financial institution's risk-based assessment.

Notwithstanding any reliance on an eligible introducer's KYC/ CDD procedures, financial institutions should ensure that they immediately obtain all the relevant information pertaining to a customer's identity. Financial institutions should have clear and legible copies of all documentation in their possession within 30 days of receipt of the 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. 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 should be terminated.

A. Introduced Business by Companies within a Financial Institution's Group

When a prospective customer is introduced from within a financial institution's group, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. This is provided that 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 this Guideline.

Financial institutions should obtain written confirmation from the group member confirming completion of verification and retain copies of the identification records in accordance with the requirements in the FOR.

Where a financial institution or its subsidiary initiates transactions 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 possible. In accepting such transactions, institutions should:-

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

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

c) Consider submitting a suspicious activity report (SAR).

B. Introduced Business by Professional Service Providers

Professional service providers act as intermediaries between clients and the financial institution and such persons 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:-

a) Adequately assess the account risk and monitor the relationship for suspicious or unusual activity;

b) Determine whether the person is duly registered under relevant legislation e.g. insurance agents and brokers under the IA, brokers and dealers under the SIA etc.;

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

d) 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 this Guideline.

12.3.2. (vii.) Politically Exposed Persons

Regulation 20 of the FOR defines a "politically exposed person" or PEP as one who is or was entrusted with important public functions in a foreign country and includes examples of who are PEPs.

Business relationships with individuals holding important public positions and with the immediate family members[21] of PEPs or companies in which the PEP is the beneficial owner may expose financial institutions to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud.

Important public positions mentioned above include heads of state, heads of government, senior officials in the executive, legislative, administrative, military or judicial branches of government (whether elected or not), senior officials of major political parties, and senior executives of government-owned corporations. Immediate relatives to such persons such as parents, siblings, the spouse, and children should also be subjected to enhanced due diligence. In addition, a close associate includes any individual who is widely and publicly known to maintain an unusually close relationship with a PEP, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

Provision of financial services to corrupt PEPs exposes financial institutions to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of a whole financial system can be undermined. As such, a financial institution should conduct enhanced due diligence where it has determined that an applicant for business is a PEP.

Financial institutions should also consider extending the application of enhanced due diligence procedures to domestic PEPs and are encouraged to be vigilant in relation to

21 Refer to the FOR, Regulation 20(1)(e)

PEPs from all jurisdictions, in particular high risk countries, who are seeking to establish business relationships.

To mitigate the significant legal and reputational risk exposures that financial institutions face from establishing and maintaining business relationships with PEPs, the following enhanced due diligence procedures should be followed prior to the commencement of such relationships:

a) have appropriate risk management systems to determine whether the customer is a PEP;

b) develop policies, procedures and processes such as the use of electronic databases to assess whether a customer is or has become a PEP;

c) take reasonable measures to establish the source of wealth and the source of funds of PEPs;

d) conduct enhanced ongoing diligence of the business relationship; and

e) obtain senior management approval to establish the relationship where a customer is found to be a PEP.

The abovementioned procedures should also be followed for the existing client base to ensure that all current PEPs have been so identified and remain subject to enhanced customer due diligence processes.

Financial institutions should not establish business relationships with PEPs if the financial institution knows or has reason to suspect that the funds derive from corruption or misuse of public assets. Senior management with ultimate responsibility for banking operations should ensure that the personal circumstances[22], income sources and wealth of PEPs are known and verified as far as possible, and should also be alert to sources of legitimate third party information.

Whilst it is appreciated that efforts must be made to protect the confidentiality of PEPs and their businesses, these accounts must be available for review by the Central Bank, the FIU, Law Enforcement Authorities where required, the compliance officer and the financial institution's internal and external auditors.

12.3.2.(viii.) Private Banking Customers

22 This includes information on (i.) estimated net worth, including financial statements; (ii) 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.

Institutions that offer private banking services for high net worth individuals must ensure that enhanced due diligence policies and procedures are developed and clearly documented in the overall KYC policy to govern this area of operations. Similar to PEPs, senior management with ultimate responsibility for private banking operations should ensure that the personal circumstances, income sources and wealth of private banking clients are known and verified as far as possible, and should also be alert to sources of legitimate third party information. The approval of private banking relationships must be obtained from at least one senior level officer, other than the private banking officer/relationship manager.

12.3.2.(ix.) Transactions Undertaken by Non-Customers on an Occasional Basis

Where a financial institution undertakes these transactions, satisfactory evidence of identity must be obtained failing which, the transaction should be terminated.

12.3.2. (x.) Transactions by Non-Customers

Funds deposited into an existing account by persons whose names do not appear on the mandate for that account, should be handled with particular care. In cases where such transactions are not routine, they should be treated in the same way as transactions with non-account holders.

12.4 High Risk Activities

12.4.1 Examples of high risk activities or services include correspondent banking, payable through accounts, wire transfers, business relations with persons in high risk jurisdictions, hold mail and in care of addresses, transferred accounts, transactions undertaken by non-customers on an occasional basis and transactions by non-customers.

12.4.1.(i.) Correspondent Banking

Correspondent banking is the provision of banking services by one bank in Trinidad and Tobago ("the correspondent bank") to another bank ("the respondent bank") in a foreign country[23]. Correspondent banking relationships are established between banks to facilitate, among other things, transactions between banks made on their own behalf; transactions on behalf of their clients; and making services available directly to clients of other banks.

23 Refer to the FOR, Regulation 21.

Examples of these services include inter-bank deposit activities, international electronic funds transfers, cash management, cheque clearing and payment services, collections, payment for foreign exchange services, processing client payments (in either domestic or foreign currency) and payable-through accounts.

Financial institutions must apply appropriate levels of due diligence to such accounts by gathering sufficient information from and performing enhanced due diligence processes on correspondent banks prior to setting up correspondent accounts.

Regulations 21(2) and (3) of the FOR detail some specific due diligence requirements for correspondent banks prior to their establishing relationships with a respondent bank. The due diligence process prior to the establishment of a correspondent banking relationship should involve:

a) obtaining authenticated/ certified copies of Certificates of Incorporation and Articles of Association (and any other company documents to show registration of the institution within its identified jurisdiction of residence) ;

b) obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;

c) determining the supervisory authority which has oversight responsibility for the respondent bank;

d) determining the ownership of the financial institution;

e) obtaining details of respondent bank's board and management composition;

f) determining the location and major activities of the financial institution;

g) reviewing FATF notices or (or FATF style regional body's) mutual evaluation report or other assessment of the home country's measures to implement the FATF 40 Recommendations and 9 Special Recommendations;

h) establishing and periodically update an AML country risk rating system and assign a rating to each country in which a correspondent banking relationship has been established, for the purpose of implementing an appropriate level of monitoring;

i) ensuring that the documentation of the agreement includes an obligation to provide relevant customer identification information when requested to do so;

j) obtaining details regarding the group structure within which the respondent bank may fall, as well as any subsidiaries it may have;

k) obtaining proof of its years of operation, along with access to its audited financial statements (5 years if possible);

l) information on its external auditors;

m) ascertaining whether the bank has established and implemented sound customer due diligence, anti-money laundering and anti-terrorism financing policies and strategies and appointed a Compliance Officer (at senior management level), inclusive of obtaining a copy of its AML/CTF policy and guidelines;

n) ascertaining whether the correspondent bank has in the previous 7 years (from the date of the commencement of the business relationship or negotiations therefore), been the subject of or is currently subject to any regulatory action or any AML/CTF prosecutions or investigations;

o) establishing the purpose of the correspondent account;

p) documenting the respective responsibilities of each institution in the operation of the correspondent account; and

q) identifying any third parties that may use the correspondent banking services.

A financial institution is prohibited from entering or continuing a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence[24]. Consequently, financial institutions will need to satisfy themselves that the foreign respondent banks do not permit their accounts to be used by shell banks. In this regard financial institutions should take account of whether:-

a) the respondent bank permits "payable through accounts". This would be one likely way in which shell banks could take advantage of respondent banks;

b) the respondent bank's inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank; and

c) the country in which the foreign respondent bank resides; (see note on countries with inadequate AML/CTF frameworks) has secrecy laws that prohibit the release of any KYC information or which laws present an obstacle to the KYC due diligence process may pose a particular problem in this regard.

12.4.1.(ii.) Payable-Through Accounts

Payable-through accounts refer to correspondent accounts that are used directly by third parties to transact business on their own behalf. In this regard, banks must be guided by the criteria established for introduced business.

Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf. FATF also requires

24 Refer to the FOR Regulation 22.

financial institutions that use payable through accounts to apply enhanced due diligence measures in addition to normal measures.

12.4.1.(iii.) Wire/funds transfers

A wire transfer from one financial institution to another, is exempted from the CDD where both the originator and beneficiary are financial institutions acting on their own behalf[25]. Financial institutions are required to apply CDD for one-off or occasional wire transfers of six thousand dollars or more.

Regulations 33 and 34 of the FOR detail the information required by a financial institution in respect of wire transfers. Such provisions should be incorporated into the financial institution's compliance programme.

Where a financial institution is acting on behalf of another financial institution, its shall ensure compliance with applicable law and guidelines in respect of any financial transaction carried out by the financial institution for which it has accepted responsibility.

Particular care must be paid to wire transfers emanating from high risk jurisdictions and/or jurisdictions that do not sufficiently comply with international standards for AML/ CTF. Where a relationship is deemed high risk e.g. located in a high-risk jurisdiction, further to standard due diligence, a financial institution should:

a) undertake a more detailed understanding of the AML/CTF programme of the respondent bank and its effectiveness;

b) review effectiveness of the respondent's group programme;

c) identify the respondent's owners, director and senior managers; and

d) determine the ownership structure.

12.4.1.(iv.) Hold Mail and c/o Addresses

Sometimes the directors or beneficial owners of client companies request that mail not be forwarded but held at the registered office for storage or later collection. These are not necessarily suspicious acts but do carry higher risk and should warrant special attention. Additionally, clients who request "c/o" addresses should also be subject to enhanced due diligence.

25 Refer to the FOR, Regulation 35.

12.4.1.(v.) Transferred Accounts

Where accounts are transferred from another financial institution, enhanced KYC standards should be applied especially if the financial institution has any reason to believe that the account holder has been refused banking facilities by the other financial institution.

12.5 Business relations in high risk jurisdictions[26]

Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to financial institutions. 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.

Financial institutions are encouraged to consult publicly available information to ensure that they are aware of countries/territories which may pose a higher risk e.g. FATF and other useful websites.

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.

The commencement of business relationships with clients residing in high-risk countries must have the prior approval of senior management. All suspicious transactions originating from such countries must be investigated, the findings established in writing and immediately reported to the FIU.

13. REDUCED DUE DILIGENCE AND EXEMPT CLIENTS

13.1 A financial institution 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 are set out below:-

a) 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.

b) Where an existing customer opens a new account. 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.

26 Refers to countries that appear on FATF public lists of high risk and non-cooperative jurisdictions, UN Lists or any other such lists.

c) Where a financial institution acquires the business of another regulated entity, whether in Trinidad and Tobago or elsewhere, and it is satisfied that the due diligence standards of the acquired institution are at least equivalent to that set in this Guideline, it need not re-verify the customers.

13.2 If the financial institution is not satisfied that equivalent standards have been followed, it should seek to identify and verify the identity of customers who do not have existing relationships with the financial institution.

13.3 Regulations 14 and 29 of the FOR outline certain circumstances where documentary evidence of identity is not required. Such circumstances include:-

a) where a financial institution carries out a one-off transaction with a third party following an introduction by a person who has provided a written assurance that the identity of the third party introduced by him has been obtained.

b) in the case of a pension scheme taken out with the person's employer and where contributions to the scheme are made via deductions from wages and assignment of a member's interest is not permitted under the scheme.

c) where there is a contract of long-term insurance or where a contract of insurance has no surrender clause and may not be used as collateral for a loan.

13.4 Additionally, documentary evidence of identification may not be required in the case of exempt customer such as:-

a) any central or local government agency or statutory body;

b) a publicly traded company or investment fund listed on the Trinidad and Tobago Stock Exchange or any other stock exchange specified by the Central Bank where there is no shareholder with 10 percent or more of the shares of the company[27];

c) financial institutions regulated by the Central Bank, or the Trinidad and Tobago Securities and Exchange Commission; and

d) foreign financial institutions regulated by a Central Bank or equivalent supervisory authority in a jurisdiction that adequately complies with the FATF 40 + 9 Recommendations on AML/ CTF[28].

14. RETROSPECTIVE DUE DILIGENCE

14.1 Regulation 37 of the FOR requires a financial institution to conduct retrospective due diligence on all existing accounts. Where the identity information held on existing customers does not comply with the

27 Refer to the FOR, Regulation 16(2)(c).
28 Refer to FATF Public Statement on jurisdictions with strategic AML/CTF deficiencies at www.fatf.org.

requirements of relevant AML/ CTF legislation and this Guideline, financial institutions are required to develop a risk-based programme for ensuring compliance. Financial institutions should therefore:-

a) record their non-compliant business relationships, noting what information or documentation is missing;

b) 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, a material change in the way that an account is operating, or doubts about previously obtained customer due diligence data; and

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

14.2 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, reported to the board and a note placed on the individual's file.

15. PRE-EMPLOYMENT BACKGROUND SCREENING KNOW YOUR EMPLOYEE (KYE)

15.1 In addition to establishing and implementing CDD policies and procedures, every financial institution shall utilize best practices of the industry, to determine its staff recruitment policy, to attract and retain staff of the highest levels of integrity and competence[29]. The ability to implement an effective AML/ CTF programme depends in part on the quality and integrity of staff.

15.2 Consequently, financial institutions should undertake due diligence on prospective staff members. The financial institution should:

a) verify the applicant's identity;

b) develop a risk-focussed 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;

c) 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 for conduct, ethics, conflicts of interest) for assessing staff; and

d) have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

29 Refer to the FOR, Regulation 5.

15.3 The names, addresses, position titles and other official information pertaining to staff appointed or recruited by the financial institution should be maintained for up to a period of six years after termination of employment and made available to the Central Bank upon request.

15.4 Financial institutions should ensure to the extent permitted by the laws of the relevant country, that similar recruitment policies are followed by its branches, subsidiaries and associate companies abroad, especially in those countries which are not sufficiently compliant with the recommendations of the Financial Action Task Force[30].

16. COMPLIANCE OFFICER[31]

16.1 Every financial institution shall for the purpose of securing compliance with section 55(3) of POCA and Regulation 3 of the FOR, designate a manager or official employed at managerial level as the Compliance Officer[32] of that institution[33] and such person must be approved by the Central Bank. In the case of a financial institution licensed under the FIA, or an insurer registered under the IA, the Compliance Officer must satisfy the definition of an "officer" as contained in the respective legislation and satisfy "fit and proper" requirements. Further, where a financial institution has five or fewer employees, as may be the case with an insurance broker, cambio or money remittance business, the most senior employee shall be the Compliance Officer[34].

16.2 A financial institution shall ensure that its Compliance Officer receives appropriate training to enable him/her to perform his/her duties adequately and such training shall be provided on at least an annual basis.

16.3 The financial institution must ensure that the Compliance Officer and other employees have timely access to customer identification data and other records and relevant information to enable them to produce reports in a timely manner.

16.4 In accordance with Regulation 4(3) of the FOR, the identity of the Compliance Officer must be treated with strictest confidence by the members of staff of the institution.

30 Refer to the FOR, Regulation 5.
31 The requirements for a compliance officer are outlined in Regulations 3, 4 and 8 of the FOR.
32 A Compliance Officer is defined in Part I of the FOR.
33 Refer to the FOR, Regulation 3.
34 Refer to the FOR, Regulation 3(3).

16.5 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 Compliance Officer should be conducive to the effective and independent exercise of his/her duties.

16.6 At a minimum, the Compliance Officer must perform the functions and duties as prescribed in Regulation 4(1) of the FOR. In addition, the Compliance Officer is required to consider any report submitted to him/her on a transaction which is believed or known to be proceeds of a specified offence and where necessary submit a suspicious activity report (SAR) to the Financial Intelligence Unit (FIU).

16.7 The Compliance Officer may consider an annual self-assessment of the institution's AML/ CTF controls. The self-assessment would provide financial institutions with:

a) insight into the efficacy of controls in the AML/CTF program, and the overall extent to which the program adequately mitigates the identified inherent risks of ML and TF; and

b) information to aid in prioritizing remediation efforts if controls are under-performing and opportunities to capture economies of scale to better allocate resources to areas of higher risk.

16.7.1 While the assessments in business areas can and should be conducted by individuals in those business areas, financial institutions should ensure that the assessment process is designed to enable results in each area to be consolidated for analysis and other purposes.

16.7.2 The self-assessment in each relevant area of the financial institution should cover, at a minimum, the adequacy of the inherent risk assessment, AML/ CTF policies and procedures, training and other controls implemented to mitigate ML and TF risks.

16.7.3 Financial institutions should ensure that the self-assessment is neither too narrow nor too broad. For example, a narrow legal/regulatory-based assessment could fail to cover broader ML and TF controls. Similarly an operational-based assessment might fail to cover prescribed controls.

16.7.4 All significant information used in the self-assessment process should be verified or readily verifiable. Methods used to ensure that information is verified or verifiable will depend on the size, complexity and governance structure of the financial institution.

17. INTERNAL AND EXTERNAL AUDIT

17.1 Internal and external auditors must conduct regular reviews of a financial institution's compliance programme[35]. However, the external auditor is required to submit an external audit report to the Central Bank and the financial institution's Board of Directors annually. The copy of the external audit report should be submitted to the Central Bank within four (4) months of the financial institution's year end.

17.2 Where a financial institution fails to engage the services of an external or internal auditor, the Central Bank shall appoint a competent professional to perform those functions and the costs shall be borne by the financial institution[36].

17.3 The audit scope should at a minimum review the financial institution's compliance programme to ensure compliance with all relevant AML/ CTF laws[37], regulations and these Guidelines.

17.4 Internal audit should perform regular reviews to evaluate the effective implementation of compliance policies. The regularity of internal audit review should be determined by the financial institution and should be carried out on a frequency consistent with the financial institution's size and risk profile. The review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external audit and the Central Bank have been satisfactorily addressed.

18. SUSPICIOUS ACTIVITY REPORTING (SARS)

18.1 Financial institutions must ensure that, in the event of a suspicious activity being discovered, all staff are aware of the reporting chain and the procedures to follow.

18.2 Staff at all levels of the financial institution must be made aware of the identity of the Compliance Officer and the procedure to be followed when making a suspicious activity report. All staff must be aware that all suspicious activity should be reported to the Compliance Officer.

18.3 Staff of financial institutions should report all suspicious activities to the Compliance Officer, and any such report must be considered in the light of all other relevant information, for the purpose of determining

35 Refer to the FOR Regulation10.
36 Refer to the FOR Regulations 10(3) and 10(4).
37 Refer to 2.1 of these Guidelines.

whether or not the information or other matter contained in the report gives rise to a suspicion as soon as possible[38].

18.4 Where staff continues to encounter suspicious activities on an account which they have previously reported to the Compliance Officer, they should continue to make reports to the Compliance Officer whenever a further suspicious transaction occurs.

18.5 All reports of suspicious activities must reach the Compliance Officer who should have the authority to determine whether a disclosure in accordance with the legislation is appropriate. However institutions may have internal reporting procedures that allow a suspicious report to be channeled through the relationship or line manager before it reaches the Compliance Officer. Where such internal reporting procedures are in place, the line manager cannot alter the report but can attach his/ her comments as to why he/ she believes that the suspicion is not justified. Regardless, of the internal reporting procedures adopted all reports of suspicious activities must reach the Compliance Officer.

18.6 The Compliance Officer of the financial institution is required to make a suspicious transactions or a suspicious activity report (SAR) to the FIU where the financial institution knows or has reasonable grounds to suspect that funds are the proceeds of a specified offence and are being used either for:

a) business transactions with persons and financial institutions in or from other countries which do not or insufficiently comply with the FATF Recommendations;

b) for complex, unusual or large transactions whether completed or not; or

c) transactions which have no apparent economic or visible lawful purpose.

18.7 A financial institution may in accordance with section 13 of the FIUTTA seek the approval of the FIU to complete a suspicious transaction and the Director may grant such approval with such conditions as he sees fit, but the granting of the approval shall not prejudice any analysis or evaluation being undertaken by the FIU[39].

18.8 The SAR should be made as soon as possible but within fourteen days of the date on which the financial institution knew or had reasonable grounds to suspect that the funds used for the transaction were the proceeds of a specified offence[40]. The SAR should be in the format prescribed in the Third Schedule of the POCA[41] or such other form as the FIU may prescribe. A SAR can be submitted either electronically, in writing or by facsimile[42].

38 Refer to POCA Section 30(3)(B)
39 Refer to the FIUATT section 13.
40 Refer to POCA, Section 30(3B).
41 Refer POCA 55(3)
42 Refer to Regulation 6 of FIUTT Regulations, 2011.

18.9 Financial institutions should ensure that all contact between their departments or branches with the FIU and law enforcement agencies is reported to the Compliance Officer so that an informed overview of the situation can be maintained.

19. LEGAL PROTECTION AND INDEMNIFICATION

19.1 Where financial institutions, their directors, officers, employees and agents disclose a suspicion or belief that any property represents another person's proceeds of a specified offence under POCA[43], such disclosure is not treated as a breach of any restriction upon the disclosure of information imposed by contract or by any regulation or rule of conduct.

19.2 When a suspicious activity report is made to the FIU in good faith, financial institutions their employees, staff, directors, owners or other representatives as authorised by law, are exempted from criminal, civil or administrative liability as the case may be, 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[44].

19.3 It is illegal for employees, directors, officers or agents of a financial institution to disclose that a suspicious transaction report or related information on a specific transaction has been reported to the FIU. This is known as 'tipping off'[45].

20. UNUSUAL, COMPLEX AND SUSPICIOUS TRANSACTIONS

20.1 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. Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis. In this regard, financial institutions should examine, to the extent possible, the background and purpose of transactions that appear to have no apparent economic or visible lawful purpose, irrespective of where they originate.

20.2 Complex transactions or structures may have entirely legitimate purposes. However, financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of

43 Refer POCA 47.
44 Refer POCA 55.
45 Refer POCA 51(1).

transactions, which have no apparent economic or visible lawful purpose[46]. The background and purpose of such transactions should as far as possible be examined and documented by the financial institution. Findings regarding enquiries about complex, unusual large transactions, and unusual patterns of transactions should be kept by the financial institution, and be available to help supervisory authorities and auditors for at least six years.

20.3 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 complex, unusual or large or may represent an unusual pattern. 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. A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and determination of consistent transaction limits.

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. The key is to know enough about the customer (KYC) and the customer's normal expected activities to recognize when a transaction, or series of transactions, is unusual. Although there is a tendency to focus on new business relationships and transactions, institutions should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant, unexpected and unexplained change in the behaviour of an account.

20.4 Financial institutions should develop procedures to assist in the identification of unusual or suspicious activity in all types of business transactions, products and services offered, but particularly for transactions with high risk customers and using high risk services (for example wire transfers, credit/debit cards and ATM transactions, lending, trust services and private banking). For example, to facilitate the detection of suspicious transactions, a financial institution should:-

a) require customers to indicate/reveal 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.

b) 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;

c) require its staff to document in writing their suspicion about a transaction; and

d) require documentation of internal enquiries.

20.5 The following factors should be considered by the financial institution when seeking to identify a suspicious transaction:

46 Refer to the POCA 55 (2)(a)(ii)

a) Is the customer known personally?

b) Is the transaction in keeping with the customer's normal activity known to the financial institution, the markets in which the customer is active and the customer's own business? (i.e. does it make sense?)

c) Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market, size and frequency?

d) Is the role of the agent involved in the transaction unusual?

e) Is the transaction to be settled in the normal manner?

f) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries? and,

g) Can you understand the reasons for the transaction i.e. might there be an easier, cheaper or more convenient method available?

20.6 Internal reporting procedure

20.6.1 Where the staff member conducts enquiries and obtains what he considers to be a satisfactory explanation of the complex, unusual or large[47] transaction, or unusual pattern of transaction, he may conclude that there are no grounds for suspicion, and therefore take no further action as he is satisfied with matters. However, where the enquiries conducted by the staff member do not provide a satisfactory explanation of the transaction, he may conclude that there are grounds for *suspicion* requiring disclosure.

20.6.2 Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, forwarded to the Compliance Officer who will determine whether the transaction should be reported to the FIU as soon as possible or within fourteen days of the date on which the financial institution knew or had reasonable grounds to suspect that the funds used for the transaction were the proceeds of a specified offence[48].

20.6.3 Enquiries to check whether complex or unusual transactions or structures have legitimate economic or lawful purpose, where conducted properly and in good faith, are not regarded as tipping off.

47 Refer to the POCA 55(3C) – a large transaction means a transaction, the value of which is ninety five thousand dollars or such other amount as the Minister may by Order prescribe.
48 Refer to POCA Section 55 (3B).

20.7 Reporting Declined Business

20.7.1 It is normal practice for financial institutions to turn away business that they suspect might be criminal in intent or origin. Where an applicant for business or a customer fails to provide adequate documentation, including the identity of any beneficial owners or controllers, consideration should be given to filing a SAR.

20.7.2 Where an attempted transaction gives rise to knowledge or suspicion of money laundering or terrorist financing, that attempted transaction should be reported to the FIU. Reporting of such events will allow the FIU to build a clearer picture of the money laundering threat, and to use such intelligence on a proactive basis. Furthermore, the financial institution should refrain from referring such business to other financial institutions

20.7.3 Pursuant to the United Nations Resolutions on terrorist financing, financial institutions should freeze any funds or other assets held for individuals or organisations listed on the UN list of persons connected to terrorism, and submit a report to the Authority. This list may be accessed at www.un.org.

21. RECORD KEEPING PROCEDURES

21.1 Part V of the FOR stipulates the minimum requirements for financial institutions with regard to record keeping.

21.2 To facilitate compliance with Part V of the FOR and to facilitate investigations undertaken by the FIU, financial institutions 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. Once a business relationship has been formed, the financial institution should maintain records of client identification and transactions performed.

21.2.1 The document retention policy should incorporate the requirement that a financial institutions is required to keep records of all domestic and international transactions as well as identification data on a customer for a minimum period of 6 years, unless a longer time period is required by other statutory requirements or mandated by the Central Bank. It may also be necessary for financial institutions 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 there :

a) has been a report of a suspicious activity; or

b) is an on-going investigation relating to a transaction or client.

21.2.2 In addition, transaction records should contain sufficient detail to permit reconstruction of individual transactions. Such details are specified in Regulation 32 of the FOR.

21.2.3 Records should be retained in a format, including electronic, scanned or microfilm, that would facilitate reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity and to enable financial institutions to comply swiftly with information requests from the FIU. This applies whether or not records are stored off the premises of the financial institution.

21.3 Financial institutions should ensure that records held by a subsidiary or affiliate outside Trinidad and Tobago at a minimum, comply with the requirements of Trinidad and Tobago law and this Guideline.

21.4 Where the financial institution has outsourced any or all of the foregoing functions to a company in another jurisdiction then it must be satisfied that the relevant records will be maintained in accordance with Trinidad and Tobago law and will be available to the Central Bank on request and to the FIU or law enforcement authorities.

21.5 When a financial institution merges with or takes over a financial entity, it should ensure that the records such as customer due diligence, transactions, external audit and training 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.

21.6 Each financial institution is required to maintain a register of all enquiries and containing such details as specified in Regulation 38 of the FOR.

21.7 Financial institutions are also required to maintain records of staff training which at a minimum should include:-

a) details of the content of the training programmes provided;

b) the names of staff who have received the training;

c) the date on which the training was delivered;

d) the results of any testing carried out to measure staff understanding of the anti-money laundering requirements; and

e) an on-going training plan.

22. TRAINING AND AWARENESS

22.1 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 analysing potential illicit transactions. Therefore, in accordance with Regulation 6 of the FOR, financial institutions are required to ensure that its directors and staff and appropriately trained to equip them to perform their obligations in respect of AML/ CTF requirements.

22.2 Training should be targeted at all employees but greater emphasis should be placed on the training of the Compliance Officer as well as the compliance and audit staff because of their critical role in sensitizing the broader staff complement to AML/CTF issues and ensuring compliance with established AML/ CTF policies and procedures.

22.3 At a minimum, a financial institution is required to:

a) Develop an appropriately tailored training and awareness programme consistent with their size, resources and type of operation to enable their employees to be aware of the risks associated with ML and TF. The training should also ensure employees understand how the institution might be used for ML or TF; enable them to recognise and handle potential ML or TF transactions; and to be aware of new techniques and trends in money laundering and terrorist financing;

b) Document, as part of their AML/ CTF policy document, their approach to training, including the frequency, delivery channels and content;

c) Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the Reporting Officer to whom they should report unusual or suspicious transactions;

d) Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:

   i. new employees;

   ii. operations staff;

   iii. supervisors;

   iv. board and senior management; and

   v. audit and compliance staff.

e) Obtain an acknowledgement from each staff member on the training received;

f) Assess the effectiveness of training; and

g) Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

22.4 A financial institution should clearly explain to its directors, senior management and employees the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious activity reporting. In particular directors, senior management and other employees should be sensitized as to:-

a) the importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;

b) the procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;

c) the completion of unusual and suspicious transaction reports;

d) treatment of incomplete or declined transactions; and

e) the procedures to follow when working with law enforcement or the FIU on an investigation.

23. STATUTORY REPORTING REQUIREMENTS

23.1 In addition to the internal reporting requirements (see section 20.6 of this Guideline), several statutory reports are required to be provided to the FIU and the Central Bank.

23.2 Where a financial institution is required to report to the FIU, the format of such reports and the manner in which such reports are to be submitted to the FIU shall be prescribed or specified by the FIU. Similarly, where a financial institution is required to report to the Central Bank as is the case with the submission of the external audit report, the manner of such reporting may be specified by the Central Bank.

23.3 In addition to the reporting of SARs (section 18 of this Guideline refers), every financial institution is required to disclose forthwith to the FIU:

a) The existence of any property in his possession or control, which to his knowledge is terrorist property or which there are reasonable grounds to believe is terrorist property;
b) Any information regarding a transaction or proposed transaction in respect of terrorist property; or
c) Any information regarding a transaction or proposed transaction which there is reasonable grounds to believe may involve terrorist property[49].

23.4 Subsequent to the initial disclosure under 23.3, every financial institution is required to report every three months to the FIU if:

a) it is not in possession or control of terrorist property, that it is not in possession or control of such property; or

49 Refer to ATA, Section 33 (1).

b) it is in possession or control of terrorist property that it is in possession or control of such property and the particulars relating to the persons, accounts and transactions involved and the total value of the property[50].

23.5 Every financial institution shall report, to the FIU every transaction which occurs within the course of its activities, in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of a terrorist act[51].

23.6 In addition, the FIU may request any other information from a financial institution either orally, in writing or electronically[52].

50 Refer to ATA, Section 33 (3).
51 Refer to ATA, Section 33(4).
52 Regulation 3.4 of FIUTT Regulations, 2011.

APPENDIX I - SECTOR SPECIFIC GUIDANCE:

For Institutions Licensed under the Financial Institutions Act 2008

Indicators of Suspicious Transactions/ Activity

1. Cash Transactions

(a) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(b) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(c) Deposit and withdrawal transactions conducted in cash rather than through forms of debits and credits normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

(d) Customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.

(e) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(f) Frequent exchange of cash into other currencies.

(g) Branches that have a great deal more cash transactions than usual. (Head Office statistics may detect aberrations in cash transactions.)

(h) Customers whose deposits contain counterfeit notes or forged instruments.

(i) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(j) Large cash deposits using night safe facilities (which may be inconsistent with the customer's business or profile) and thereby avoiding direct contact with bank staff.

2. Bank Accounts

(a) Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with the type of business, including transactions which involve nominee names.

(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business.

(d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or providing information that is difficult or expensive to verify.

(e) Customers who appear to have accounts with several financial institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(f) Matching of payments out with credits paid in by cash on the same or previous day.

(g) Deposits via large third party cheques endorsed in favour of the customer.

(h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(j) Greater use of safe deposit facilities, especially where sealed packets are deposited and withdrawn.

(k) Companies' representatives avoiding contact with the branch.

(l) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred to other client company and trust accounts.

(m) Customers who decline to provide information that would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(n) Preference for the use of low interest earning accounts for large balances, where options exist for higher earnings.

(o) Large number of individuals making payments into the same account without an adequate explanation.

3. Investment Related Transactions

(a) Back-to-back deposit/ loan transactions with subsidiaries or affiliates of overseas financial institutions in known drug trafficking areas.

(b) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent financial position.

(c) Large or unusual settlements of securities transactions in cash.

(d) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering by International Activity

(a) Customers introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Customers who make regular and large payments that cannot be clearly identified as bona fide transactions to, or who receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs; or who conduct transactions with proscribed terrorist organizations.

(d) Accumulation of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

(f) Frequent paying in of travellers' cheques, foreign currency drafts or other negotiable instruments.

5. Money Laundering Involving Employees and Agents

Financial Institutions should pay particular attention to the following: -

(a) Changes in employee characteristics, e.g., sudden lavish lifestyle or avoidance of vacations.

(b) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

(c) Refusal of a change in responsibility such as a promotion.

6. Money Laundering by Secured and Unsecured Lending

(a) Customers who repay problem loans unexpectedly.

(b) Requests to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's apparent financial position.

Request by a customer to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

7. Provision of Safe Custody and Safety Deposit Boxes

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

APPENDIX II - SECTOR SPECIFIC GUIDANCE:

For Insurance Companies Registered under the Insurance Act

A: TRANSACTIONS WITH INTERMEDIARIES

In addition to the guidance given in Part IV of the FOR, insurance companies should also:

(i) ensure that if an agent or broker is responsible for collecting the information required to make a third party determination , these responsibilities are documented;

(ii) ensure they receive client identification information in the required timeframes; and

(iii) periodically review, in a systemic manner, the quality of client information gathered and documented by the agent or broker to ensure that it continues to meet their requirements.

Documentation of relationships and communications with, and client due diligence work of, agents and brokers, should be complete and current, and client information should be placed in the client's record promptly upon receiving it. Insurers should consider terminating relationships with agents or brokers that do not comply with agreed upon client identification responsibilities or provide the insurer with the requisite client information on a timely basis.

Contracts with agents and brokers should be reviewed and updated as necessary to ensure compliance with the AML/ CTF laws and guidelines. The extent of the insurer's exposure to the agent or broker for the results of client due diligence should be addressed expressly in the insurer's inherent risk assessment.

B: EXAMPLES OF SUSPICIOUS TRANSACTIONS

a) Insurance Policies

(i) Application for insurance outside the policyholder's normal pattern of business needs.

(ii) Any lack of information or delay in the provision of information to enable verification to be completed.

(iii) Any transaction involving an undisclosed party.

(iv) Early termination of policy, especially at a loss caused by front end loading, or where cash was tendered and/or the refund cheque is to a third party.

(v) A transfer of the benefit of a policy to an apparently unrelated third party.

(vi) Request for purchase of a policy requiring a large lump sum payment where the policyholder has previously requested only small, periodic-payment contracts.

(vii) Attempts to use a third party cheque to make a purchase of a policy.

(viii) Applicant shows no concern for the performance of the policy but much concern for its early cancellation provisions.

(ix) Applicant is reluctant to provide normal information when applying for a policy, provides minimal or fictitious information, or provides information that is difficult or expensive to verify.

(x) Applicant appears to have an unusual number of policies with different insurers.

(xi) Applicant purchases policies in amounts considered beyond the customer's apparent means.

(xii) Applicant establishes a large insurance policy and within a short time period cancels the policy and requests that the cash value be paid to a third party.

(xiii) Applicant wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

(xiv) Applicant uses a mailing address outside the area where the application is made and where the home telephone is found to have been disconnected, upon verification attempt.

b) Money Laundering Using Cash Transactions

(i) Applicant attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.

(ii) Applicant requests to make a lump sum payment by a wire transfer or with foreign currency.

c) Money Laundering by International Activity

(i) Application for a policy from a potential client in a distant place where a comparable policy could be obtained "closer to home".

(ii) Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (e.g. drug trafficking or terrorist activity) are prevalent.

d) Money Laundering by Employees or Agents

Insurance entities should pay particular attention to employees and agents who show: -

(i) a sudden lavish lifestyle or do not take vacations.

(ii) dramatic, unexpected increases in sales.

C: RISKS ASSOCIATED WITH GENERAL AND LONG-TERM INSURANCE BUSINESS

In relation to insurance business, significant factors that will affect the level of risk of any transaction or business relationship include:

i. The applicants for business,

ii. The product to be underwritten or sold,

iii. The nature of the business relationship formed, and

iv. The method of payment of the premium.

NATURE OF PRODUCTS UNDERWRITTEN OR SOLD

A significant factor determining the level of AML/CTF risk in any product is the level of premium payable on the policy and method of payment. For example, a motor policy with an annual premium of $1000 will present a much lower risk than one on a luxury car or car fleet in the case of a commercial motor policy, which commands a much higher premium and value at risk. Premium payments made in cash are generally a concern. For example, premiums for property and casualty policies in the case of condominium developments may be significant and insurers should be especially vigilant when requests are made for large premiums to be paid in cash. Sound claims management is essential as money laundering or terrorist financing can occur through inflated or bogus claims, e.g. by arson or other means causing a fraudulent claim to be made.

FEATURES OF HIGH RISK AND LOW RISK GENERAL INSURANCE PRODUCTS

Low risk	Low premiums, inability to make claims without substantial reliable evidence of loss. Products rated as low AML/CTF risk may also be rated a low fraud risk, but not always. **Example** A single, individual travel policy may be considered low risk simply because the premium is low and the term date is short. Other travel policies however, for example, annual or group, may be considered to pose a relatively increased risk and thus controls should be applied appropriately.
High risk	High premium amounts; and the ability to pay in cash, to overpay premiums, and to cancel the policy to seek a premium refund. Also the greater risk of fraud will generally mean a greater risk of AML/CTF. **Example** May include Cash-In-Transit policies or Fidelity Guarantees where the likelihood of manipulation and conspiracy is greater.

FEATURES OF HIGH RISK AND LOW RISK LONG TERM (LIFE) INSURANCE PRODUCTS

Low	Life insurance policies where the premium payable annually is low.
High	1. Unit-linked or with profit single premium contracts 2. Single premium life insurance policies that store cash value 3. Fixed and variable annuities 4. (Second hand) endowment policies.

Additional Guidance

In insurance, various transactions or 'trigger events' occur after the contract date and indicate where due diligence may be required. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. In this respect "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, requests for changes in cover, redemption, cancellation, claim submission premium payments, requests for changes in benefits, beneficiaries, duration, etc.

Monitoring the Customer's Business

In general, the insurer should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

Red Flags

(a) Requests for a return of premium to be remitted to persons other than policy holder.

(b) Claims payments paid to persons other than policyholders and beneficiaries.

(c) Unusually complex holding company or trust ownership structure.

(d) Claims fraud.

(e) A change in beneficiaries (for instance, to include non-family members).

(f) A change/increase of the premium payment (for instance, which appear unusual in the light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party).

(g) Use of cash and/or payment of large single premiums.

(h) Payment/surrender by a wire transfer from/to foreign parties.

(i) Payment by banking instruments, which allow anonymity of the transaction.

(j) Change of address and/or place of residence of the policyholder.

(k) Lump sum top-ups to an existing life insurance contract.

(l) Lump sum contributions to personal pension contracts.

(m) Requests for prepayment of benefits.

(n) Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution).

(o) Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment).

(p) Early surrender of the policy or change of the duration (including where this causes penalties).

(q) Requests for multiple policies to be taken out for premiums slightly below any publicized limits for performing checks, such as checks on the source of wealth or cash payments.

Additional Red Flags

Money laundering and the financing of terrorism can occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, and fronting arrangements, or by the misuse of normal reinsurance transactions. Examples include:

(a) the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds;

(b) the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding; and

(c) the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

Even the typically lowest risk product could potentially be used for money laundering for example, workers compensation schemes may be established for fictitious personnel or be funding mechanisms for terrorists awaiting assignment. One factor that should help to mitigate this risk is the involvement of independent third parties e.g. medical practitioners, claims adjusters and government agencies to substantiate claims. In the international market the scope for lines of business in insurers is unlimited. The focus should be the operators and owners of the insurer, the business rationale for the insurer, its relationships and source of funding.

APPENDIX III - SECTOR SPECIFIC GUIDANCE

For Money Remittance Business

""Money transmission or remittance business"" (MTB) can be considered as the business of accepting cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money transfer business belongs. Remittances may be domestic or international.

Vulnerability of MTBs to Money Laundering and Terrorist Financing

The fleeting relationship with its customers makes MTBs 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 MTB and can repeatedly use different MTBs to transact business. The MTB is 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 globe.

While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, 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.

Apart from money transmission, cheque cashing is another important segment of the business for some MTBs. MTBs should be aware that endorsed third party cheques from overseas are a money laundering risk. Even where a local cheque, endorsed by a third party, is presented to the MTB for cashing, the MTB 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.

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.

Transaction Monitoring

Because of the large number of customers involved and the relatively small amounts transacted, it is imperative for MTBs to have adequate systems in place to collate relevant information and monitor customers' activities. In the

MTB, the amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MTBs to determine whether there is any risk that the customer is utilising multiple recipients to facilitate money laundering or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

Indicators of the Misuse of MTBs

The following activity may be suspicious and indicate money laundering or other illegal activity through the misuse of MTBs.

Transactions Which Do Not Make Economic Sense

a) Transactions which are incompatible with the licensee'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 attempting to hide the size of a large cash transaction by breaking it into multiple, smaller transactions by, for example, conducting the smaller transactions -

   i. at different times on the same day;

   ii. with different MTB cashiers on the same day or different days; and

   iii. at different branches/offices of the same MTB.

c) Transactions that cannot be reconciled with the usual activities of the customer.

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

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

Transactions Involving Large Amounts of Cash

a) Frequent transactions of large cash amounts that 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, to countries associated with the production, processing or marketing of narcotics or other illegal drugs.

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

Other Types of Transactions and Activity

a) Transaction volume and activity is not commensurate with the customer's known profile (e.g. age, occupation, income).

b) Transactions with countries or entities that are reported to be associated with terrorist activities or with persons that have been designated as terrorists.

c) Use of multiple transactions and multiple recipients, including structuring of transactions to avoid identification threshold or whatever enhanced due diligence threshold that the MTB may have.

d) A business customer that is reluctant to provide complete information regarding: the type of business, the purpose of the transaction, or any other information requested by the MTB.

Red Flags

a) Deposit of cheques or funds transferred to/from high-risk jurisdictions or from different jurisdictions than expected or typically seen in the account;

b) Unusually large or frequent deposits or fund transfers;

c) Use of multiple transactions and multiple recipients, including structuring of transactions to avoid identification threshold or whatever enhanced due diligence threshold that the MSB may have;

d) Multiple customers remitting multiple small sums to one recipient where the aggregate amount exceeds the reporting threshold requirements;

e) A single customer remitting to several persons overseas where the aggregate sum exceeds reporting thresholds;

f) Multiple large remittances over a short period of time, executed by the same sender or for the benefit of the same recipient;

g) A customer or group of customers attempting to hide the size of a large cash transaction at different times on the same day, with different MSB cashiers on the same day or different days, at different branches/offices of the same MSB;

h) Large volumes of cash received or remitted to one or more recipients over a period of time;

i) A customer purchases money transfers, money orders, traveller's cheques, etc, with large amounts of cash

j) Business customer reluctant to provide complete information regarding the type of business, the purpose of the transaction, or any other information requested by the MSB; and

k) Lack of adequate client identification or source of funds being provided.

APPENDIX IV - SECTOR SPECIFIC GUIDANCE

For Cambios and Bureaus De Change

Cambios and bureaus de change in Trinidad and Tobago are prohibited from dealing with cheques, consequently the risk of money laundering is lowered. Nevertheless, cambios should pay particular attention where the applicant for business is a corporate customer seeking to act through an agent/bearer (whether employed or contracted, and which is usually the case), the letter should clearly indicate the business to be transacted, that the agent/bearer is acting on the corporate customer's behalf for this matter and that the person signing to the letter is authorized so to do. Where in relation to the corporate customer it appears to the cambio conducting the transaction that the agent/bearer is not the usual agent/bearer, or the letter from the corporate customer is in any way defective, (e.g. it is not on official letterhead; there have been alterations or amendments to the contents of the letter, and/or these amendments are not signed in verification clearly by the author of the letter; or the letter itself is not signed) business should either not be transacted at all, or should be delayed until the corporate customer is contacted by the cambio and asked to confirm in writing or issue renewed written instructions and the confirmation or renewed instruction is in fact received. Even in the absence of these warning signals cambios should, as a matter of course, employ the practice of conducting random checks with the corporate customer to satisfy itself of the genuineness and accuracy of the transaction to be conducted.

The minimum financial information that cambios should obtain from corporate customers are:-

a) total capital as at the end of the last financial year for the customer;

b) total assets as at the end of the last financial year for the customer;

c) total liabilities as at the end of the last financial year for the customer;

d) change of directors/principals/significant shareholders/ signing officers/ since the completion of the last corporate profile form;

e) main business to be carried out/services to be offered by the customer;

f) purpose of FX activities the company expects to conduct with the cambio i.e. –

   i. Importation of commercial goods;

   ii. Own account investment activities;

   iii. Other (details to be provided as to what the activity entails)

In outlining the purpose of the FX activities to be conducted, a general estimation of the frequency with which the company expects to be conducting or actually conducted these activities for the relevant period to be included e.g. daily; weekly; fortnightly; monthly; bi-monthly; quarterly; bi-yearly; annually; occasionally; or as the need arises.

APPENDIX V. (A)

Terrorist Financing Typologies

Terrorist financing is generally more difficult to detect especially since the funds can arise from seemingly legitimate sources. Appendix V.(A) therefore provides examples of some terrorist financing typologies to aid financial institutions in detecting terrorist financing.

Example 1: The financial intelligence unit (FIU) in Country D received a suspicious transaction report from a domestic financial institution regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an individual from another country. This second person represented a group of companies whose activities focused on hotel and leisure sectors, and he appeared to be the ultimate buyer of the real estate. On the basis of the analysis within the FIU, it appeared that the subject of the suspicious transaction report was acting as a front for the second person. The latter as well as his family are suspected of being linked to terrorism.

Example 2: Abuse of Non-Profit Organisation

A non-profit organisation held an account, over which two locally resident persons held power of attorney. Attention was drawn to transfers made from the account by the fact that the accompanying references were written in Arabic or referred to the term 'Mujahideens'.

Analysis by Law Enforcement showed that the non-profit organisation's account was credited by transfers of small amounts from different persons, for the purpose of donations to the poor in the Middle East.

A number of cash deposits were also received into the account. Some of the funds were subsequently withdrawn in cash.

Police enquiries revealed that the non-profit organisation was the subject of an investigation linked to terrorist financing and that the funds that were raised through this group were sent to military camps in the Middle East. These elements indicated that it was likely that the money raised by this non-profit organisation was used to finance terrorist activities, and the cash withdrawals concealed the trail of the funds, possibly to avoid prosecution.

Example 3: High account turnover indicates fraud allegedly used to finance terrorist organisation

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over USD 17,000 per annum had a turnover in his account of nearly USD 356,000. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate funds collection for a terrorist organisation through a fraud scheme. In Country B, the government provides matching funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into to the account under investigation, and the government matching funds were being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. The charity retained the matching funds. This fraud resulted in over USD 1.14 million being fraudulently obtained. This case is currently under investigation.

Example 4: Diamond trading company possibly linked to terrorist funding operation

The financial intelligence unit (FIU) in Country C received several suspicious transaction reports from different banks concerning two persons and a diamond trading company. The individuals and the company in question were account holders at the various banks.

In the space of a few months, a large number of fund transfers to and from overseas were made from the accounts of the two individuals. Moreover, soon after the account was opened, one of the individuals received several USD cheques for large amounts.

According to information obtained by the FIU, one of the accounts held by the company appeared to have received large US dollar deposit originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but residing in Africa, maintained an account at another bank in Country C. Several transfers had been carried out to and from overseas using this account. The transfers from foreign countries were mainly in US dollars. They were converted into the local currency and were then transferred to foreign countries and to accounts in the Country C belonging to one of the two subjects of the suspicious transaction report.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organisation. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and individuals and companies already tied to the laundering of funds for organised crime. This case is currently under investigation.

Example 5: Frequent cash deposits, mingling, wire transfers and structuring

A subject opened two accounts in different branch offices of the same bank, in Country A where he had no official links. The first account was opened in the name of company X, established in North America, and the second one was opened in the name of company Y, established in another jurisdiction.

Both companies were active in the catering supplies sector and their accounts were mainly credited by significant cash deposits (often for round figures) and to a lesser extent by transfers from abroad by order of companies also active in the catering supplies sector.

The funds were then transferred to other European companies in the same sector.

No business rationale or economic justification could be found for performing these transactions in this manner.

Further enquiries found that the individual concerned was the subject of a terrorism investigation in another jurisdiction. It is suspected that the catering supplies business and the co-mingling may have been a cover for his criminal activities.

Example 6: Use of nominees, trusts, family members or third parties

A political refugee resident in a European country held power of attorney over two accounts (at a bank in that country) in the names of his family members. He did not hold any accounts of his own. One of the accounts exclusively received state assistance benefit payments as the subject was unemployed and had no independent income. The other account was credited by cash deposits. All of the credits were withdrawn via cash machines, thus preventing the identification of the final beneficiary of the money.

Open source checks revealed that the subject had links to a terrorist organisation and further analysis suggested that he was a fund raiser for that organisation.

Example 7: Lack of clear business relationship appears to point terrorist connection

The manager of a chocolate factory (CHOCCo) introduced the manager of his bank accounts to two individuals, both company managers, who were interested in opening commercial bank accounts. The two companies were established within a few days of each other, however in different countries. The first company (TEXTCo) was involved in the textile trade while the second one was a real estate (REALCo) non-trading company. The companies had different managers and their activities were not connected.

The bank manager opened the accounts for the two companies, which thereafter remained dormant. After several years, the manager of the chocolate factory announced the arrival of a credit transfer issued by the REALCo to the account of the TEXTCo. This transfer was ostensibly an advance on an order of tablecloths. No invoice was shown. However, once the account of TEXTCo received the funds, its manager asked for them to be made available in cash at a bank branch near the border. There, accompanied by the manager of CHOCCo, the TEXTCo manager withdrew the cash. The bank reported this information to the financial intelligence unit (FIU).

The FIU's research showed that the two men crossed the border with the money after making the cash withdrawal. The border region is one in which terrorist activity occurs, and further information from the intelligence services indicated links between the managers of TEXTCo and REALCo and terrorist organizations active in that region.

Example 8: Abuse of wire transfers

Mr X, a resident of a European country who originated from the Middle East held a bank account which received significant credits from abroad, which were immediately withdrawn in cash. Mr X stated that the money was from a family member abroad. Apart from these international transfers, the account was also credited with several cash deposits by X a few months later.

Mr X was not known to have any professional activity and received state assistance. He was known to the police for trafficking in humans and terrorism financing. These elements revealed that his account may have been used to place money from trafficking in humans intended for terrorism financing.

Example 9: Abuse of wire transfers and use of false identification.

Two Northern Africans, residing in a European country, repeatedly went to the same exchange office to transfer money to several beneficiaries in the Middle East and Northern Africa. The exchange office thought it was suspicious that they mentioned a different address on the various transfer vouchers and used different signatures when performing the transactions.

The FIU's analysis showed that the transactions took place in the months preceding the attacks on 11 September 2001. Police sources revealed that the individuals were known under different names and that they, together with several other beneficiaries of the transfers, were the subject of an investigation on suspicion of being a member of a terrorist organisation involved in the attacks of 11 September 2001. They have both since been convicted.

APPENDIX V. (B)

Indicators of Suspicious Transactions/ Activity For Terrorist Financing

As a normal part of carrying out their work, financial institutions should be aware of elements of individual transactions that could indicate funds involved in terrorist financing. The following list of potentially suspicious or unusual activities is meant to show types of transactions that could be a cause for additional scrutiny. This list is not exhaustive, nor does it take the place of any legal obligations related to the reporting suspicious or unusual transactions that may be imposed by individual national authorities.

Financial institutions should pay particular attention to:

A. Accounts

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

(7) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(8) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

(9) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

B. Deposits and Withdrawals

(1) Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(2) Large cash withdrawals made from a business account not normally associated with cash transactions.

(3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

(6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

(7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

(8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

C. Wire Transfers

(1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

D. Characteristics of the customer or his/ her business activity

(1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

(3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(4) Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

E. Transactions linked to locations of concern

(1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(6) The opening of accounts of financial institutions from locations of specific concern.

(7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

APPENDIX V. (C)

International Sources of Information on Terrorist Groups/ Individuals

Several sources of information exist that may help financial institutions in determining whether a potentially suspicious or unusual transaction could indicate funds involved in the financing of terrorism and thus be subject to reporting obligations under national anti-money laundering or anti-terrorism laws and regulations. The FIU or other Supervisory Authorities may circulate lists to financial institutions from the sources listed below. However, where such lists may not be forthcoming, the financial institution's compliance framework should include a requirement to check such lists.

A. United Nations List

Committee on S/RES/1267 (1999) website: http://www.un.org/Docs/sc/committees/AfghanTemplate.htm

B. Other Lists

(1) Financial Action Task Force

FATF Identification of Non-Cooperative Countries and Territories

FATF website: http://www.fatf-gafi.org/NCCT_en.htm

(2) United States

Executive Order 13224, 23 September 2001 (with updates)

US Department of the Treasury website: http://www.ustreas.gov/terrorism.html

(3) Council of the European Union

Council Regulation (EC) Nº 467/2001 of 6 March 2001 [on freezing Taliban funds]

Council Decision (EC) Nº 927/2001 of 27 December 2001 [list of terrorist and terrorist organisations whose assets should be frozen in accordance with Council Regulation (EC) Nº 2580/2001]

Council Common Position of 27 December 2001 on application of specific measures to combat terrorism [list of persons, groups and entities involved in terrorist acts]

EUR-lex website: http://europa.eu.int/eur-lex/en/index.html

C. *Standards*

(1) Financial Action Task Force

FATF Special Recommendations on Terrorist Financing

FATF website: http://www.fatf-gafi.org/TerFinance_en.htm

FATF Forty Recommendations on Money Laundering

FATF website: http://www.fatf-gafi.org/40Recs_en.htm

(2) UN Conventions and Resolutions

International Convention on the Suppression of Terrorist Financing

Website: http://untreaty.un.org/English/Terrorism.asp

UN Security Council Resolutions on Terrorism

Website: http://www.un.org/terrorism/sc.htm

(3) Council of the European Union

Council Regulation (EC) Nº 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism

EUR-lex website: http://europa.eu.int/eur-lex/en/index.html

APPENDIX VI:

Website References

Name of Organisation	Website Address / Link
Basel Committee on Banking Supervision	http://www.bis.org/bcbs/
Core Principles for Effective Banking Supervision	http://www.bis.org/publ/bcbs30.pdf
Core Principles Methodology	http://www.bis.org/publ/bcbs61.pdf
Customer Due Diligence for Banks	http://www.bis.org/publ/bcbs85.htm#pgtop
Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering – December 1998	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
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
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 – 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

Name of Organisation	**Website Address / Link**
Wolfsberg Group	http://www.wolfsberg-principles.com/index.html
IDENTIFICATION PROCEDURES Information on the status of sanctions	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-sif.gc.ca.
NON-PROFIT ASSOCIATIONS (INCLUDING CHARITIES)	For a list of all IRS recognized non-profit organizations including charities - www.guidestar.org; list of registered charities go to www.charitycommission.gov.uk.
POLITICALLY EXPOSED PERSONS ("PEPs")	Transparency International Corruption Perceptions Index at www.transparency.org. (b) For information about recent developments in response to PEPs risk- Wolfsberg Group's web site at www.wolfsberg-principles.com.
HIGH RISK COUNTRIES	FATF website at www.fatfgafi.org. Financial Crimes Enforcement Network (FinCEN) www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov/ofac

APPENDIX VII -

Offences and Penalties

Financial Obligations Regulations

A financial institution which does not comply with FOR commits an offence and is liable on summary conviction or on conviction on indictment, to the penalty prescribed in section 57 of POCA.

Where a company commits an offence under FOR, any officer, director or agent of the company:

(i) who directed, authorized, assented to, or acquiesced in the commission of the offence; or

(ii) to whom any omission is attributable, is a party to the offence and is liable on summary conviction or on conviction on indictment, to the penalty prescribed in section 57 of the Act whether or not the company has been prosecuted or convicted.

Where a partnership commits an offence under FOR and it is proved that the partner acted according to paragraph (i) or (ii), the partner and the partnership are liable on summary conviction or on conviction on indictment, to the penalty prescribed in section 57 of POCA.

Where an unincorporated association, other than a partnership, commits an offence and it is proved that an officer or member of the governing body acted according to paragraph (i) or (ii) of that officer or member as well as the unincorporated body, commits an offence and is liable on summary conviction or on conviction on indictment, to the penalty prescribed in section 57 of POCA.

Regulation 40 of the FOR also empowers a Supervisory Authority to take whatever regulatory action is available in the legislation governing financial institutions to ensure compliance with AML/ CTF statutory obligations and requirements.

Proceeds of Crime Act

Everyone who knowingly contravenes or fails to comply with the provisions relating to the compliance programme[53], is guilty of an offence and liable:

(a) on summary conviction, to a fine of five hundred thousand dollars and to imprisonment for a term of two years; or

53 Refer to POCA section 55

(b) on conviction on indictment, to a fine of three million dollars and to imprisonment for a term of seven years.

Where a company commits an offence under POCA any officer, director or agent of the company

who directed, authorised, assented to, acquiesced in or participated in the commission of the offence is a party to, and guilty of, the offence and liable on conviction to the punishment provided for the offence, whether or not the company has been prosecuted or convicted.

Anti-Terrorism Act

Failure of any person who has any information which will assist in:

(a) preventing the commission by another person, of a terrorist act; or

(b) securing the arrest or prosecution of another person for an offence under ATA Act, or an offence under any other law and which also constitutes a terrorist act, to disclose the information to a police officer not below the rank of sergeant or the Central Authority as defined in the Mutual Assistance in Criminal matters Act commits an offence and is liable on conviction on indictment to a fine of ten thousand dollars and to imprisonment for two years[54].

Pursuant to section 33(1) any person who fails to disclose to the FIU:

(a) the existence of any property in his possession or control, which to his knowledge is terrorist property, or which there are reasonable grounds to believe is terrorist property;

(b) any information regarding a transaction or proposed transaction in respect of terrorist property; or

(c) any information regarding a transaction or proposed transaction which there are reasonable grounds to believe may involve terrorist property,

commits an offence and shall on conviction on indictment be liable to imprisonment for five years

A financial institution which fails to report, every three months, to the FIU:

(a) if it is not in possession or control of terrorist property, that it is not in possession or control of such property; or

(b) if it is in possession or control of terrorist property, that it is in possession or control of such property, and the particulars relating to the persons, accounts and transactions involved and the total value of the property,

commits an offence and shall on conviction on indictment be liable to imprisonment for five years

.

In addition to the above requirements, any financial institution which fails to report, to the FIU every transaction which occurs within the course of its activities, in respect of which there are reasonable grounds to suspect that the

54 ATA section 32(1)

transaction is related to the commission of a terrorist act, commits an offence and shall on conviction on indictment, be liable to imprisonment for five years.

The Financial Intelligence Unit Regulations

Section 36 of the FIU Regulations provides that where a financial institution or listed business commits an offence under the Regulations for which no penalty is specified it shall be liable to:-

a) a fine of $500,000 and to a further fine of $20,000 for each day that the offence continues upon summary conviction;

b) a fine of $1,000,000 and to a further fine of $50,000 for each day that the offence continues on conviction on indictment.

The Financial Obligations (Financing of Terrorism) Regulations, 2011

Regulation 8 of the Financing of Terrorism Regulations stipulate that a financial institution or listed business which does not comply with the Regulations commits an offence and is liable on summary conviction or on conviction on indictment to the penalty prescribed in the Anti-Terrorism Act.

Regulation 9 of the Financing of Terrorism Regulations requires that where a company commits an offence under the Regulations, any officer, director or agent of the company –

a) who directed, authorized, assented to, or acquiesced in the commission of the offence; or

b) to whom any omission is attributable,

is a party to the offence and is liable on summary conviction or on conviction on indictment , to the penalty prescribed in the Anti-Terrorism Act.

Regulation 9 also prescribes offences and penalties in respect of partnerships and unincorporated associations.