SUPERVISION GUIDELINE NO. 13

ISSUED UNDER THE AUTHORITY OF THE ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT) ACT 2009

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Bank of Guyana
June 28, 2013

TABLE OF CONTENTS

PART 1 - INTRODUCTION

1.1 INTRODUCTION

This Guideline is issued in accordance with section 22 (2) (b) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009 and section 19 (1) of the AML/CFT Regulations 2010. The Guideline also provides guidance on what is required to implement an adequate AML/CFT compliance risk-based framework within each financial institution (FI).

Money laundering and the financing of terrorism prevention should not be viewed in isolation from an institution's other business systems, but rather as an integral part of its overall risk management strategies. Consequently, it is essential that the board of directors (board) and senior management of a FI ensure that policies, procedures and monitoring mechanisms are put in place to prevent the FI from being used as a conduit for money laundering and terrorist financing.

Effective enforcement of policies to deter money laundering and the financing of terrorism should therefore enhance the integrity of the financial system and reduce incentives for the commission of crime within a jurisdiction.

1.2. PURPOSE

This Guideline seeks to provide FIs with the broad parameters within which to aid its compliance with:

(a) the AML/CFT Act 2009;

(b) AML/CFT Regulations 2010; and

(c) the standards of the Financial Action Task Force (FATF) [1]

It also sets out expectations of the Bank of Guyana (BOG) in relation to the minimum standards for AML/CFT practices by all FIs.

[1] The FATF was established by the G-7 Summit in Paris in July 1989. In 1990, it issued its Forty Recommendations setting out the basic framework for AML efforts. The Forty Recommendations were first revised in 1996 and most recently in 2012 to take into account changes in money laundering methods, techniques and trends that have developed as counter-measures to combat this crime and can be viewed at www.fatf-gafi.org

1.3 MONEY LAUNDERING

Money laundering means conduct which constitutes an offence as described under section 3 of the AML/CFT Act 2009. "A person commits the offence of money laundering if he knowingly or having reasonable grounds to believe that any property in whole or in part directly or indirectly represents any person's proceeds of crime…" With new dirty money constantly being introduced into the financial system, the money laundering process is continuous.

There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. properties, cars and jewellery), to passing money through a complex international web of legitimate businesses and "shell" companies. However, in the case of drug trafficking and other specified serious offences[2] enforceable under the AML/CFT Act 2009, the proceeds usually take the form of cash which needs to enter the financial system.

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:-

(i) **Placement**: refers to the placing of "dirty money" or unlawful cash proceeds into the financial system without arousing suspicion for example via deposits and purchases of monetary instruments such as cheques, or bank drafts.

(ii) **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, travellers' cheques and letters of credit.

[2] See Second Schedule – AML/CFT Act 2009

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

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.

The most common form of money laundering that a financial institution will encounter during the ordinary course of 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.

1.4 FINANCING OF TERRORISM[3]

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. These activities are primarily motivated by ideological or religious beliefs. In contrast, financial gain is the main objective of financial crimes like money laundering. Nonetheless, terrorists[4] and terrorist organizations[5] 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[6].

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 organizations to move, collect, hide or make available funds for their activities are similar to those used by criminal organizations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organization would have similar concerns to a typical criminal organization in laundering the funds. Where the funds are derived from legitimate sources, terrorist organizations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organization and the funds.

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

[3] In October 2001 the FATF expanded its mandate, which was until then limited to money laundering, to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organizations, and are complementary to the Forty Recommendations. In October 2004 the FATF issued a new measure, Special Recommendation IX on Cash couriers.

[4] Refer to AML/CFT Act 2009 – Section 2 (1)

[5] Refer to AML/CFT Act 2009 – Section 2 (1)

[6] Refer to AML/CFT Act 2009 – Section 2 (1)

(travellers' cheques, bank drafts, and money orders), use of credit or debit cards, and wire transfers.

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.[7]

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 organization has opened an account. It is therefore important that LFIs scrutinize circulars, notices, etc both local and international for names of suspicious customers that may be applying for a service from the institution[8]. 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. In this regard, financial institutions should pay particular attention to: -

(a) the nature of the transaction itself;

(b) the parties involved in the transaction; and

(c) the pattern of transactions or activities on an account over time.

It is the Financial Intelligence Unit (FIU), the competent enforcement authority, which 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.

[7] Refer to AML/CFT Act 2009 –Section 68 (1)
[8] Refer to AML/CFT Act 2009 –Section 68 (6)

1.4.1 Sources of Terrorist Financing

Terrorist financing usually comes from 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.

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.

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 organizations. 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.

1.5 APPLICABILITY OF THE GUIDELINE

This Guideline applies to institutions licensed under:-

(a) the Financial Institutions Act, 1995 (FIA);

(b) the Money Transfer Agencies (Licensing) Act 2009; and

(c) the Dealers in Foreign Currency (Licensing) Act 1989.

Hereinafter in this Guideline, these institutions will be collectively referred to as financial institutions.

All financial institutions listed under (a), (b) and (c) should ensure that, at a minimum, this Guideline is also implemented in their branches/subsidiaries abroad. Where the local applicable laws and regulations prohibit the implementation of this Guideline, the BOG must be notified.

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

Where Guyana's AML/CFT requirements exceed those in the host jurisdiction, subsidiaries and branches of the financial institution in those jurisdictions should apply the higher standard to the extent that the host jurisdiction laws and regulations permit.

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/CFT laws, regulations, and Guidelines.

Financial institutions should be required to pay particular attention that the principle stated in section 22 (2) of the AML/CFT Act 2009 is observed with respect to branches and subsidiaries in countries which do not or insufficiently apply the FATF recommendations.

PART 2 – LEGISLATIVE AND REGULATORY FRAMEWORK

2.1 Legislative

The AML/CFT Act 2009 and Regulations 2010 provide the legal framework for detecting and preventing money laundering and terrorist financing.

- Section 22 (1) (a) of the AML/CFT Act 2009 stipulates that the Governor of the BOG is the Supervisory Authority of the financial institutions named therein.
- Section 9 of the AML/CFT Act 2009 speaks to the establishment and functions of the FIU.
- With respect to the FIs, sections 15,16,18,19 and 20 of the AML/CFT Act 2009 speak to the following:-

    (a) identifying and verification of a customer's identity;

    (b) reporting obligations;

    (c) appointment and duties of a Compliance Officer;

    (d) attention to and reporting, if suspicious, of large business transactions which are unusual and complex, as well as transactions which have no apparent economic or visible lawful purpose and are inconsistent with the profiles of the persons carrying out such transactions;

    (e) making a suspicious transaction or a suspicious activity report to the FIU;

    (f) recordkeeping;

    (g) training of employees in AML/CFT.

2.2. Regulatory Framework

The primary responsibilities of the BOG as a Supervisory Authority include:-

(a) reviewing the AML/CFT compliance programme of all financial institutions to determine its adequacy and assess its compliance with applicable laws and Guidelines and AML/CFT measures consistent

with FATF Recommendations to the extent that host countries laws and Regulations permit ;

(b) issuing Guidelines,[9] circulars or recommendations as appropriate to aid compliance with AML/ CFT requirements;

(c) cooperating and sharing information promptly with other competent domestic authorities, by requesting and providing assistance in investigations, prosecutions or proceedings relating to proceeds of crime, money laundering and terrorist financing;

(d) taking regulatory action against those institutions and persons regulated by it which fail to adequately comply with statutory AML/CFT obligations and Guidelines issued by the BOG;

(e) sharing of information with the FIU as required for the purposes of AML/CFT. This includes disclosing information to the FIU as soon as is reasonably practicable but no later than three working days after acquiring any information concerning suspicious transactions or activities that could be related to money laundering, terrorist financing or the proceeds of crime;

(f) maintaining statistics concerning measures adopted and sanctions imposed under the Act;

(g) developing standards and criteria applicable to the communication of suspicious activities that reflect other existing and future pertinent national and internationally accepted standards;

(h) ensuring that financial institutions as it relates to their foreign branches/subsidiaries implement and enforce standards consistent with the AML/CFT Act, Regulations, guidelines or directives. The BOG should be duly notified in cases where the foreign branches/subsidiaries are unable to implement and observe these standards; and

(i) sharing of information with agencies in other jurisdictions with similar functions as it relate to investigations, prosecutions pertaining to the

[9] Refer to Section 22 (1) of the AML/CFT Act 2009 and Section 13 of the AML/CFT Regulations 2010

proceeds of crime, money laundering, terrorist financing, and violations of the law and regulations dealing with financial institutions.

Regulatory actions[10] that could be taken by the BOG include:

(a) the issuance of written warnings;
(b) compliance orders with specific instructions;
(c) suspension, restriction or revocation of licence;
(d) prohibiting convicted persons from gaining employment within the sector;
(e) requesting regular reporting from the financial institution on the measures it is taking to comply with the law.

The BOG is required to inform the FIU as to the sanctions imposed and may publish its decision.

2.3 ENFORCEMENT OF THE GUIDELINE

Section 19 of the AML/CFT Regulations 2010 makes the failure to comply with the requirements of the Guideline a summary conviction offence. The Courts by Regulation 19 may also take account of the provisions of the Guideline in determining whether there has been compliance with the requirements of the AML/CFT Regulations. FIs are therefore advised to adopt the provisions of this Guideline and to implement the requisite internal systems and procedures.

2.4 LEGAL PROTECTION AND INDEMNIFICATION[11]

When a suspicious transaction or suspicious activity report is made to the FIU in good faith, financial institutions their employees, officers, directors, owners or other representatives as authorized by law, are exempted from criminal, civil or professional liability action 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, who in good faith transmit information or submits reports to the FIU regardless of the result of the communication.

[10] Refer to AML/CFT Act 2009 –Section 23 (1)
[11] Refer to AML/CFT Act 2009 – Section 11 (1) & (2)

2.5 TIPPING OFF[12]

It is an offence 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; or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

In the event that a person is found guilty of tipping off he/she may, on conviction, be liable to a fine not exceeding one million dollars and to imprisonment for a term not exceeding 3 years.

[12] Refer to AML/CFT Act 2009 –Section 5 (1) & (2)

PART 3 – RESPONSIBILITY OF FINANCIAL INSTITUTION

3.1. THE RESPONSIBILITY OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

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

Directors and senior management should be aware that:

(a) subsidiaries and branches of financial institutions including those that may be domiciled outside of Guyana are expected to, at a minimum, comply with the requirements of the AML/CFT Act, Regulations, and this Guideline; and

(b) where some of financial institution's operational AML/CFT functions may be outsourced, the financial institution retains full responsibility for compliance with local laws, regulations and Guidelines.

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

(a) understanding the statutory duties placed upon them, their staff and the entity itself;

(b) approving AML/CFT policies and procedures that are appropriate for the risks faced by the licensee;

(c) ensuring that the institution appoints a Compliance Officer in accordance with section 19 (1) of the AML/CFT Act and section 14 (1) of the Regulations;

(d) ensuring that the financial institution is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports

from the Compliance Officer, internal audit, external auditors and supervisory authority on the operations and effectiveness of compliance systems.

Senior management in collaboration with the Compliance Officer is responsible for the development of sound risk management programmes and for keeping directors adequately informed about these programmes and their effectiveness. These programmes should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments.

Financial institutions should formally document policies and procedures which at a minimum, should provide for:

(a) the development of internal policies, procedures and controls for, inter alia:

  (i) the opening of customer accounts and verification of customer identity;
  (ii) establishing business relations with third parties (correspondent banks, business introducers);
  (iii) determining business relationships that the financial institution will not accept;
  (iv) the timely detection of unusual and suspicious transactions, and reporting to the Authority;
  (v) internal reporting; and
  (vi) record retention.

(b) the recruitment of staff, appropriate to the nature and size of the business, to carry out the AML/CFT compliance function;

(c) an on-going training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers they and the financial institution face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;

(d) the appointment of a Compliance Officer at an appropriate level of authority, seniority and independence to, inter alia, coordinate and monitor the

compliance programme, receive internal reports, and issue suspicious transaction reports to the FIU;

(e) establishment of management information/reporting systems to facilitate aggregate and group/branch wide monitoring;

(f) an effective independent risk-based oversight function to test and evaluate the compliance programme; and

(g) screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the financial institution from being used for criminal activity.

Policies should be periodically reviewed for consistency with the business model, and changes and developments in the financial institution's products and services. Special attention should be paid to emerging technologies and new payment products as well as trends in money laundering and terrorist financing.

3.2 DEVELOPING A RISK-BASED FRAMEWORK

The FATF in its revised Forty Recommendations plus nine Special Recommendations on AML/CFT 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 a customer's identity based on the nature and degree of risk inherent in the customer relationship.

Each financial institution should develop and implement a risk-based framework in its AML/CFT programme which should be approved by its BOD and which is 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 examination, the BOG will assess the adequacy of the institution's risk rating policies, processes and procedures, as it relates to the type of business conducted, as well as compliance with legislative requirements.

The risk rating framework should include at a minimum:

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, type and volume of transactions, and conformity 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 customer risk ratings.

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 customer 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 or the board of directors as to whether the relationship should be discontinued. All decisions regarding discontinuation of business with high risk customers should be documented.

The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason(s) for such change(s). 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 area of the customer's business activities including the location of the counterparties with which the customer conducts business, and whether the customer is otherwise connected with certain high risk jurisdictions, or those known to the institution to lack proper standards with respect to AML/CFT.

(c) the nature of the customer's business (whether cash intensive e.g. casinos, supermarkets, retail/wholesale outlets) which may be particularly susceptible to money laundering or terrorist financing risk;

(d) the nature and frequency of activity. This should include the pattern of account activity, the complexity, volume and pattern of transactions given the institution's information on the customer and or his business;

(e) the type of customer, i.e. whether a trust or politically exposed person (PEP), or whether the customer's employment income supports the account activity;

(f) delivery channels used for transactions (e.g. internet banking, wire transfers to third parties, remote cash withdrawals from branches that are geographically distant from customer's place of business or home);

(g) the unwillingness of the customer to cooperate with the institution's customer due diligence (CDD) 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 (e.g. private banking, mortgage, one-off transaction);

(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 previously dormant is now being reactivated with large cash inflows; and

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

3.2.1 Prospective Customers

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

3.2.2 Existing Customers

Financial institutions are required to risk rate all existing customers' relationships including those in existence prior to the implementation of this Guideline. Financial institutions should review the KYC documentation in relation to their existing customers to ensure compliance with the AML/CFT Act 2009 and the financial institution's internal KYC requirements. All risk ratings should be documented.

3.3 Risk management

3.3.1 Implementing a Compliance Programme

Financial institutions have a statutory obligation to implement robust compliance programmes to prevent money laundering and terrorist financing[13]. The minimum elements of a compliance programme are outlined in section 19 of the AML/CFT Act 2009 and section 14 (1) of the AML/CFT Regulations 2010. As a general rule, the compliance function should provide an independent evaluation of the financial institution's compliance with all relevant sections of the AML/CFT Act, Regulations and Guideline.

Despite the implementation of AML/CFT policies and procedures, common barriers may hinder an effective organizational system of AML/CFT control. Financial institutions need to recognize and address them. The human element is very important in this context in that policies and procedures only work if they are understood, followed and enforced by those required to comply with them. Sometimes referred to as 'human factors', the inter-relationships between different employees within a financial institution and between employees and customers, can result in the following damaging barriers:

[13] Refer to AML/CFT Act 2009 – section 19 and section 14 (1) of the AML/CFT Regulations 2010

(a) senior management being unwilling to lead on the concept of the need for sound corporate ethics;

(b) more junior employees assuming that their concerns or suspicions are not significant;

(c) employees being unwilling to subject high value (therefore important) customers to effective CDD checks;

(d) management or customer relationship managers placing pressure junior employees to process transactions without obtaining all relevant CDD and business information;

(e) employees being unable to understand the linkages between customer relationships, so that potentially suspicious activity is not recognized;

(f) lack of time and/or resources to address concerns generating a tendency for managers to discourage employees from raising concerns;

(g) conflict between the desire on the part of employees to provide a confidential and efficient customer service and the requirement for employee vigilance in respect of money laundering and terrorist financing prevention and detection;

(h) lack of proper staff training.

Policies and procedures must be documented and the board and senior management must, therefore, identify and take appropriate steps to resolve these barriers if they are to implement effective AML/CFT policies.

3.4 The Role of Internal and External Audit

Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. 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 BOG have been satisfactorily addressed. Management should ensure that the internal audit function is adequately resourced and implemented with individuals who are knowledgeable of AML/CFT policies and procedures and that compliance testing of procedures, policies and controls include sample testing. In addition, internal auditors should be proactive in following-up their findings.

External auditors also have an important role to play in monitoring FIs internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

3.5 THE COMPLIANCE OFFICER

It is important and imperative that the Compliance Officer appointed by the financial institution has the necessary knowledge, expertise and required authority to effectively discharge assigned responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations, and the latest developments in money laundering and financing of terrorism techniques. The Compliance Officer should be appointed at a management level and the financial institution should inform immediately the BOG in writing and submit a Personal Declaration Sheet (PDS) to the BOG at the earliest opportunity.

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.

At a minimum, the Compliance Officer must be appointed and perform the functions and duties in accordance with section 19 of the AML/CFT Act 2009 and section 14 of the AML/CFT Regulations 2010.

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 an STR to the FIU.

Further, where a financial institution has less than five employees, as may be the case with a cambio or money remittance business, it is prudent to have someone designated as responsible for AML/CFT compliance.

The Compliance Officer should have the authority and the resources necessary to effectively discharge responsibilities. To ensure consistent and ongoing attention to the compliance regime, the appointed officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a branch to ensure that compliance procedures are properly implemented at that location. However, the appointed compliance officer remains responsible for the firm's overall compliance program and its effectiveness. It is also recommended that the financial institution identify a Deputy, who should be a staff member of similar status and experience to the Compliance Officer, and who must be able to conduct all functions of the Compliance Officer in his/her absence.

The Compliance Officer should:

(i) undertake responsibility for developing internal policies, procedures, controls and systems for an effective AML/CFT compliance programme within the financial institution;

(ii) develop and maintain AML/CFT guidelines for the financial institution in relation to the business of the institution;

(iii) implement the customer identification requirements;

(iv) implement record keeping and retention requirements;

(v) monitor compliance with the financial institution's internal AML/CFT programme;

(vi) receive internal reports and consider all such reports;

(vii) prepare and submit written suspicious transactions reports to the FIU as soon as practicable after determining that a transaction warrants reporting. Such forms should be prepared in the specified format as the FIU may determine;

(viii) monitor the accounts of persons for whom a suspicious report has been made;

(ix) establish and maintain an on-going awareness programme for the officers and employees of the financial institution's AML/CFT internal policies and procedures and conduct training programmes for staff at all levels to recognize suspicious transactions;

(x) establish standards for the frequency and means of training;

(xi) conduct a self-assessment and report to the board of directors (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat money laundering and the financing of terrorism;

(xii) review compliance policies and procedures to reflect changes in legislation or international developments, non-compliance and new services or products. It is essential that the scope and the results of the review be documented. Deficiencies should be identified and reported to senior management and the Board of Directors, and corrective actions taken to address these deficiencies in a timely manner;

(xiii) participate in the approval process for high-risk business lines and new products, including those involving new technologies;

(xiv) screen persons before employing them in the compliance department;

(xv) act as the Liaison between the financial institution and the BOG and/or FIU on matters pertaining to compliance with the AML/CFT function.

3.6 PRE-EMPLOYMENT BACKGROUND SCREENING / KNOW YOUR EMPLOYEE (KYE)

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. The ability to implement an effective AML/ CTF programme depends in part on the quality and integrity of staff. 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-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual staff member may warrant additional background screening, which should include verification of references, experience, education and professional qualifications, details of any criminal convictions etc;

(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. code of conduct) 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.

3.6.1 Staff Training and Awareness

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analyzing potential illicit transactions. Therefore, financial institutions should establish on-going employee training programmes, which shall include new developments including information on current money laundering and financing of terrorism techniques, methods and trends; clear explanations of all aspects of AML/CFT laws and obligations and in particular requirements concerning CDD.

The effectiveness of the procedures and recommendations contained in this Guideline depends on the extent to which staff of financial institutions appreciates the serious nature of the background against which this Guideline has been issued. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to cooperate fully and to provide a prompt report of any unusual or suspicious transactions without fear of reprisal.

Training should be targeted at all employees but added emphasis should be placed on the training of the Compliance Officer and the compliance and audit staff because of their critical role in sensitizing the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures. Additionally, front line staff should be targeted so as to enable them to respond appropriately when interacting with the public.

At a minimum, a financial institution is required to:

(i) develop an appropriately tailored training and awareness programme consistent with its size, resources and type of operation to enable its employees to be aware of the risks associated with money laundering and terrorist financing. The training should also ensure employees understand how the institution might be used for money laundering or terrorist financing, enable them to recognize and deal with potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;

(ii) document, as part of its AML/ CFT policy document, its approach to training, including the frequency, delivery channels and content;

(iii) 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;

(iv) establish and maintain a regular schedule of new and refresher programmes, including new developments and current techniques appropriate to the risk profile of the organization, for the different types of training required for:

(a) new employees;

(b) operations staff;

(c) supervisors;

(d) board and senior management; and

(e) audit and compliance staff.

(v) obtain an acknowledgement from each staff member on the training received;

(vi) assess the effectiveness of training; and

(vii) 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.

(viii) clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious transaction reporting.

PART 4 – KNOW YOUR CUSTOMER (KYC)

4.0 KYC STANDARDS

The essential elements of KYC standards should start from the financial institution's risk management and control procedures and should include the following:

(i) customer acceptance policy,

(ii) customer identification,

(iii) ongoing due diligence (monitoring) of accounts and transactions

4.1 Customer Acceptance Policy

Financial institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a financial institution. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

Financial institutions should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, enhanced due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons should be taken exclusively by the Compliance Officer or at senior management level.

When considering whether to enter into a business relationship with a customer acting on behalf of another person, the financial institution shall establish the true identity of the person on whose behalf or benefit the customer may be acting in the proposed transaction, whether as a trustee, nominee, agent or otherwise and to ascertain that the customer is authorized to do so.

Financial institutions are also prohibited from establishing or keeping anonymous accounts, numbered accounts alone or accounts in fictitious names. 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.

4.2 Customer Identification

4.2.1 General Identification Requirements

Customer identification is an essential element of KYC standards. According to Regulation 4 (2) customers shall include, inter alia persons whether natural, legal or legal arrangements who are or who seek to be-

(a) in a business relationship with the FI;

(b) engaged in one or more occasional transactions with the FI when the total value of the transactions equals or exceeds one million dollars.

The customer identification process applies at the outset of the relationship, and in instances as specified in section 15 (3) of the AML/CFT Act 2009 and Regulation 4 (3). A financial institution must document and implement adequate policies and procedures to establish and verify the identity including proof of address of an individual or business customer or those acting on their behalf in accordance with section 15 of the AML/CFT Act, and should not establish a relationship until the identity of a new customer is satisfactorily verified.

Financial institutions need to obtain all information necessary to establish to their full satisfaction, the identity of each new customer and the purpose and intended nature of

the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

For existing accounts, if problems of verification of identification and proof of address arise in the banking relationship the bank should terminate the relationship.

4.2.2 Verification of KYC Details

The onus is on the financial institution to verify the customer's identity and to be satisfied that a prospective customer is who he claims to be prior to establishing a business relationship.

Satisfactory evidence of identity according to Regulation 2 (2) (b) shall be determined by the FIU and includes among others:

(i) the production of an official or identifying document, one of which shall be a national identification card or passport;

(ii) proof of address.

For a document to be considered adequate as evidence of proof of address it must be a document issued or obtained from an independent and reliable source. The proof of address must be of such a nature that it would eliminate as reasonably practicable, any suspicion of counterfeiting or being obtained illicitly. The document obtained should be current, i.e issued within the last 6 to 8 months.

Where doubt exists, the name and permanent address and employment/business details of a customer should be verified by an independent source, other than those provided by the customer, as per the following examples:

(a) a current utility bill for the customer's place of residence or business. In some cases where the customer is considered low-risk a bank statement from another bank may be used but it is strongly recommended to guard against forgeries that only originals should be accepted;

(b) independent confirmation of national identifications with the relevant government authorities;

(c) independent confirmation of customer's stated place of employment, salary and benefits with the employer;

(d) cross-checking KYC details with other financial institutions or businesses. In so doing financial institutions will need to be guided by the respective agreements with the customer which should ideally reflect that the customer's consent has been obtained to do this type of check;

(e) cross-checking KYC details for one account holder with the other holder of the account;

(f) cross-checking KYC details provided with other affiliated companies. (In so doing financial institutions will need to be guided by the respective agreements with the customer which should ideally reflect that the customer's consent has been obtained to do this type of check.); and

(g) Credit Bureau.

In respect of joint personal accounts, the names and addresses of all account holders should be obtained and verified.

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

(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 material change in the operation of a business relationship;
(d) a new product or account being established within an existing relationship;
(e) a change in an existing relationship which increases a risk profile; and
(f) the assignment or transfer of ownership of any product.

When an existing customer closes one account and opens another, good practice requires that the details on the customer's file be reconfirmed. This is particularly important if there has been no recent contact with the customer e.g. for the past twelve months. Details of the previous accounts and steps originally taken to verify identity or any introduction records should be transferred to the new account records.

4.2.3 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 original documents, a copy is acceptable where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the account holder.

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

4.2.4 Specific Identification and Verification Procedures

(a) Natural Persons (Individual Customers)

A financial institution should obtain relevant information on the identity of its customer and seek to verify some of the information on a risk basis, through the use of reliable, independent source documents, data or information to prove to its satisfaction that the individual is who that individual claims to be.

The basic information should include but not be limited to:

(a) the person's true name. The institution may want to include maiden names for married women and aliases as this may also be helpful in locating the customer at a later time;

(b) date of birth. Recording a customer's date of birth provides an extra safeguard if for example a forged or stolen passport or identification card is used to confirm the identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document;

(c) proof of residential and/or business address. P.O. box addresses are usually not acceptable. The residential or business address of a relative can be collected in cases where the customer resides with a relative. The relationship between the customer and the relative should be ascertained and noted on the financial institution's records. Additionally only the customer or someone authorized by him should be allowed to change the address on the account and this should be documented;

(d) current valid photo-bearing identification such as the national identification card, passport or other applicable official identifying document;

(e) contact details e.g. telephone numbers (home and cell), fax number and e-mail address;

(f) purpose of the account and nature of the business relationship;

(g) business registration (if any);

(h) residence and Nationality (if dual, should be indicated). 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[14];

(i) signature;

(j) occupation/name of employer;

(k) recent financial statements/current pay slip;

(l) taxpayers identification number (TIN) certificate.

The examples quoted above are not the only possibilities that can be used to verify a customer's identity. In addition, the institution may obtain any other information deemed appropriate and relevant e.g. source of funds, source of wealth if the customer is considered high risk, estimated account turnover, birth and marriage certificates, character references preferably from a reputable person in society or any other reliable independent source documents.

In cases where the customer is unable to produce the identification described at item 4.2.4 above, the financial institution will need to determine whether it should exercise its discretion to facilitate the transaction on the basis of alternative forms of identification such as an affidavit of identity.

The discretion lies with the financial institution in deciding what other forms of identification may be appropriate for the verification of a customer's identity. Whatever the other alternative forms accepted by the institution it remains that these should beyond a reasonable doubt establish the customer to be who he is.

Where prospective customers provide documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take

[14] This information would also assist in the identification of US citizens

reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining notarized copies.

The underlying principles of customer identification for natural persons (individual persons) have equal application to customer identification for all types of business relationships.

(b) Non-Resident Natural Persons (Individual Customers)

Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The identification requirements for natural persons resident in Guyana also apply to natural person's resident outside of Guyana. Financial institutions are required to obtain the same identification documentation or their equivalents for prospective customer's resident outside of Guyana. Institutions should exercise due caution when accepting certified copies of documents, especially where such documents originate overseas and especially from a country perceived to represent a high risk, with weak or nonexistent AML/CFT programmes. Where certified copies of documents are accepted, it is the institution's responsibility to satisfy itself that the certifier[15] is authentic. In all cases, institutions should also ensure that the customer's signature is the same on all the identification documents presented.

Financial institutions should also ascertain why a non-resident customer has chosen to open an account in the local jurisdiction.

Institutions should also exercise particular care when dealing with overseas counterparties or financial institutions acting for overseas customers, where to the local financial institution's knowledge, the overseas counter-party or representative financial institution is not subject to AML/CFT laws and regulatory arrangements. Additionally, financial institutions should carefully scrutinize any transaction proposed to be carried

[15] Preferably certified by the customer's bankers overseas or by an official from the Guyanese Consulate in the country where the customer resides abroad if one is located there.

out with any customer, counter-party or banking institution situated in a jurisdiction with weak or nonexistent AML/CFT programmes.

(c) Persons without Standard Identification Documentation

There may be circumstances where some types of customers are unable to provide the usual types of identification. Such customers include the elderly, the disabled, students, and individuals dependent on the care of others. In other instances the identification document may have expired or have been lost. Internal procedures must allow for this, and must provide appropriate advice to staff on how a customer's identity can be confirmed in these exceptional circumstances. In particular, a common sense approach and some flexibility without compromising rigorous AML/CFT procedures are recommended. A financial institution may determine what alternate identity documentation to accept and the verification process to employ.

The important point is that a person's identity can be verified from an original or of another document, preferably one with a photograph. Financial institutions must also retain this information in the same manner and for the same period of time as other identification records. Where a proposed facility holder's address is a temporary accommodation, for example an expatriate or foreign national on a short term contract, financial institution's should adopt flexible procedures to obtain verification under other categories, such as copy of contract of employment, or employer's written confirmation in addition to a copy of the customer's passport.

(d) Minors or other young people

Under normal circumstances, an account for a minor will be opened by the child's parents, a close family member such as grandparents or a guardian who may already have an existing relationship with the financial institution. In cases where the adult opening the account is not already known, the identity and requisite information of that person, and any other person who will have control of the account, should be taken and verified. In addition the birth certificate or passport of the child should be obtained. It should be noted that this type of account could be open to abuse and therefore strict monitoring should be undertaken and maintained.

(e) Locally Incorporated Companies (LICs)

Financial institutions should be vigilant when dealing with LICs as they may be used by natural persons as a method of ensuring anonymity. In all cases the financial institutions should fully understand the structure of the prospective LIC, the source of funds and the beneficial owners and controllers and who has ultimate control over the business and its assets. Particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Special care should be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals.

Where a company is listed on a recognized stock exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration should be given to whether there is effective control of a listed company by an individual, small group of individuals or another corporate entity or trust. If this is the case then those controllers should also be considered to be principals and identified accordingly.

This should be the case whether the corporate customer is locally incorporated or a foreign company.

With regard to LIC, financial institutions should obtain and verify:-

(a) Name of the corporate entity;

(b) The identity of those who ultimately own or have control over the company's business and assets, more particularly -

(i) their directors. For non-resident directors documents should be authenticated by their overseas bankers or a representative of the Guyana consulate if there is one in that country;

(ii) their significant shareholders. If the company is publicly listed on a recognized stock exchange and not subject to

effective control by a small group of individuals, identification of shareholders is not required;

(iii) their authorized signatories.

(c) with respect to employees authorized to open and operate accounts for an LIC, the same documents required for the identification of a personal customer should be obtained and retained;

(d) address of the principal place of business and registered office;

(e) LIC's business and mailing address, telephone, fax numbers and email address.

(f) description and nature of business including the products and services offered.

(g) purpose of the account, source of funds and the estimated account activity (turnover);

(h) source of wealth of the LIC where that customer is considered high-risk;

(i) tax compliance certificate;

(j) official documents which collectively establish the legal existence of that entity e.g. certified copies of the certificate of incorporation of the company, memorandum of association and certificate of incorporation details of its registered office and place of business etc.

(k) financial institution's mandate, signed application form, or other account opening authority containing specimen signatures and signing authority on the account.

(l) financial statements for the company may be requested if applicable;

(m) a certified copy of the resolution of the BOD or managing body and the power of attorney granted to its employees to open and to operate accounts on their behalf;

(n) character references for directors;

(o) directors' Resolution authorizing company's management to establish an account with the financial institution and engage in transactions and the authorised signatures and signing authority.

In addition, the institution may obtain any other information deemed appropriate and relevant in establishing the veracity of the customer. Only authorised signatories on the account may make changes to the account.

Enquiries should be made to confirm:

(i) with the Registrar of Companies that the LIC continues to exist and has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;

(ii) in cases of doubt where appropriate a visit to the place of business of the LIC, to verify that there is an actual physical presence and that the LIC exists for a legitimate trading or economic purpose.

As with personal accounts, 'KYC' is an ongoing process. Where doubt exists financial institutions should make enquiries to confirm that the company exists for a legitimate trading or economic purpose, and where appropriate, visit the business/company to ensure that there is an actual physical presence before establishing the account. If changes to the company structure or ownership occur subsequently or suspicions are aroused by a change in the nature of business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

(f) Foreign Companies

Where the applicant for business is a foreign company, the same documents required for locally incorporated companies should be requested and retained. The financial institution should ensure that the company is duly registered in Guyana before entering into a business relationship with the customer.

In addition financial institutions may check the veracity of the information provided with a credit or financial institution of good standing in the home country. Financial institutions may also rely on other regulated institutions or intermediaries to verify the identity of foreign companies, in accordance with section 15 (8) of the AML/CFT Act 2009.

The identification requirements at items (a) to (o) under LIC would be applicable to foreign companies.

(g) Partnership/Unincorporated Business

In the case of a partnership, each partner/controller and authorized signatories should be identified as well as the ownership control. The identity of each partner and their authorized signatories should be verified in accordance with procedures required for the identification of natural persons, and the same documents as are required for natural persons should be requested and retained.

In addition to providing the identification documentation for partners/controllers and authorized signatories, where a formal partnership arrangement exists, there should be a mandate from the partnership authorizing the opening of an account or any other facility and the authorized signatories who will undertake transactions. When partners/controllers and authorized signatories change, care should be taken to ensure that the identities of the new partners/controllers and current signatories are verified.

The following information may also be required when financial institutions seek to verify the identity of partnerships and unincorporated businesses:

(a) Description and nature of the business
(b) Date of commencement of business
(c) Products or services provided
(d) Location of principal place of trading business;
(e) Reason for establishing the business relationship
(f) An indication of expected transaction (turnover) volume of the account;
(g) The source of wealth in circumstances where the financial institution's customer is considered a high risk client;
(h) The source of funds
(i) A copy of the last available financial statements where appropriate
(j) A copy of the partnership agreement (if any) or other agreement establishing the unincorporated business.

(k) Sole proprietor registration

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

(m) Financial institution's Mandate, signed application form, or other account opening authority containing specimen signatures and signing authority on the account if there are more than one beneficial owner.

(h) Powers Of Attorney

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. Powers of Attorney should be in force and should be authenticated by the Registrar of Deeds, Deeds Registry Guyana. In addition, Powers of Attorney issued overseas must be registered at the Deeds Registry, Guyana and should be in force. Due diligence must be taken by the financial institution to guard against forgeries. Copies of the Power of Attorney and records of all transactions undertaken in accordance with a power of attorney should be kept in accordance with the record keeping procedures of this Guideline.

(i) Foreign Consulates

The authenticity of applicants that request to open accounts or undertake transactions in the name of Guyanese resident foreign consulates and any documents of authorization presented in support of the application should be checked with the Ministry of Foreign Affairs or the relevant authorities in the Consulate's home country.

4. 3 Ongoing Due Diligence (Monitoring) of Accounts and Transactions

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 such as with cash intensive businesses require ongoing due diligence and the continuous review and intensive monitoring of

transactions. The purpose of this monitoring is for financial institutions to be vigilant for any significant changes in the pattern of transactions and any unusual or suspicious activity and to maintain up to date records[16].

Financial institutions should consider monitoring by: -

(a) Transaction type;
(b) Frequency;
(c) Amount;
(d) Geographical origin/ destination;
(e) Account signatories.

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 computerized and manual human solutions. The financial institution should have in place an adequate management information system to complement its customer due diligence.

The management information system should provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect any suspicious activity. Such information would include multiple transactions over a certain period, large transactions, anomaly in transactions pattern and transactions exceeding any internally specified threshold.

It should be noted that failure to adequately monitor customers' activities could expose a financial institution to potential abuse by criminals, and may call into question the adequacy of systems and controls, or the prudence and integrity of the management of the financial institution.

[16] Refer to AML/CFT Act 2009 –Section 16 (5)

PART 5 – DUE DILIGENCE / HIGH RISK

5.1 CUSTOMER DUE DILIGENCE (CDD)

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

CDD policies and procedures should however, not only be geared toward the timely prevention and detection of money laundering and terrorism financing activities, but must also form a fundamental part of the financial institution's overall risk management and internal control systems. It must contain a clear statement of management's overall expectations and establish specific lines of responsibilities not only at the point of the institution's first contact with the customer, but throughout the business relationship. Policies and procedures should be properly documented and clearly communicated to all relevant staff.

This is essential, as inadequate CDD standards can result in undue risk exposures, particularly as they relate to reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to financial institutions (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

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

(a) identify and verify a customer's identity using reliable, independent source documents, data or information prior to establishing a business relationship.

(b) identify the beneficial ownership and control structure of the customer and take reasonable measures to verify the identity of the beneficial owners[17] and

[17] "Beneficial owner" is defined in the FATF 40 Recommendations as a natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

controllers such that a financial institution is satisfied that it knows who the beneficial owners and controllers are.

(c) gather information on the nature of the customer's business, economic circumstances, purpose and intended nature of the business relationship. 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) and source of funds to be used during the relationship should be provided.

(d) obtain information on the type, volume and value of the activity that can be expected within the relationship. Where major changes have been noted, an explanation should be sought from the customer for these changes.

Once a business relationship has been established, ongoing due diligence on the business relationship and scrutiny of transactions should be undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile.

5.2 ENHANCED DUE DILIGENCE (EDD)

Financial institutions are required to perform enhanced due diligence for higher risk customers. Such measures shall be on a risk sensitive basis for categories of customers, business relations or transactions as the financial institution may assess to present a higher risk for money laundering or terrorist financing. A financial institution may conclude, under its risk based approach, that a customer is high risk because of the following:

(i) the customer's business activity;

(ii) ownership structure;

(iii) nationality;

(iv) residence status;

(v) countries the customer is doing business with. 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. In some cases it may be necessary to refuse the business relationship from the inception because of the higher risk involved;

(vi) anticipated or actual volume of transactions;

(vii) types of transactions.

The extent of additional information sought and any monitoring carried out in respect of any particular customer or class/category of customer, will depend on the money laundering or terrorist financing risk that the customer poses to the financial institution and the product or service being sought 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.

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

(i) where a customer has not been physically present for identification purposes;
(ii) correspondent relationship;
(iii) a business relationship or occasional transaction with a PEP;
(iv) business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML/CFT measures;
(v) corporate customers able to issue bearer shares or bearer instruments;
(vi) cash transactions in excess of two million dollars.

In addition the reporting institution should establish internal criteria (red flags) to detect suspicious transactions. The reporting institution should be prompted to conduct

enhanced due diligence if any transaction matches the red flags list. Transactions that match the red flags should be subjected to on-going monitoring.

5.3 HIGH RISK CUSTOMERS

High-risk customers should be identified by the Compliance Officer or senior management and stringent documentation, verification and transaction monitoring procedures should be established. Enhanced due diligence for such customers should be considered where deemed relevant:-

(i) an evaluation of the principals
(ii) a review of the current financial statements
(iii) verification of the source of funds/wealth
(iv) the conduct of reference checks
(v) checks of electronic databases, government lists and
(vi) periodic reporting to the BOD about high risk accounts.

5.3.1 Trust, Nominee and Fiduciary 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 and to circumvent customer identification procedures. The principal means of preventing money laundering or terrorist financing 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 original Trust Deed;
(b) the nature and purpose of the trust; and
(c) verification of the identity of the trustee.

The financial institution should also obtain the following:

(a) name of trust;
(b) the source of funds;
(c) country / date of establishment;
(d) documentary evidence similar to that required for Natural Persons on the identity of the trustee(s), settlor (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 subparagraphs (a), (b), (c) or (d): and
    (vi) 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 controllers should be undertaken 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.

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 as far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection.

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.

5.3.2 Non Profit Organizations (NPOs) such as Clubs, Societies and Charities

NPOs may be vulnerable to abuse by terrorists and money launderers for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. 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" and typically depend in whole or in part on charitable donations and voluntary service for support.

Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity.

NPOs differ in size, income, structure, legal status, membership and scope and 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.

It is at the placement stage that there may be difficulties in identifying the source of funds, identity of the donor, and verifying the information where it is provided. In some circumstances, such as the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of funds.

It is increasingly being recognized that money launderers and terrorist groups are seeking recourse internationally to clubs and charities for the financing of terrorism and laundering of money. Institutions should therefore, determine the risk level of activities in which the NPO is engaged.

In conducting due diligence on a club, society or charity the financial institution should be satisfied of:

(a) the purpose, ideology or philosophy of the NPO by requesting certified copies of the constitution of the club or charity, certification of registration or other similar documents;
(b) the geographic areas served (including headquarters and operational areas);
(c) organizational structure;
(d) the NPO's primary donor and volunteer base;
(e) funding and disbursement criteria (including basic beneficiary information);
(f) record keeping requirements;
(g) affiliation with other NPOs, Governments or groups;
(h) identity of all signatories to the account, and of changes as appropriate; and
(i) identity of all board members and trustees, where applicable.

The identity of the persons exercising control or significant influence over the NPO's assets should be ascertained, in accordance with the procedures required for natural persons. These will often include members of a governing body or committee, the President, any board members, the treasurer, and all signatories.

Financial institutions can also carry out due diligence by checking against publicly available terrorist lists and other government or supervisory watch lists and monitor on an ongoing basis whether funds are being sent to or received from high-risk countries.

In cases of doubt the financial institution can also pay a visit to the NPO's premises, where practicable, to satisfy itself as to the true nature of its activities. They may also satisfy themselves by independent confirmation of the purpose of the club or charity.

Where a non-profit association is registered in an overseas jurisdiction, it may be useful to contact the appropriate NPO's commission or equivalent body, to confirm the registered local branch of the NPO and to obtain any documentary evidence that supports the legitimacy of the NPO.

5.3.3 Foundations

A foundation (also a charitable foundation) is a legal characterization of an 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 organization, a private foundation does not generally solicit funds from the public. In the case of foundations, financial institutions should obtain information on:

1. The foundation's charter;
2. The certificate of registration or document of equivalent standing in a foreign jurisdiction in order to confirm the existence and legal standing of the foundation;
3. The source of funds. In cases where a person other than the founder provides funds for the foundation, financial institutions should verify the identity of this third party and the relationship with the founder and foundation as a whole;

4. The identification evidence for the founder(s), other officers, council members that may be signatories for the foundation and all other beneficiaries of the foundation similar to those required for natural persons.

5.3.4 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.

If any suspicions are aroused about the nature or origin of assets comprising an estate that is being wound up, then a report of the suspicions should be made to the FIU in accordance with the procedures set out in the FIU's Suspicious Transactions Reporting Guideline No 1 - 2013.

5.3.5 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, because of its convenience or because they wish to deliberately avoid face-to-face contact.

Whilst it is recognized that on-line transactions and services are convenient, 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 shall be followed up with appropriate identification checks and personal interviews.

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

FIs shall have policies and procedures in place to address specific risks associated with non-face-to-face business relationships or transactions. Those policies and procedures should apply when establishing customer relationships and conducting ongoing due diligence. FIs shall also have measures for managing risks including specific and effective CDD procedures that apply to non-face-to-face customers.

In accepting business from non-face-to-face customers, such as non-residents applying from abroad, financial institutions shall apply equally effective customer identification procedures and on-going monitoring standards as for those available for face-to-face interview.

Financial institutions should:

(a) ensure that documents presented are completed properly with the requisite details and are certified by an acceptable certifier. Documents presented can be duly authenticated further by contacting the certifier for confirmation;

(b) require customers to submit additional documents to complement those which are required for face-to-face customers to verify identity including more than one photo-bearing ID. This can be done if the prospective customer is required to attend the financial institution to conduct the first transaction, or to collect account documentation or credit/debit cards, then further valid photo bearing identification can be obtained at that time or personal information submitted can be verified;

(c) make face to face contact with the customer as soon as possible;

(d) require the first payment be made through a financial institution which has equivalent or higher customer due diligence standards;

(e) make independent contact with the customer, for example by telephone on the number provided or by communicating with the customer at the address that has been provided. Such communication may take the form of a direct mailing of account opening documentation to the customer, which will be required to be returned completed or acknowledged without alteration;

(f) carry out employment checks (where applicable) with the customer's consent through a job letter or by independent contact with the employer;

(g) ensure that all company documents are signed by the Company Secretary;

(h) require internet sign-on following verification procedures where the customer uses security codes, and/or passwords which have been set up during account opening;

(i) obtain any other information if deemed appropriate.

Copies of supporting evidence should be retained for the statutory period.

5.3.6 Introduced Business

A financial institution should satisfy itself that third parties are regulated and supervised in accordance with FATF Recommendation 23, 24, and 29, and have measures in place to comply with CDD and EDD requirements.

BOG will make available information on countries that do not adequately apply the FATF recommendations.

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 permitted by the financial institution's policies and local laws;

(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 its home supervisory authority;

(b) it is based in a country subject to equivalent or higher AML/ CFT standards; 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 the Compliance Officer or 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. 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 a reasonable time 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.

(i) 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 the AML/CFT Act 2009, Regulations, and 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 AML/CFT Act 2009.

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 time frame, may trigger the termination of the transaction; and
(c) consider submitting a Suspicious Transaction Report (STR).

(ii) Professional Intermediaries

Professional intermediaries include managers of pension funds and unit trusts as well as lawyers, stockbrokers, securities dealers, accountants and other third parties who act as financial liaisons for their clients. Funds are held on behalf of their clients in single or pooled accounts held on deposit or in escrow at financial institutions.

When establishing and maintaining relationships with professional intermediaries, a financial institution should:-

(a) adequately assess the risk and monitor the relationship for suspicious or unusual activity;
(b) determine whether the person is duly registered e.g. insurance agents and brokers under the relevant legislation.
(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.

With respect to pooled accounts the financial institution should identify each beneficial owner.

5.3.7 Private Banking Customers

Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one senior level officer other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, financial institutions must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by the bank's own compliance officers, auditors and supervisory authority.

In particular, 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. 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.

5.3.8 Politically Exposed Persons (PEPs)

Section 2 (1) of the AML/CFT Act 2009 defines a "Politically Exposed Person" or PEP as any individual who is or has been entrusted with prominent public functions on behalf of a state, including a Head of State or of government, senior politicians, senior government, judicial or military officers, senior executives of state owned corporations, important political party officials, including family members or close associates of the politically exposed person whether that person is resident in Guyana or not.

PEP status itself does not automatically mean that the individual is corrupt or has been incriminated in any corruption. However, their office and position can leave them vulnerable to corruption. The risks increase when the person concerned is from a country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards, or where these do not meet international financial transparency standards.

Business relationships with individuals holding important public positions and with the immediate family members of PEPs or companies in which the PEP is the beneficial owner may expose financial institutions to significant reputational, legal risk and costly information requests and seizure orders from law enforcement or judicial authorities. 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.

Furthermore, public confidence in the ethical standards of a whole financial system can be undermined since such cases can receive extensive media attention and strong

political and public reaction, even if the illegal origin of the assets is often difficult to prove. As such, a financial institution should conduct enhanced due diligence where it has determined that an applicant for business is a PEP.

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

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;
(b) obtain the senior management's approval before establishing such business relationships;
(c) take reasonable measures to establish the source of wealth/property/funds.
(d) develop policies, procedures and processes such as the use of electronic databases and publicly available information to assess whether a customer is or has become a PEP.

In addition to the identity information normally requested for natural persons, for PEP information on immediate family members or close associates having transaction authority over the account should be obtained.

Following the commencement of banking relationships, there should be:

(a) enhanced due diligence of the business relationship with regular review by the Compliance Officer or senior management using a risk-based approach, at least yearly, with the results of the review duly documented;
(b) close scrutiny of any complex structures e.g. involving legal structures such as corporate entities, trusts, foundations and multiple jurisdiction established by the PEP;
(c) close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer negotiable instruments which break an audit trail, the use

of unknown financial institutions and regular transactions involving sums just below a typical reporting level;

(d) close scrutiny of transactions requested by the PEP that are unexpected given the customer's account profile;

(e) close scrutiny of amount and transaction which do not make sense given the PEP's known income source and uses;

(f) close scrutiny of transaction which exceeds reasonable amounts in relation to the PEP's known net worth.

The financial institution should regularly review and maintain a current listing of PEPs.

Financial institutions should not establish business relationships with PEPs if the financial institution knows or has reason to suspect that the funds are derived from corruption or misuse of public assets.

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 BOG, the FIU, Law Enforcement Authorities where required, and external auditors.

5.3.9 Shell Banks

A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is not affiliated with a financial services group which is subject to effective consolidated supervision.

To be deemed as having a "physical presence", a bank should: -

(i) be physically located (i.e. 'brick and mortar' presence) at a fixed address in the country in which it has been licensed to do banking business. This fixed address must therefore be one other than a post office box or electronic address;

(ii) employ adequate staff on a full-time basis at the above-named location;

(iii) maintain operating records relating to its banking activities at its fixed address;

(iv) be subject to inspection by the BOG.

Section 15 (7) (c) of the AML/CFT Act 2009 states that "Banks or financial institutions shall not maintain any business relationship with other banks that do not maintain a physical presence under the laws of which they were established, unless they are part of a financial group subject to effective consolidated supervision".

Financial institutions should ensure that required due diligence procedures are undertaken to ensure that correspondent relationships are not established or continued with shell banks.

5.4 HIGH-RISK ACTIVITIES

Certain financial services and activities are more vulnerable to being exploited in money laundering and terrorist financing activities. These conduits are often utilized because each typically presents an opportunity to move large amounts of funds embedded within a large number of similar transactions. Most activities discussed in this section also offer access to international banking and financial systems. Sections 5.4.1 to 5.4.8 deal with examples of high risk activities that require enhanced due diligence.

5.4.1 Correspondent Banking

Correspondent banking refers to the provision of banking services by one bank – in Guyana (the correspondent bank) to another bank – in a foreign country (the respondent bank). 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.

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 about and performing enhanced due diligence processes on correspondent banks prior to setting up correspondent accounts. This should, at a minimum include: -

(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) reference letter from the Supervisory Authority with oversight responsibilities for the financial institution;
(c) obtaining authenticated/certified copies of banking licences or similar authorization documents;
(d) determining the ownership of the financial institution;
(e) obtaining details of the correspondent bank's board and management composition;
(f) determining the location and major business activities of the financial institution;
(g) information on its external auditors;
(h) obtaining proof of its years of operation, along with access to its audited financial statements;
(i) ascertaining whether a respondent institution has been subject to a money laundering or terrorist financing investigation or regulatory action, and that the AML/CFT controls of a respondent institution are adequate and effective;
(j) ascertaining whether the correspondent bank has been the subject of or is currently subject to any regulatory action or any AML/CFT prosecutions or investigations. A primary source from which this information can be sought and ascertained include the Supervisory Authority for the jurisdiction in which the correspondent bank is resident. Information may also be available from the bank's website.
(k) ensuring that approval to open a new correspondent relationship is obtained from senior management or the Board of Directors.

(l) establish the purpose of the account;

(m) assess the institution's AML/CFT controls and ascertain that they are adequate and effective and at least equivalent to those required under Guyana's law. Correspondent relationships should be established with foreign financial institutions only if the financial institution is satisfied that the foreign financial institutions are effectively supervised by the relevant authorities and have effective customer acceptance and KYC policies;

(n) 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 i.e. shell banks. Consequently, financial institutions will need to satisfy themselves that the respondent financial institution in a foreign country do not permit their accounts to be used by shell banks. In this regard financial institutions should take account of whether the foreign correspondent bank permits "payable through accounts". This would be one likely way in which shell banks could take advantage of respondent banks.

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

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

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

5.4.2 Payable-Through Accounts

Payable-through accounts refer to correspondent accounts that are used directly by third parties to transact business on their own behalf. Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with 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.

Where such a relationship has been established a financial institution shall ensure that the person or entity with whom it has established the relationship–

(i) has verified the identity of and performed on-going due diligence on those of that person's customers that have direct access to accounts of the financial institution; and

(ii) is able to provide the relevant customer identification data upon request to the financial institution.

5.4.3 Wire/Funds Transfers

The terms 'wire transfer' and 'funds transfer' refer to any transaction carried out on behalf of an originator who is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer for availability to a beneficiary person at another financial institution. The originator and beneficiary may be the same person. FIs are required to have effective risk - based procedures to identify wire transfers lacking complete originator information.

Although wire systems are used in many legitimate ways, most money launderers use wire transfers to aggregate funds from different sources and move them through accounts at different banks until their origin cannot be traced.

Before initiating one-off wire transfers on the instructions of non-account holding customers, the originating financial institution must verify the identity and address of the originator. In such cases enhanced due diligence must be conducted to verify the authenticity of the transaction moreso if 'cash' is being used to pay for the transfer.

Where money laundering or terrorist financing is known or suspected, the financial institution should make a suspicious transaction report, regardless of the size of the transaction, to the FIU in accordance with section 18 (4) of the AML/CFT Act 2009.

5.4.3.1 Mitigation of Wire Transfer Money Laundering Risks

Familiarity with the customer and type of business enables the financial institution to more accurately analyze transactions and thereby identify unusual wire transfer activity. With appropriate CDD policies and procedures, financial institutions should have some expectation of the type and volume of activity in accounts, especially if the account belongs to a high-risk customer or entity or use higher-risk products or services. Consideration should be given to the following items in arriving at this expectation:

(i) type and size of business;
(ii) customer's stated explanation for activity;
(ii) historical customer activity; and
(iii) activity of other customers in the same line of business.

Enhanced due diligence should be conducted and verification of the identity and address of the originator/customer /beneficial owner should:-

(i) be done before the establishment of the business relationship or before conducting any one off (i.e. occasional) transactions with customers.
(ii) be applied to existing customers and at appropriate times i.e. when significant transactions are being conducted; when transactions which do not appear consistent with the nature or pattern of transactions normally carried out by the customer are conducted; when transactions are conducted after long periods of inactivity of the account or when transactions are paid for in cash.

Please note that these circumstances are not exhaustive and financial institutions are therefore expected to maintain a reasonable level of diligence and monitoring in conducting wire transfers or any other kind of funds transfers.

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/ CFT. Where a relationship is deemed high risk e.g. located in a high-risk jurisdiction, a financial institution should conduct enhanced due diligence and should:

(a) undertake a more detailed understanding of the AML/CFT programme of the respondent bank and its effectiveness;
(b) review effectiveness of the respondent bank's group programme;
(c) identify the respondent bank's owners, directors and senior managers; and
(d) determine the ownership structure.

5.4.3.2 Cross –border Wire Transfers

(1) Remitting Financial Institution

Financial institutions that initiate wire transfers on behalf of customers to a beneficiary overseas must ensure that the customer's information conveyed in the payment message or instruction is accurate and has been verified. Verification of the identity of the originator/customer should be done before conducting any funds transfer or one off (i.e. occasional) transactions with customers and should include:

(i) the identity of the originator/remitting customer (including name and address, official identification information)
(ii) the name and address of the ultimate recipient/beneficiary
(iii) related narrative /instructions that accompany transfers
(iv) amount and currency type should be clearly stated
(v) routing number if applicable
(vi) execution date of the payment order
(vii) identity of the beneficiary' financial institution

(viii) Account number of the beneficiary where such an account is used to process the transaction. In the absence of an account number, any other unique transaction reference number may be included.

The payment message should be signed by the customer or the authorized signatories on the account and authenticated.

The above shall not apply to wire transfers/settlements between financial institutions where the originator and beneficiary of the funds transfer are acting on their own behalf.

(2) Beneficiary Financial Institution

Where the financial institution is the beneficiary financial institution that institution should apply a risk-based system, to the review of transfers for complete originator information and the reporting of unusual or suspicious activity, and should ensure that at a minimum the details similar to that at items (i) to (viii) above are included on the incoming wire transfer.

Financial institutions should conduct enhanced scrutiny of, and monitor for suspicious activity, incoming funds transfers which do not contain complete originator information. This will involve examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (eg originating in a country known to harbour terrorists or terrorist organizations). The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transaction is suspicious and to consider, as appropriate, whether they are thus required to be reported to the FIU. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet the above requirements.

Transfers not accompanied by the complete originator information should not be processed by the receiving or intermediary financial institution unless and until the

complete originator information is available. Where a transfer of this nature is identified, it should be immediately flagged for either termination or as one not to be acted on, until the requisite information is received. To this end it is the responsibility of financial institutions to ensure that they are legally in a position to terminate the transaction, or to delay acting on the transaction until the requisite information has been received. The originating financial institution must be contacted immediately for complete originator/beneficiary information.

In the interest of good customer relations, financial institutions should pursue methods of making their customers aware from the outset that all wire funds transfers must be accompanied by the complete originator details as the absence of this information can cause the transaction to be delayed or terminated.

The above is also equally applicable to financial institutions conducting outgoing domestic transfers and outgoing cross border transfers.

Where the beneficiary or intermediary financial institution finds that there is an ongoing situation of consistent or the frequent receipt of transfers of the nature described above, it should consider terminating its business relationship with the financial institution from which such transfers are received.

A beneficiary financial institution should have effective risk-based policies and procedures for determining:

(i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(ii) the appropriate follow-up action.

(3) Intermediary Financial Institution

An intermediary financial institution refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

For cross-border wire transfers where funds transfers are processed as an intermediary, e.g. where financial institution "B" is instructed by financial institution "A" to pay funds to an account held by a beneficiary at financial institution "C", the originator and beneficiary data and other payment instructions should be provided by financial institution "A" and should be retained and, included in the payment message generated by financial institution "B" to institution "C'.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least seven years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution in a situation where technical difficulties prevent the full originator information accompanying a cross border wire transfer from being transmitted along with a related domestic wire transfer.

An intermediary financial institution should take reasonable measures to identify cross border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

An intermediary financial institution should have effective risk-based policies and procedures for determining:

(i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
(ii) The appropriate follow-up action.

5.4.3.3 Occasional Transactions

As defined in the AML/CFT Regulations 2010, a one-off transaction means any transaction other than a transaction carried on in the course of an established business relationship between a financial institution and a customer.

Where a financial institution undertakes these transactions, satisfactory evidence of identity must be obtained failing which, the transaction should be terminated. The non-account holder must produce positive evidence of identity as set out in this guideline and in accordance with sections 3; and 4 (2) (b); and 4 (3) (b) of the AML/CFT Regulations 2010.

It is important for a financial institution to determine whether a customer is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship, as this can affect the verification requirements.

Occasional transactions include:

a. encashment of cheques drawn on the financial institution;
b. exchange of coins for cash;
c. purchase of foreign currency for holiday travel; and
d. one off transfer of funds overseas via wire transfer.

Due diligence measures including identifying and verifying the identity of customers, should be undertaken on, inter alia, occasional transactions equal to or exceeding one million dollars or its equivalent in foreign currency, whether conducted in a single transaction or multiple operations that appear to be linked.

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

At a minimum, a financial institution should:

(i) identify and verify the persons conducting occasional transactions below the above thresholds;

(ii) maintain an effective system to monitor for abuse of occasional transactions; and

(iii) establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

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

Verification of identity will not normally be needed in the case of an exempted occasional transaction referred to above. If, however, the circumstances surrounding the occasional transaction appear to the financial institution to be unusual or questionable, further enquiries should be made. If as a result of enquiries, the financial institution becomes aware of or suspects money laundering or the financing of terrorism the financial institution must take steps to verify the proposed client's identity.

Where money laundering or terrorist financing is known or suspected, the financial institution should make a suspicious transaction report regardless of the size of the transaction to the FIU in accordance with section 18 (4) of the AML/CFT Act 2009.

5.4.3.4 Transactions by Non-Customers

Funds deposited into an existing account by third parties whose names do not appear on that account, should be handled with particular care. The financial institution should conduct enhanced due diligence to ascertain whether the person(s) making the deposits is/are authorized to do so or is a known agent. In cases where such transactions are not routine, it could be an attempt by the account holder to remain unknown and avoid disclosing the source of the funds moreso if the depositor has no knowledge of where the funds came from.

In such instances, the financial institution must have documented evidence on record from the account holder authorizing such persons to conduct business or specific transactions on the account. The requisite photo-bearing identification and details as outlined in this Guideline should also be obtained and placed on file.

The financial institution should also have systems in place to identify transactions whether singly or the aggregate of a series of linked transactions exceed the reporting threshold of two million dollars.

Where the depositor is unable to provide adequate details concerning the source of funds for a transaction in excess of the reporting threshold, the financial institution should contact the account holder for verification. If as a result of enquiries, the financial institution has reasonable grounds to suspect that the funds/transaction are connected to the proceeds of crime, money laundering or terrorist financing activities it should refuse the funds/transaction and consider preparing an STR report.

5.4.3.5 High-Risk Countries[18]

Financial institutions must exercise added care when dealing with clients residing in countries with weak or non-existent laws and regulations to detect and prevent money laundering and terrorist financing. Such high-risk countries should be clearly outlined in the financial institution's policy manual and updated whenever necessary

Certain countries are associated with crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to financial institutions. Conducting a business relationship with such a country or with institutions in that country exposes the financial institutions to reputational risk and legal risk.

Enhanced due diligence should be undertaken before establishing a business relationship and caution should be exercised in respect of the acceptance of certified documentation from individuals and entities located in high-risk countries and

[18] Refers to countries that appear on FATF public lists of high risk and non-cooperative jurisdictions, UN lists, government or Bank of Guyana lists or any other such lists.

territories. Appropriate verification checks should be undertaken on such individuals/entities to ensure their legitimacy and reliability.

Business relationships or financial transactions with the identified country or persons in that country should be limited or terminated where serious doubt exist as to the authenticity of the business relationship or transactions.

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

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[19].

5.4.3.6 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 continued banking facilities by the other financial institution.

5.4.3.7 Monetary Instruments

(a) Cash Transactions

The use of cash or currency (*i.e.* banknotes and coins used as a medium of exchange) is attractive to criminals mainly because of its anonymity and lack of audit trail. Criminals look for as much flexibility as possible and are interested in avoiding

[19] See FATF Public Statement - High-risk and non-cooperative jurisdictions:
- jurisdictions for which an FATF call for action applies
- other monitored jurisdictions

detection. Cash provides that flexibility, as it is universally accepted and can be used and moved with little or no record keeping.

Care must be exercised when establishing account relationships with businesses that are cash-intensive[20] as they can be used to:

(a) provide a front to launder money and expand criminal enterprises;

(b) reinvest criminal income in the legitimate economy (for example, the business is acquired using tainted money but operates legitimately);

(c) co-mingle illicit and legitimate income.

Where cash transactions (deposits, withdrawals, loan installments, payments etc.) are being proposed by a customer, and such requests are not in accordance with the customer's known reasonable practice, financial institutions must approach such situations with caution and make relevant EDD enquiries to ascertain the origin of the funds (i.e. whether funds are derived from the proceeds of crime or not) and that turnover on the account is in accordance with expected activity.

Where the financial institution has been unable to satisfy itself that a particular cash transaction is reasonable, and therefore considered suspicious, the financial institution should make a suspicious transaction report regardless of the amount to the FIU.

In accordance with section 12 (3) (c) of the AML/CFT Regulations 2010, a financial institution is also required to submit a report of all cash transactions in excess of two million dollars or its foreign currency equivalent to the FIU, whether or not such transactions are considered suspicious. A copy of the Source of Funds Declaration form must be retained by the financial institution and should be kept for the statutory seven (7) year period in the event that it is required in the future.

[20] Examples of cash-intensive businesses include but are not limited to supermarkets, wholesale distributors, retail outlets, gas stations, restaurants, shops, nightclubs/ bars etc.

Whilst certain cash transactions may lead the financial institution to make further enquiries to establish or dispel suspicion, it goes without saying that equal vigilance must be applied to non-cash transactions that exceed the reporting limit.

5.4.3.8 Cash Transactions below the Reporting Threshold

As an internal control, a financial institution should utilize a "large cash transaction report" (LCTR) to identify multiple smaller cash transactions done at different branch locations by the same customer or by different persons on behalf of the same customer over a specified period of time which cumulatively exceeds G$2,000,000 (two million dollars). In such cases the entire series of transactions should be treated as a single transaction if the financial institution has knowledge that the transactions are for the same person's beneficial use and a report must be submitted to the FIU. Likewise if any or all of these transactions are deemed suspicious by the financial institution a STR should be submitted to the FIU regardless of the amount. Nothing however, precludes a financial institution especially in smaller financial institutions from instituting lower cash thresholds and time frames for multiple transactions in order to detect transactions that are potentially being structured to avoid detection.

The above will be applicable for large cash deposits, payments for monetary instruments such as wire transfers, traveler's cheques, bank drafts or any other cash transactions that exceed singly or cumulatively within a given period the reporting threshold.

(b) Other Monetary Instruments

Other monetary instruments such as bank drafts, traveller's cheques, and money orders offer a portable and compact way to smuggle high-value assets across international borders.

Criminals may attempt to purchase these monetary instruments with co-mingled funds (consisting of legitimate business earnings and the proceeds of crime) to camouflage the connection to underlying crimes.

Whether the purchaser is an account holder or not the following information should be recorded at the time of the transaction:

(a) name of the purchaser;

(b) address of the purchase;

(c) valid photo-bearing identification;

(d) date of purchase;

(e) type(s) of instruments purchased;

(f) serial numbers of each of the instruments purchased;

(g) value of each of the instruments purchased;

(h) amount/Currency type;

(i) purpose of instrument;

(j) specific identifying information, if applicable such as beneficiary name and address;

(k) source of funds used to pay for the instrument whether from the customer's account or by cash;

(l) signature of the customer;

(m) beneficiary (payee) name and address;

(n) name of the institution on which the instrument is drawn.

(o) details of any endorsement appearing on the instrument.

The financial institution should have procedures in place to identify multiple purchases of monetary instruments during a specified period, and to aggregate this information from all of the financial institution's branches. Purchases of different types of instruments at the same time should be treated also as one purchase and the amounts should be aggregated to determine if the total exceeds the reporting threshold.

If a customer first deposits the cash in a bank account, then purchases a monetary instrument, the transaction is still subject to this regulatory requirement. The financial institution should have procedures in place to recreate the transactions if required. The information required to be obtained must be retained for the statutory period.

If the purchaser cannot provide the required information at the time of the transaction or through the bank's own previously verified records, the transaction should be refused and a STR prepared. Where the value of the transaction whether singly or aggregated exceeds two million dollars the financial institution is required to prepare a Source of Funds Declaration form for submission to the FIU.

5.5 REDUCED DUE DILIGENCE AND EXEMPT CUSTOMERS

The CDD measures set out in FATF Recommendation 10 – Customer due Diligence do not imply that financial institutions have to repeatedly identify and verify the identity of each customer 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 of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

Furthermore, the Minister in accordance with section 17(1) of the AML/CFT Act 2009 may reduce or simplify the identification and verification requirements of the identity of the customer or beneficial owner by financial institutions.

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 may be:

(i) 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.

(ii) where an existing customer opens a new account. However, if the source of funds/wealth is questionable or originates from an external source, or country where, for example, it is believed that there is a high level of drug trafficking or corruption, reduced due diligence should not apply.

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

(v) the customer is itself a financial institution to which the FIA 1995 applies and which has been licensed or registered, and is supervised for anti-money laundering and countering of terrorist financing measures by a regulatory authority and the financial institution has satisfied itself as to the adequacy of the measures to prevent money laundering and terrorist financing.

(vi) identification procedures shall also not be required in relation to a one-off transaction, in which the proceeds of the transaction are not paid, but are directly reinvested on behalf of the person to whom the proceeds are payable in another transaction :-

(a) of which a record is kept; and

(b) which results only in another reinvestment made on that person's behalf or, in payment made directly to that person. In the absence of this his/her identification requirements must be obtained before the proceeds are paid to the customer or be re-invested on his behalf.

Where a financial institution has taken a decision to apply reduced CDD measures, the financial institution must retain documentation that supports the basis for arriving at

this decision. However, reduced or simplified customer due diligence measures shall not be permitted by financial institutions whenever there is a suspicion of money laundering or terrorist financing activities.

Financial institutions should not grant blanket exemptions to customers, and should clearly document the financial institution's policy for granting of such exemptions including the criteria for exemption and the officers of the institution authorized to grant such exemptions. An authorized customer exemption list should be maintained and should show the criteria for each customer exemption, any transaction threshold limits and any other information to support the financial institution's position. In addition the exemption list should be reviewed annually to ensure that qualifying customers continue to satisfy the institution's risk profile. Where it is noted that a customer's financial activity is not in keeping with expected norms, that customer should be removed immediately from the exemption list and should be subject to EDD.

Customer due diligence may not be required in some cases of exempt customers such as:-

(i) any central or local government agency or statutory body
(ii) a publicly traded company or investment fund listed on the Guyana Stock Exchange
(iii) a financial institution licensed under the FIA 1995 and regulated by the BOG
(iv) an insurance company licensed under the Insurance Act 1998 and regulated by the BOG
(v) a foreign financial institution regulated by a Central Bank or equivalent supervisory authority in a jurisdiction that adequately complies with the FATF 40 + 9 Recommendations on AML/CFT.
(vi) a financial institution and a customer, where the customer is, at the time the transaction takes place, an established customer of the financial institution and the transaction consists of a deposit into, or withdrawal from, an account maintained by the customer with the financial institution, where the

transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of the customer.

PART 6 – SPECIAL CONSIDERATIONS

6.0 PRODUCTS AND SERVICES REQUIRING SPECIAL CONSIDERATION

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

6.1 Custody Arrangements (Safe Custody, Safety Deposit Boxes)

A financial institution must take certain precautionary measures in relation to requests to hold boxes, parcels, sealed envelopes and other valuables in safe custody.

Where such facilities are made available to account holders and non-account holders, the customer identification and verification procedures set out in this Guideline shall be followed, depending on the type of customer (natural/corporate) involved. Valid photo-bearing identification, mandates outlining the access arrangements for multiple customers and the relationship with each other and references for each customer with access to the facility etc. should be obtained by the financial institution. These should be verified in accordance with the steps set out in section 4.2 of this Guideline.

Because custody arrangements offer privacy of the contents placed in them, these facilities can be used to conceal the proceeds of crime, money laundering, terrorist financing and other illicit activities. It is therefore important that enhanced due diligence be conducted for potential customers requesting such facilities. Where a customer is considered high-risk such a facility should be denied. It is also important that financial institutions monitor and record the frequency of visits and the name(s) of the person accessing the facility as it is not expected that items placed in a safe deposit box or safe custody for the purpose of safe keeping would attract many visits. The time taken during each visit should also be recorded and monitored.

It may not be necessary to reverify the KYC details submitted, especially if the customer is an account holder already with the financial institution and considered low-risk based on the institution's risk-based assessment.

6.2 Trade Finance

FATF defines trade-based money laundering as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include:

- over - and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over - and under-shipments of goods and services; and
- falsely described goods and services.

Reasonable measures to address this risk could include but are not limited to:

(i) periodic verification, using credible open source material or information, of the business of the client that triggers the need for such payments;

(ii) periodic review of electronic funds transfer data to determine whether the client's business includes significant trade activity;

(iii) periodic review of the client's transactions compared to the financial institution's record of the intended purpose of the account;

(iv) meeting or other interaction with the client.

Where the assessed risk of money laundering and terrorist financing in trade finance services is elevated, financial institutions should take reasonable measures designed to mitigate the risk of misuse of trade financing measures. Reasonable measures could include:

(i) subjecting requests involving letters of credit and other trade financing instruments to cover shipments of goods that are not consistent with the applicant's normal business patterns to more detailed review and noting the results in the client's records;

(ii) identifying significant differences (either between different clients, different shipments or market quotes) in prices of a good or commodity being financed under a letter of credit, or other trade financing instrument and determining the business rationale for the differences;

(iii) making additional enquiries about the business rationale of transactions involving multiple banks and payments flowing through intermediaries as opposed to directly from the importer's bank to the exporter's bank; and

(iv) reviewing the routing of shipments and note ports of call or transhipment points that are inconsistent with a standard commercial transaction, where there is no apparent business rationale for the routing, or where the routing or the carrier is located in a high risk country.

Financial institutions shall accordingly, have adequate systems to properly manage risks associated with trade finance activities. Such systems shall depend on the financial institution's size, complexity, location and types of customer relationship and shall effectively enable a financial institution to identify and monitor its trade finance portfolio for suspicious or unusual activities, in particular those that pose a higher risk for money laundering.

Financial institutions shall also have their trade finance accounts regularly sample-tested with the view of verifying whether they are meeting their customer due diligence, record keeping, monitoring and reporting obligations.

6.3 Emerging Technology and New Payments Methods (NPMs)

A number of innovative products for making payments have been developed in recent years, taking advantage of rapid technological progress and financial market

developments. This product range continues to grow at a rapid pace and include such services as debit, credit and prepaid cards, telephone/mobile and internet based products and services. However, because of the anonymity[21], rapid transaction speed and wide geographic availability, NPMs are becoming increasing vulnerable to abuse for money laundering and terrorist financing purposes.

FIs must have policies and procedures in place or take such measures to prevent the misuse of technological developments in money laundering and terrorist financing.

FATF recommendation 15 states that financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to

(a) the development of new products and new business practices, including new delivery mechanisms, and

(b) the use of new or developing technologies for both new and pre-existing products. For financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

The money laundering and terrorist financing risks posed by emerging technology and NPMs can be effectively mitigated by several countermeasures that can be taken by financial institutions. User anonymity as a risk factor can be mitigated by implementing robust identification and verification procedures as outlined earlier in this guideline at the time of granting such a service.

It is recommended that only current customers, who already have a relationship with the financial institution and who are fully identified according to KYC rules, may open accounts using internet and phone banking.

Customer verification during account origination is important in reducing the risk of identity theft, fraudulent account applications and money laundering. Failure on the

[21] The account can be opened by one person but used anonymously by another person or the customer other than at the time of opening the account , can remain anonymous as most transactions are done online or through ATMs.

part of the financial institution to adequately verify customers could result in unauthorized individuals gaining access to e-banking accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activities.

Additionally, the risk posed by an NPM can be effectively mitigated by imposing value limits (*i.e.* limits on transaction value either per single payment or cumulatively and the frequency of permitted transactions per day/week/month/year) or by implementing strict monitoring systems.

It is also essential that financial institutions confirm that a particular communication, transaction, or access request is legitimate. Accordingly, financial institutions that offer internet based and/or telephone products and services should ensure that they have reliable and secure methods for authenticating the identity and authorization of a customer each time an attempt is made to access his/her private information or initiate an electronic transaction. Wherever appropriate, they should implement multi-factor verification measures, layered security, or other controls reasonably calculated to mitigate those risks.

The authentication methods can involve confirming one or more of these factors:

(i) information only the user should know, such as a password or personal identification number (PIN) or security questions.

(ii) an object the user possesses, such as an automatic teller machine (ATM) card, credit card, prepaid or reloadable or account-linked value cards.

6.4 Hold mail, C/O and P.O Box Addresses

The use of "Hold Mail", c/o, and P.O Box addresses while not necessarily suspicious carry a higher risk as they can lend to attempts by a customer to conceal his identity and whereabouts. It can also indicate that the customer for whatever reasons is trying to hide his business/account relationship with the financial institution. Especially where it

relates to a business relationship, the lack of a permanent residence or business address can also indicate that the business is non-existent or simply a 'front' for criminal activities.

"Hold Mail" relationships are defined as those where the customer has instructed the financial institution not to forward any correspondence by post or otherwise to the customer's residential or business address but to hold them at the financial institution for storage and later collection.

Regardless of the source of "Hold Mail" business, evidence of identity of the account holder should be obtained by the financial institution in accordance with CDD requirements in these Guidelines.

Due to the increased money laundering risk these accounts represent, "Hold Mail" relationships must be treated with caution and should be regularly monitored and reviewed. Financial institutions should establish procedures to conduct annual checks of the current permanent address of "hold mail" customers. Where such relationships are allowed, it should be an exception and where there are plausible and legitimate reasons.

Financial institutions must have controls in place for identifying when existing relationships change their status to "Hold Mail", and that necessary steps to obtain the identity of the customer are taken when such evidence is not on file.

Accounts with c/o and P.O Box addresses should not be treated as "Hold mail" accounts as mail is being issued albeit not necessarily to the account holder's address. There are of course many genuinely innocent circumstances where a "c/o" or P.O box address is used, but like with "Hold Mail" financial institutions should verify that this is the case and should monitor such accounts more closely if they believe these accounts may represent higher risks.

In all of the abovementioned cases, the financial institution should still have on file a permanent address for the customer's residence and/or place of business in cases where the above situations are allowed.

Only the customer/beneficial owner(s) or the authorised signatories on the account should be permitted to request changes to the address status and at all times such requests should be documented.

6.5 Dormant Accounts

The financial institution should have policies and procedures in place to identify the risk related to dormant accounts.

PART 7 – RECORDS AND REPORTS

7.1 UNUSUAL, COMPLEX AND SUSPICIOUS TRANSACTIONS

As the types of transactions which may be used by money launderers are almost unlimited, it is difficult to define a suspicious transaction. However, it is important to properly differentiate between the terms "unusual" and "suspicious".

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.

Complex transactions or structures may have entirely legitimate purposes. However, financial institutions should pay special attention to all complex, unusual transactions, which have no apparent economic or visible lawful purpose. 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 or unusual transactions should be kept by the financial institution, and be available to the auditors, supervisory authorities and FIU for at least seven years.

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 whether completed or not may be unusual or large or may represent an unusual pattern that has no apparent or visible economic or lawful purpose. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or a very high account turnover that is inconsistent with the

expected pattern of transactions. In some instances, the origin of the transaction may give rise to suspicion. These are not expected to be exhaustive but they do provide examples of the most basic ways by which money may be laundered or terrorism can be financed.

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. A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and the determination of consistent transaction limits. The financial institution is expected 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 or suspicious. 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.

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. 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. Of course, a transaction can also be reported as a suspicious transaction that does not meet the reporting threshold or multiple transactions test because it can suggest attempts at structuring of transactions by a customer in order to evade the reporting requirements;

(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;

(d) require documentation of internal enquiries;

(e) develop effective manual and/or automated systems to enable staff to monitor, on a solo, consolidated and group or branch wide basis, transactions undertaken throughout the course of the business relationship and identify activity that is inconsistent with the financial institution's knowledge of the customer, their business and risk profile.

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

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

(a) Internal Reporting Procedure

Where a staff member conducts enquiries and obtains a satisfactory explanation for the unusual or complex transaction or pattern of transaction, it may be concluded that there are no grounds for suspicion, thus further actions may not be necessary, except for the documentation of the reasons for such determination.

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.

Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented and forwarded to the Compliance Officer who will determine whether the transaction should be reported to the FIU as soon as possible.

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

Financial institutions may have internal reporting procedures that allow a suspicious report to be channeled through the branch manager or department head before it reaches the Compliance Officer. Where such internal reporting procedures are in place, the branch manager or department head 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.

7.2 SUSPICIOUS TRANSACTION REPORTING (STR)

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. Staff at all levels should also be aware of the identity of the Compliance Officer and the steps to be followed when making a suspicious transaction report. All staff must be aware that all suspicious transactions should apply regardless of whether they are thought, among others, to involve tax matters.

Where a suspicious report has been filed with the FIU, and further unusual or suspicious activity pertaining to the same customer or account arises, a financial institution should file additional reports with the FIU.

Pursuant to section 18 (4) of the AML/CFT Act 2009 a financial institution is required to report as soon as possible but not later than three working days to the FIU, where the

identity of the person involved, the transaction, proposed transaction or attempted transaction or any other circumstance concerning that transaction lead the financial institution to have reasonable grounds to suspect that a transaction:

(i) involves proceeds of crime to which the AML/CFT Act 2009 applies;

(ii) involves or is linked or related to or to be used for terrorism, terrorist acts or by terrorist organizations or for the financing of terrorism; or

(iii) is of a suspicious or an unusual nature.

The STR should be in the format prescribed in the Guideline No.1 – 2013 issued by the FIU or in accordance with section 18 (4) (b) of the AML/CFT 2009. All reports must be accompanied by a letter signed by the financial institution's Compliance Officer.

A financial institution which has reported a suspicious transaction shall if requested by the FIU provide further information as required on the said transaction.

7.3 RECORD KEEPING PROCEDURES & RETENTION

Financial institutions should develop clear standards on what records must be kept on customer identification and individual transactions and their retention period. Such a practice is essential to permit a financial institution to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

To ensure that records remain up-to-date and relevant, there is a need for financial institutions to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, or at least upon occurrence of a material change to the business relationship (e.g. change of employment, marital status, address etc.), or when there is a material change in the way that the account is operated. In addition, it is recommended that records for high risk customers are updated at least annually.

If during the course of the updating exercise or anytime after the business relationship has commenced the financial institution discovers that the information on file is inaccurate, insufficient or is no longer applicable it should take steps to ensure that all relevant and updated information is obtained as quickly as possible. Where the correct information is not available or cannot be obtained for any reason, then the financial institution must take steps to terminate the relationship and should consider referring the matter to the Supervisory Authority or FIU.

Part III section 16 (1) – (5) of the AML/CFT Act 2009 and sections 6 (10) of the AML/CFT Regulations 2010 stipulate the minimum requirements for financial institutions with regard to record keeping.

To facilitate compliance with the above 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.

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 7 years, from the date the relevant transaction or series of linked transactions was completed or when the business relationship was terminated, whichever is the later. It is an offence to knowingly destroy, falsify or conceal any document or material which would aid in an investigation into money laundering, terrorist financing or the proceeds of crime[22].

It may also be necessary for financial institutions to retain records for a longer time period as required by other statutory requirements or mandated by the Central Bank or

[22] Refer to AML/CFT Act 2009 –Section (6) (1) (2)

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 customer.

In addition, transaction records should contain sufficient details[23] to permit reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, an audit trail and 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.

Records should be retained in a format, including electronic, scanned or original, that would facilitate retrieval in legible form without undue delay.

Financial institutions should ensure that records held by a subsidiary or affiliate outside of Guyana at a minimum, comply with the requirements of Guyana law and this Guideline. 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 Guyana law and will be available to the BOG on request and to the FIU or law enforcement authorities.

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.

[23] Such details are specified in Section 16 of the AML/CFT Act 2009.

(a) Establishment of Registers

A financial institution is required to maintain a register of all suspicious transactions reports made to the Compliance Officer and should contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant documents.[24]

Additionally a financial institution is required to maintain a register of all enquiries made to it by the FIU and other law enforcement authorities acting under powers provided by the AML/CFT Act 2009 or any other law relating to money laundering, terrorist financing and proceeds of crime. The register should be kept separate from other records and contain at a minimum the date and nature of the enquiry, the name and agency of the enquiring officer, the powers being exercised, and details of the accounts or transactions involved.

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 AML requirements; and
e) an on-going training plan.

(b) Internal Record Keeping

Financial institutions should maintain internal records related to unusual and suspicious business transactions for no less than 7 years. These should include:

(i) all reports such as Source of funds Declaration made by staff to the Compliance Officer;

[24] Refer to Section 11 (2) (3) of the AML/CFT Regulations 2010

(ii) the internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;

(iii) consideration of those reports and of any action taken; and

(iv) reports by the Compliance Officer to senior management and board of directors.

MSBs are required to maintain a current list of all its agents, if any, which must be made available to the BOG upon request.

7.4 OTHER FORMS OF REPORTING

Financial institutions shall report to the FIU in accordance with section 12 (1) (c) of the AML/CFT Regulations 2010 all cash transactions in excess of GY$2,000,000 (or its foreign currency equivalent) for both individuals and business entities or amounts as may be determined from time to time.

7.5 REPORTING DECLINED BUSINESS

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 STR.

Section 18 of the AML/CFT Act 2009 requires FIs to report to the FIU, not later than three days after forming that suspicion, that funds, a transaction or attempted transaction are connected to the proceeds of criminal activity, money laundering or terrorist financing offences.

PART 8 – TERRORISM FINANCING

8.1 COMBATING THE FINANCING OF TERRORISM

The reporting institution should ensure that the existing suspicious transaction reporting system and mechanism for the identification of suspicious transactions are extended to cover financing of terrorism.

Financial institutions should protect themselves from being used as a conduit for the financing of terrorism and make use of their already existing due diligence requirements, along with current policies and procedures on money laundering and enhance them where necessary to detect transactions that may involve terrorist funds[25].

Financial institutions should review their practices in this area as part of their general internal and external audit processes.

In ensuring efficient detection of suspected financing of terrorism, the reporting institution should develop and maintain a database of names and particulars of terrorist from government lists published in the Gazette[26] or submitted from time to time through circulars issued by the BOG. In addition, the reporting institution should consolidate its database with advisories from other recognized bodies such as the United Nations Security Council Resolutions and FATF.

The FI should conduct regular checks on the names of new and existing customers against the names in its database. Section 18 (4) of the AML/CFT Act 2009 requires FIs who suspect that funds are connected to the proceeds of criminal activity, money laundering or terrorist financing offences confirm the identity of its customer. If the customer's name fully matches any name in the database, the financial institution should immediately:

[25] See FATF document - Guidance for Financial Institutions in Detecting Terrorist Financing
[26] Refer to AML/CFT Act 2009 –Section (68) (6)

(a) Inform the Financial Intelligence Unit

(b) Reject the customer, if the transaction has not commenced; and

Where the reporting institution suspects that a transaction is terrorist related, it should make a suspicious transaction report to the Financial Intelligence Unit.

In addition to the reporting of STRs every financial institution is required to disclose forthwith to the FIU:

(i) the existence of any property in its possession or control;

(ii) any information regarding a transaction or attempted transaction in respect of terrorist property; or where there is reasonable grounds to believe may involve terrorist property.

Such information should include the particulars relating to the persons, accounts and transactions involved and the total value of the property.

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.

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

Annex 1

MONEY TRANSFER AGENCIES AND CAMBIOS

1. MONEY TRANSFER AGENCIES (MTAs)

The following guidance applies to money transfer services providers and their agents licensed under the Money Transfer Agencies (Licensing) Act 2009 who conduct money transfer and remittance business.

"Money transfer or remittance business" can be considered as the business of accepting cash, cheques and other monetary instruments in one location and the payment of a corresponding sum in cash (local or foreign) 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.

1.1 Vulnerability of MTAs to Money Laundering and Terrorist Financing

The fleeting relationship with its customers makes MTAs 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 MTA and can repeatedly use different MTAs to transact business. The MTA 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.

All MTAs are required to implement an AML/CFT compliance program. All AML/CFT compliance program must be balanced to the risks presented by the MTAs location, size, and the nature and volume of the services it provides. The purpose of the AML compliance program is to prevent money laundering issues and to understand how to prevent them. It is the responsibility of each money transfer services provider to have policies in place to prevent money laundering and terrorist financing in line with the FATF Forty Recommendations. Such policies should include documented provisions for:

(i) internal systems of controls, policies and procedures;

(ii) CDD procedures;

(iii) a risk-based framework;

(iv) a records management system; and

(v) education and training of employees in recognizing and reporting suspicious transactions.

1.2 Identification Documentation

Proper identification documentation is required for all money transmissions. The requirement for specific pieces of the remitting customer information that are to accompany each wire transfer applies to money transfers. MTAs must therefore request and obtain customer identification documentation for money transfers similar to that required under the section "Cross-Border Wire Transfers sub-section (1) - Remitting Financial Institutions."

Customer identification information should be obtained prior to a transaction being carried out. If identification information is not obtained, the transaction should not proceed. For further guidance on customer identification and record keeping requirements, money transfer services providers should refer to those particular sections 4 and 7 of this Guideline.

In ensuring that there is compliance with this requirement, money transfer agencies are not expected to apply the exact verification procedures outlined earlier in this guideline in relation to customers. However, money transfer agencies must employ alternative verification processes more suited to their operations in order to satisfy themselves of the veracity of the information provided and of the authenticity and validity of the identification tendered. Techniques to be employed may include but not be limited to checking the signature of the applicant for business with the signature on any transaction instrument or documentation offered by the customer; ensuring that identifications tendered are current and do not appear to be forged

documents or documents that have been tampered with; that the picture in the identification used is consistent with the features of the person tendering the identification; questioning the customer for confirmation details where this becomes necessary in the circumstances.

1.3 Transaction Monitoring

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

An MTA shall report to the FIU all money transfers over G$200,000 (two hundred thousand dollars) as soon as is practicable in accordance with section 12 (3) (a) of the AML/CFT Regulations 2010.

1.4 Identifying Unusual and Suspicious Transactions

Providing quality customer service involves knowing who your customers are and being alert to those individuals who may wish to use a MTA for illegal purposes. By getting to know your customers, you will be better able to identify suspicious or unusual transactions. The following list provides examples of questionable activity and behavior that may assist you in monitoring your transaction activity. These examples, by themselves, may not necessarily be suspicious, but they need to be taken into consideration along with other circumstances surrounding the transaction.

All suspicious transactions reports must be submitted to the FIU no later than three (3) days after forming a suspicion.

1.5 Transactions Which Do Not Make Economic Sense (Red Flags)

(i) Transactions which are incompatible with the MTA's knowledge and experience of the customer in question or with the purpose of the relevant business transaction.

(ii) 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 -

  (a) at different times on the same day;

  (b) with different cashiers of the MTA on the same day or different days; and

  (c) at different branches/offices of the same MTA.

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

(iv) 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.

(v) 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.

1.6 Transactions Involving Large Amounts of Cash

(i) Frequent transactions of large cash amounts that do not appear to be justified by the customer's business activity.

(ii) 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.

(iii) Cash payments remitted to a single account by many different persons without an adequate explanation.

1.7 Other Types of Transactions and Activity

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

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

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

(iv) A business customer that is reluctant to provide complete information regarding: the type of business, the purpose of the transaction, source of funds or any other information requested by the MTA.

(v) A customer receives small incoming transfers and then makes a large outgoing transfer.

(vi) Unusual or suspicious identification documents are provided, or customer refuses to show ID.

1.8 Record Keeping

In accordance with section 16 of the AML/CFT Act 2009, an MTA shall establish and maintain records of all transactions for a period of seven years from the date the relevant transaction was completed, or the business relationship was terminated whichever is later.

1.9 Cambios and Bureaus De Change

The nature of the relationship between Cambios and Bureaus De Change hereinafter referred to collectively as Money Service Business (MSB) and their respective customers can be fundamentally different from that established between banks and other regulated financial institutions and their customers. MSBs are licensed under the Dealers in Foreign Currency Licensing Act 1989 to buy and sell foreign currency only but are prohibited in accordance with section 9 (4) of the Dealers in Foreign Currency

(Licensing) (Amendment) Act 1995 from the lending or borrowing, or acceptance of deposits, of Guyana dollars or any foreign currency.

This Guideline is issued in accordance with section 22 **(2)** (b) of the AML/CFT Act 2009 and should be circulated to all sub-agents or branches of the MSB. In addition, MSBs are required to maintain a current list of all its agents, if any, which must be made available to the BOG upon request.

MSBs are an important link in the money laundering chain since it is difficult to trace the origin of the money once it has been exchanged. Typologies exercises conducted by the FATF have indicated increasing use these institutions in laundering operations. Hence it is important that there should be effective counter-measures in this area.

It is the responsibility of each MSB to have systems and training in place to prevent money laundering. Each MSB must maintain identification and record-keeping procedures, and such other procedures, controls and communications appropriate for the purposes of preventing money laundering as outlined in this Guideline, the AML/CFT Act 2009, and AML/CFT Regulations 2010.

2.0 Cambios and Bureaus De Change CDD or KYC processes

The CDD / KYC processes for an MSB differ from those of a financial institution such as a bank in that an MSB typically provides occasional, transaction based services to walk in customers and generally does not open or maintain accounts.

However, considering the possible customer profile of MSB business, it might not in all cases be practicable or feasible for the same financial institutions standards as regards establishing KYC procedures to be fully applicable to all cambios and remittance company transactions.

Consequently, cambios and remittance companies will have to employ identification verification requirements which are more compatible with the nature of the

relationships generated by such businesses (whether customer-related or otherwise) but which achieves the basic principles of KYC.

The MSB should have procedures, which are effectively implemented and used to identify and verify, by examination of the customer's identification document(s) at the time the transaction is being conducted or the business relationship is being established the identity of:

(a) of each customer conducting or attempting to conduct a transaction at or above the legal monetary thresholds;
(b) of each customer that has an ongoing business relationship involving multiple transactions over a period of time with a cambio;

An MSB shall ensure that it knows the true identity of its customers when the total value of a transaction equals or exceeds G$20,000 (twenty thousand dollars) or foreign currency equivalent and a receipt must be issued. At all times the following details relating to a customer should be retained by a MSB:

(a) true name of the customer
(b) address of the customer (resident or business)
(c) identification details
(d) transaction amount (local and/or foreign currency equivalent)
(e) source of funds for large transactions

2.1 Reporting of Suspicious Business Transactions by MSB

In accordance with section 18 of the AML/CFT Act 2009, a MSB must pay special attention to all complex, unusual or large business transactions, whether completed or not, and to all unusual patterns of transactions and to insignificant but periodic transactions, which have no apparent economic or lawful purpose.

Upon reasonable suspicion that the transaction described above may constitute or relate to money laundering, proceeds or crime or terrorist financing, a MSB must promptly report the suspicious transaction to the Financial Intelligence Unit in the format specified by the FIU.

In addition regardless of whether a transaction is viewed as suspicious or not all purchases over G$400,000 (four hundred thousand) and sales over G$1,000,000 (one million) should be promptly reported to the FIU.

2.3 Appointment of a Compliance Officer

In accordance with section 19 (1) of the AML/CFT Act 2009 and section 11 of the AML/CFT Act 2010 an MSB is expected to appoint a Compliance Officer who will be tasked with ensuring compliance with the requirements of the AML/CFT Act 2009. Where the MSB has less than five employees, it is prudent to have someone designated as responsible for the AML/CFT compliance.

REFERENCE DOCUMENTS

Reference 1

Red Flags

Indicators of Suspicious Money Laundering and Terrorist Financing Transactions

Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Financial institutions are, therefore, required to put in place effective and efficient transaction monitoring programmes to facilitate the process.

Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering. This appendix, which lists various transactions and activities that indicate potential money laundering and terrorist financing, while not exhaustive, does reflect the ways in which money launderers have been known to operate.

Transactions or activities highlighted in this list are not necessarily indicative of actual money laundering if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here should put financial institutions on enquiry and provoke further investigation to determine their true legal status.

1. Insufficient or Suspicious Information

- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, financial statements anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- Customer is unwilling to provide personal background information when opening an account, cashing a cheque or purchasing negotiable

instruments.

- A customer's home or business telephone is disconnected.
- Customer's permanent home or business address is outside the financial institution's service area.

2. Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file an AML report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below the specified reporting threshold.
- Refusal or reluctance to proceed with a transaction, or abruptly withdrawing a transaction. A customer may be reluctant to proceed, or may even withdraw all or a portion of a transaction after being informed that a STR will be filed, or that a transaction will be recorded. This action would be taken to avoid AML reporting and recordkeeping requirements.
- Multiple third parties conducting separate, but related, non-reportable transactions. Customers who deposit cash by means of numerous credits so that the amount of each deposit is unremarkable, but the total of all the credits is significant, or similar deposits at a number of branches within a short space of time, all being credited to a central account. (This activity is often referred to as "smurfing.")
- Client is quick to volunteer that funds are "clean" or "not being laundered."

3. Funds Transfers

- A customer repeatedly sends or receives wire transfers of any amount when his/her business does not normally require or originate such transfers.
- Deposits followed within a short time by wire transfers to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Immediate conversions of funds transfers into monetary instruments in the name of third parties.
- Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws.
- Client makes frequent or large wire funds transfers for persons who have no account relationship with the institution.
- Many small, incoming transfers of funds are received, or deposits are made using cheques and bank drafts. Almost immediately, all or most of the transfers or deposits are transferred to another bank or wired to another country in a manner inconsistent with the customer's business or history.
- Wire transfers ordered in small amounts in an apparent effort to avoid triggering reporting requirements.
- Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel immediately or after a short time to a small number of foreign beneficiaries.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities/persons having no apparent business connection with the customer.
- Outgoing wire transfers requested by non-account holders. If paid in cash, the amount may be just under the reporting threshold to avoid the completion of Source

of Fund Declaration filing requirement. Alternatively, the transfer may be paid with several official checks or other monetary instruments.

4. Suspicious Customer Behaviour

- Customer has an unusual or excessively nervous demeanor
- Customer attempt to influence a bank employee not to file a Source of funds or STR report. This would involve any attempt by an individual or group to threaten, bribe, or otherwise corruptly influence a bank employee to bypass the filing of a Source of funds Declaration form or STR.
- Customer is accompanied and watched particularly where customer appears unaware, infirm or elderly and is accompanied by a non-relative.
- Customer shows uncommon curiosity about internal systems, controls and policies.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer over justifies or explains the transaction.
- Customer is secretive and reluctant to meet in person.
- Customer attempts to develop close rapport with staff.
- Customer insists that a transaction be done quickly.
- Customer spells his or her name differently from one transaction to another.
- Customer provides false information or information that you believe is unreliable.
- Customer offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- Customer makes it a habit to go to a specific cashier or frontline staff for all his/her transactions.

5. Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.

- A large volume of bank drafts, money orders, or funds transfers are deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.
- A business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- Goods or services purchased by the business do not match the customer's stated line of business.
- Corporate account shows little or no regular, periodic activity.
- Unexplained transactions are repeated between personal and business accounts.

6. Lending Activity

- A customer's financial statement makes representations that do not conform to international accounting standards.
- Customer suddenly repays a large problem loan with no plausible explanation for the source of funds.
- Customer purchases certificates of deposits using unknown source of fund and uses them as collateral for a loan.
- Customer defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans guaranteed by third parties with no apparent relation to the customer.
- Loans backed by assets, for which the source is unknown or the value has no relation to the situation of the customer.
- Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.

7. Changes in Bank-to-Bank Transactions

- Change in currency shipment patterns. Significant changes in currency shipment patterns between branches and/or Head Office as noted on cash shipment records may indicate a potential money laundering scheme occurring in a particular location.
- Large increase in the cash supply. A large, sustained increase in the cash balance would normally cause some concern. Another example of a red flag in this area would be a rapid increase in the size and frequency of cash deposits with no corresponding increase in non-cash deposits.
- Significant exchanges of small denomination bills for large denomination bills. Significant increases resulting from the exchange of small denominations for large denominations may be reflected in the cash shipment records.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.

8. Suspicious Non-Cash Deposits

- Customer deposits a large number of traveller's cheques often in the same denomination and in sequence.
- An incoming wire transfer followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party.
- Customer frequently shifts purported international profits by wire transfer out of the country.

9. Trade Finance

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in higher-risk jurisdictions.
- Customers shipping items through higher-risk jurisdictions, including transit through noncooperative countries.

- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.
- Customer seeks trade financing on the export or import of commodities whose stated prices are substantially more or less than those in a similar market situation.
- 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.

10. Suspicious Investment Activity

- Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- Investor seems unconcerned about the usual decisions to be made about an investment account such as fees or suitable investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions
- Customer deposits cash, traveller's cheques or bank drafts in amounts under the reporting threshold to fund an investment account.

11. Suspicious Safe deposit Box Activity

- Customer's activity increases in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash.

- Customer often visits the safe deposit box area immediately before making cash deposits or withdrawals of sums at or just below the reporting threshold.
- Customer rents multiple safe deposit boxes.
- Out-of-area customers. Safe deposit boxes may be opened by individuals who do not reside or work in the financial institution's service area.

12. Monetary Instruments

- Structured purchases of monetary instruments. An individual or group purchases monetary instruments with currency in amounts below the reporting threshold.
- Replacement of monetary instruments. An individual uses one or more monetary instruments to purchase another monetary instrument(s).
- Frequent purchase of monetary instruments without apparent legitimate reason. A customer may repeatedly buy a number of official bank drafts or traveller's cheques with no apparent legitimate reason.
- Deposit or use of multiple monetary instruments. The deposit or use of numerous official bank drafts or other monetary instruments, all purchased on the same date at different banks or different issuers of the instruments may indicate money laundering. These instruments may or may not be payable to the same individual or business.

13. Suspicious Employee Activity

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation.
- Employees may frequently submit incorrect or incomplete Source of Funds Declaration or STR forms

14. Other Unusual or Suspicious Customer Activity

- Customer does not want correspondence sent to home address

- A close relative or associate of a PEP's opens an account and begins making large deposits not consistent with the known legitimate sources of income of the family.
- Customer cash deposits often contain counterfeit bills or musty or extremely dirty bills.
- Customer frequently exchanges small-dollar denominations for large-dollar denominations
- Customer frequently deposits currency wrapped in currency straps of other banks or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Frequent exchange of cash into other currencies.
- Customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Early redemption of certificates of deposits.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Early redemption of certificates of deposits. A customer may request early redemption of certificates of deposits or investments within a relatively short period of time from the purchase date of the certificate of deposit or investment. The customer may be willing to lose interest or incur penalties as a result of the early redemption.
- Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account.
- Customer appears to have accounts with several financial institutions in one area for no apparent reason.
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client frequently uses many deposit locations outside of the home branch location.
- Staff is aware that aware that a customer is the subject of a money laundering or terrorist financing investigation.

- Staff is aware or become aware, from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
- Regular return of cheques for insufficient funds.
- Customer has no employment history but makes frequent large transactions or maintains a large account balance.
- Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Third parties make cash payments or deposit cheques to a customer's credit card.

Reference 2

Typologies
Money Laundering

1. Case Study One:

The case involved breach of trust by a bank employee with extensive AML/CFT training who had connections with a known drug dealer and his associates and who was able to convert criminal proceeds using wire transfers and bank drafts by circumventing internal procedures which were not sufficiently robust.

Details

A is an early twenties single parent who worked for about two years in a retail bank and received substantial anti-money laundering training which was augmented by further anti-money laundering training at another institution where the criminal activity was perpetrated. At both institutions, A had signed off on the training received, indicating that she understood the materials.

After just over one year, A was the subject of several internal Suspicious Activity Reports, one of which was subsequently filed with the local Financial Intelligence Unit. As a result of Production Orders and investigations, A, although not living extensively beyond her means, was able to pay off debts, meet other financial responsibilities and was shown as having close associations with a known local drug dealer.

A did not follow internal bank policies and procedures in conducting transactions, used the identification and password of a fellow employee to enter wire transactions into the bank's computer system which also included fictitious sender details and on some occasions A's own name was used but with a false address. A was arrested on suspicion of money laundering and search of a personal locker revealed two bank drafts executed just before arrest valued at US $12,000.00 and made in favour of recipients located in two jurisdictions one of which is a well known drug producing country.

A's modus operandi entailed processing wire transfers and bank draft purchases for various customers who did not hold accounts at the bank, and were operating on behalf of the local drug dealer. Many of the transactions were kept around US$3,000.00 and A would subsequently receive 10% of the value of each transaction. Over a nine month period 36 wire transfer and bank draft transactions were conducted involving a total of US$136,000.00.

Result
A pleaded guilty to five counts of money laundering amounting to US$35,000.00 and was sentenced to a period of imprisonment of 18 months suspended for two years, with a community service order for 18 months.

Source: Bermuda

2. Case Study Two
Drug trafficker concealing illegal proceeds by using wire transfers to open an account in a foreign bank, by purchasing real estate, motor vehicles and other high valued goods, and by investing in businesses through which illegal proceeds were laundered.

Details
A, a drug dealer was arrested by the competent authorities when attempting to traffic 1318 kilos of cocaine. Subsequent investigations revealed that A had deposited illegal proceeds in a bank in Country I then opened a savings account (high-interest deposit account with immediate access) with the money deposited. A requested a loan guaranteed by the same savings account and contracted a local company to manage the account, invest the money, sell and pay off the loan in the bank located in Country I. (The business of this firm was the construction of high-rise apartments). A also owned vehicle dealerships, petrol stations, farms, villas, yachts, helicopters and a number of other assets which were used to conceal his ill-gotten wealth.

Result
A has been extradited to the USA, and the assets have been confiscated.

Source: Dominican Republic

3. Case Study Three

A criminal gang in the business of extortion used the bank accounts of family members to conceal illegal proceeds which were in excess of anticipated deposits based on the profiles of the accounts.

Details

Country I is experiencing a serious problem of proliferation of criminal gangs. A who was a member of a criminal gang, by means of telephone calls, extorted money from various persons, threatening and coercing them to make deposits to accounts in the names of B, A's wife and C a relative of B. Deposits received in these accounts ranged from US $400.00 to US $2,000.00, and were then immediately withdrawn from ATMs. The total amount involved was US$23,000.00. C, according to the bank's opening of business form earned a salary US$250.00 per month.

Result

A was convicted of money laundering and imprisoned.

Source: Guatemala.

4. Case Study Four

Corruption at a government agency using wire transfers and cheques in order to channel funds to political parties during elections through a non profit organization which was 19 engaged to provide services not within its capacity.

Details

Political parties W and X in Country I were engaged in Presidential and Congressional election campaigns.

Y is described in its constitutive document as a non-profit association for total human development. Its objects are social services to the population and implementation of

health and education projects. The majority of Y's Board of Directors is composed of health professionals.

The functions of Government agency Z are mainly financial and a Task Force was formed, for the purpose of analysing, promoting and implementing actions conducive to administrative and financial improvement of the agency.

This task force contracted Y to provide advice on the needs of the agency and to propose structural and organisational reforms. For this purpose Government agency Z pays Y, by means of a transfer and cheques, a total of US $500,000.00.

Two days after the receipt of the money, Y issues two cheques totaling US $70,000.00 to political Party W and Political Party X, which were engaged in election campaigning.

Result
Money laundering conviction

Source: Guatemala

5. **Case Study Five**

A and B, a married couple, had made a large number of wire transfers totaling $55,390.00 over a period of six months which was high in comparison with their account profile. The transfers were made from an area considered to be high risk and the recipients were various persons in the border areas in other countries. The geographic pattern linked the transfers to the illegal traffic in persons. The illegal proceeds were used to purchase real estate and high valued goods such as vehicles.

Details

A and B over a period of six months, made 40 transfers totaling $55,390.00 to persons in various border areas of Republics I and II to beneficiaries who had no apparent family or obvious legal business relationship with A and B.

Bank X, the reporting institution to the Financial Intelligence Unit, maintains an account for a remittance company. The transfers by A and B were made from a branch of the remittance company in an area considered high risk for the transit of drugs and showed a geographic pattern of travel by the persons concerned to another country.

Furthermore A and B held four (4) accounts in different banks with balances of up to $20,000.00 into which deposits were made on a daily basis and from which withdrawals, transfers and the purchase of dollars were conducted. The source of these funds could not be determined.

At the couple's home documentation was found concerning houses, lands and transfer of vehicles that turned out to belong to customers who had moved to Republic II.

Result

The Ministerio Público (Public Prosecutor's Office) took the case to trial. A and B were convicted of money laundering, with the predicate offence of illegally trafficking in persons. Approximately $20,000.00, in cash as well as various dwelling houses and several vehicles were confiscated.

Source: Honduras

6. Case Study Six

Breach of trust by an employee of a financial institution who used a fictitious name to facilitate wire transfers of the illegal proceeds to associates in other countries and gave false information on the source of funds declaration.

Details

FIU in Country I received a Request for Assistance from Country II seeking the identification of funds on a bank account held by A in Country I.

It was alleged that the proceeds of a crime were wire transferred from Country II into A's account.

The funds purportedly came from B in Country II. B was an employee of a financial institution; and allegedly wire transferred employer's funds, without permission and acting in concert with individual C, to A's account in Country I.

B created a fictitious name that was used to facilitate the transfer of the funds through the banking system from Bank X in Country II to the bank in Country I.

The Financial Intelligence Unit made enquiries and located the wire transfer at an identified institution in Country I.

FIU observed that 11 days after the account was opened in Country I by a (native of Country I), one transaction valued overUS$300,000 was deposited into the account, via wire transfer from Country II. It was also noted that within two days of the deposit, A made several large withdrawals.

A then distributed the funds, via bank drafts. The bank drafts, each more than $5,000.00, were made out to individual D in Country I (A's relative); E in Country III; and company Y and company Z also in Country II.

When A opened the account in Country I, the source of funds was stated as "settlement of personal injury". However, the financial institution did not seek documentation in support of source of funds from A.

Result

B was charged with and subsequently convicted of Theft; Conspiracy to Steal; False Accounting; and Procuring Execution of Valuable Security by Deception. A and C were charged with Theft; and Conspiracy to Steal. C's trial is ongoing and A is still being sought by the authorities of Country I and Country II.

Remaining funds in the account of over US$100, 000.00 were frozen.

Source: St. Kitts and Nevis

7. Case Study Seven:

A senior government official launders embezzled public funds via members of his family.

The family of a former Country A senior government official, who had held various political and administrative positions, set up a foundation in Country B, a fiscally attractive financial centre, with his son as the primary beneficiary. This foundation had an account in Country C from which a transfer of approximately USD 1.5 million was made to the spouse's joint account opened two months previously in a banking establishment in neighbouring Country D. This movement formed legitimate grounds for this banking establishment to report a suspicion to the national FIU.

The investigations conducted on the basis of the suspicious transaction report found a mention on this same account of two previous international transfers of substantial sums from the official's wife's bank accounts held in their country of origin (A), and the fact that the wife held accounts in other national banking establishments also provisioned by international transfers followed by withdrawals. The absence of any apparent economic justification for the banking transactions conducted and information obtained on the initiation of legal proceedings against the senior government official in his country for embezzlement of public funds led to the presumption, in this particular case, of a system being set up to launder the proceeds of this crime. The official concerned was subsequently stopped for questioning and placed in police custody just as he was preparing to close his bank account. An investigation has been initiated.

8. Case Study Eight:

A senior employee of a state-owned company involved in high level corruption An investigation into a senior government official Mr A, an employee of state owned Company A, uncovered that he was in receipt of excessive payments into a number of accounts that he owned and operated. Mr. A was the vice president of Company A and had a yearly income of over USD 200,000. The investigation revealed Mr. A had 15 bank

accounts in several different countries through which over USD 200 million had been transacted.

Mr. A used the money placed in these accounts to gain political influence and to win large contracts from foreign governments on behalf of Company A.

The investigation discovered that a trust account had been created to act as conduit through which payments from Company A were then transferred to a number of smaller accounts controlled by Mr. A. Mr. A would then transfer money from these accounts or make cash withdrawals. The funds, once withdrawn were used to pay for bribes. The recipients of these payments included: heads of state and government, senior government officials, senior executives of state owned corporations and important political party officials in several countries and family members and close associates of Mr. A.

Further investigation into the financial transactions associated with the accounts held by Mr. A revealed that a shell company was being used to make and receive payments. In addition to account activity indicated there were irregular cash deposits (often more than one a day) and unusually large of cash withdrawals; one account revealed that in one six week period over USD 35 million had been withdrawn in cash. This was inconsistent with all the previous activity on the account. The investigators noticed that there was also a deliberate smurfing of the cash deposits into smaller amounts indicating Mr. A had an awareness of reporting requirements and was attempting to avoid them. The beneficial owners of payments from Mr. A made both in cash and by wire transfer implicated several PEPs and associates of PEPs:

The Senior Politician, Senior Official.

An intermediary received a payment of USD 50 million from Company A. The intermediary then transferred the money into two accounts held off-shore; the funds were then moved to company accounts that were also held offshore. The beneficial owners of these company accounts were discovered to be a former head of the secret service in Country B and a state secretary for the Ministry of Defence in Country C.

Wife of a PEP

Money was transferred from Company A to one of the bank accounts owned by Mr. A; Mr. A then placed funds into a solicitor's client account and an off-shore bank account. The beneficial owner of the off-shore account was the recently divorced wife of a PEP - Ms. C. The account was provided with funds for the purchase a property valued at over USD 500,000, a car, the redecoration of Ms. C's flat and a monthly allowance of USD 20,000.

Friend and associate of the PEP

Company A made a payment to a bank account in Country D. The bank in Country D was then instructed to make transfer the money to an associate of Mr. A, who held an account in the same bank in Country D. The associate then 'loaned' the same amount of money to a PEP.

9. Case Study Nine:

Accountant and lawyers assist in a money laundering scheme. Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and bank drafts on behalf of a drug trafficking syndicate who were importing of 24 kg of heroin concealed in cargo into Country Z. Bank drafts purchased from different financial institutions in Country Y (the drug source country) were then used to purchase real estate in Country Z.

An accountant was used by the syndicate to open bank accounts and register companies. The accountant also offered investment advice to the principals.

A firm of solicitors was also used by the syndicate to purchase the property using the bank drafts that had been purchased overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors

10. Case Study 10: An associate of a PEP launders money gained from large scale corruption

A video tape aired in Country A showed presidential adviser Mr. Z purportedly offering a bribe to an opposition politician. This publicity about Mr. Z, widely regarded as the power broker behind then-President in Country A, led the President to appoint a special prosecutor prompting numerous other investigations in Country A into the illicit activities of Mr. Z and his associates.

An investigation initiated by authorities in Country B authorities froze approximately USD 48 million connected to Mr. Z. Mr. Z fled the country and was eventually captured and extradited to Country A to face corruption, drug trafficking, illicit enrichment and other charges.

Prior to the capture of Mr. Z, an associate of Mr. Z, Mr. Y was arrested on a provisional arrest warrant and request for extradition from Country A. Mr. Z and his associates, including Mr. Y, generated the criminal proceeds forfeited in this case through the abuse of Mr. Z's official position as advisor to former the President of Country A. Some of the principal fraudulent schemes involved the purchase of military equipment and service contracts as well as the criminal investment of government pension funds.

Mr. Y was involved in a huge kickback scheme that removed money from both Country A's treasury and their military and police pension fund. Mr. Y and others used pension fund money and their own money to buy a majority interest in a Country C financial institution, Financial institutions M, which in June 1999 was bought by another financial institution in Country A. Mr. Y was in charge of seeking investments on behalf of Financial institution M and identified construction and real estate projects for the financial institutions and pension fund to finance. He also controlled the construction companies which built those projects. Mr. Y established a pattern of inflating the actual cost of the pension fund investment projects by 25 percent and billed Financial institution M accordingly. Projects recommended by Mr. Y were automatically approved by the board members at the police pension fund, as several of them received kickbacks. A

USD 25 million project was fraudulently inflated by USD 8 million. Similarly, Mr.Y covertly formed and controlled several front companies used to broker loans from Financial institution M in exchange for kickbacks from borrowers. When some loans defaulted, Mr. Y would purchase the financial institution's projects at extremely low prices for resale at a profit.

In addition, Mr. Y and members of Financial institution M's board of directors were authorised by Country A's government to arrange the purchase of military aircraft for the nation. In just two aircraft deals the government of Country A paid an extra USD 150 million, because of a fraudulent 30 percent mark-up added on to the sale price. This illicit money allegedly was funnelled through financial institution M. From there, it flowed into numerous accounts under a variety of names in financial institutions in foreign jurisdictions to conceal the origin of the funds.

Mr. Y consistently used a group of financial institutionss abroad to launder his and others' share of criminal proceeds. Ms. D, a financial institutioniser who is married to Mr. Y's cousin, formerly was a member of the board of directors of financial institution N, helped Mr. Y conceal more than US$ 20 million in one jurisdiction.

Mr. Y opened a financial institution's account in Country C, and moved about US$ 15 million through it until he was arrested. Initially, the account opening did not raise any suspicion because Country A nationals often opened financial institution accounts in the Country C to protect their assets from inflation. However, financial institutions holding financial institution and brokerage accounts owned or controlled by Mr. Y, Ms. D and others gradually noticed unusual activity in the accounts. According to financial institution officials, Mr. Y's financial transactions had no apparent business justifications and the origin of the funds was suspicious.

Reference 3

Typologies
Terrorist Financing

1. Case Study One: Exploitation of a legitimate charity

A suspicious transaction report (STR) was made following an attempt by Individual A, to deposit substantial amounts of cash into the account of a charity – over which he had power-of-attorney – with the instruction that it be transferred onward to a notary as an advance for the purchase of real estate.

The Investigation revealed that:

- Payments into the account consisted of multiple cash deposits (presumably donations) but also payments directly from the account of Individual A. In turn, A's personal account revealed multiple cash deposits that corresponded to donations from private individuals.

- The debit transactions consisted of transfers to the non-profit organisation (NPO) and international transfers to Individual B. Police sources revealed that A had links with individuals that were known for terrorist activities, including B.

- Law enforcement assessed that the charity, which continued to fulfill an important social function, was being exploited both as a "front' to raise funds and as a "means of transmission" to divert a portion of them to known terrorist associates of A.

Commentary: This case is indicative of the vulnerabilities to exploitation that arise with weak governance combined with high levels of cash deposits.

Source: Belgium.

2. Case Study Two:

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.

3. Case Study Three : 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.

4. Case Study Four: 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.

5. Case Study 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.

6. Case Study Six: 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.

7. Case Study Seven: A terrorist organization uses wire transfers to move money to further its activities across borders

A terrorist organization in Country X was observed using wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organization used "bridge" or "conduit" accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organization but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organization were deposited into financial institutions accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organization's future needs. Alternatively, the money was transferred to other financial institutions accounts managed by the organization's correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organization in its clandestine activities.

8. Case Study Eight: A NPO is used to transfer money to suspected terrorists

An FIU in Country A obtained updated information from the United Nations Security Council consolidated list of designated persons and entities. One of the organizations on the list conducted its operations under different variations of the same name in a number of countries. It was described as a tax-exempt NPO for which the stated purpose was to conduct humanitarian relief projects throughout the world. Among the multiple locations

provided UN list for branches of this organization, several of the addresses were in Country A.

The FIU received a suspicious transaction report on the NPO listed at one of the addresses indicated by the UN list. The report indicated financial institutions accounts and three individuals with controlling interest on the address in Country A. One of the individuals (Mr. A) had an address that matched one of the addresses indicated on the UN list, and the other two individuals had addresses in two different countries. A search by the FIU revealed that the Mr. A was linked to these organizations, as well as to four other international NPOs. Reports received by the FIU detail multiple wire transfers sent from locations of concern to the branches of the above-mentioned charity and to Mr. A.

Reference 4

Basic Trade-Based Money Laundering Techniques[1]

For the purpose of this guideline, trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include:

(i) Over- and under-invoicing of goods and services;
(ii) Multiple invoicing of goods and services;
(iii) Over- and under-shipments of goods and services; and
(iv) Falsely described goods and services

All of these techniques are not necessarily in use in every country.

1. Over and Under-Invoicing of Goods and Services

Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the good or service at a price below the "fair market" price, the exporter is able to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market.

Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market.

[1] Extracted from FATF document – Trade Based Money Laundering

(a) Over and Under-Invoicing of Goods – An Example

Company A (a foreign exporter) ships 1 million widgets worth $2 each, but invoices Company B (a colluding domestic importer) for 1 million widgets at a price of only $1 each.

Company B pays Company A for the goods by sending a wire transfer for $1 million. Company B then sells the widgets on the open market for $2 million and deposits the extra $1 million (the difference between the invoiced price and the "fair market" value) into a bank account to be disbursed according to Company A's instructions.

Alternatively, Company C (a domestic exporter) ships 1million widgets worth $2 each, but invoices Company D (a colluding foreign importer) for 1 million widgets at a price of $3 each. Company D pays Company C for the goods by sending a wire transfer for $3 million. Company C then pays $2 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced price and the "fair market" price) into a bank account to be disbursed according to Company D's instructions.

Several points are worth noting. First, neither of the above transactions would be undertaken unless the exporter and importer had agreed to collude. For example, if Company A were to ship widgets worth $2 each, but invoice them for $1 each, it would lose $1 million a shipment. Such a situation would not make sense unless the exporter and importer were colluding in a fraudulent transaction.

Second, there is no reason that Company A and Company B could not be controlled by the same organization. In turn, there is nothing that precludes a parent company from setting up a foreign affiliate in a jurisdiction with less rigorous money laundering controls and selling widgets to the affiliate at a "fair market" price. In such a situation, the parent company could send its foreign affiliate a legitimate commercial invoice (e.g. an invoice of $2 million for 1 million widgets) and the affiliate could then resell (and "re-invoice") these goods at a significantly higher or lower price to a final purchaser. In this way, the

company could shift the location of its over- or under-invoicing to a foreign jurisdiction where such trading discrepancies might have less risk of being detected.

Third, the over- and under-invoicing of exports and imports can have significant tax implications. An exporter who over-invoices the value of the goods that he ships may be able to significantly increase the value of the export tax credit (or valued-added tax (VAT) rebate) that he receives. Similarly, an importer who is under-invoiced for the value of the goods that he receives may be able to significantly reduce the value of the import duties (or customs taxes) that he pays. Both of these cases illustrate the link between trade-based money laundering and abuse of the tax system.

Research suggests that under-invoicing exports are one of the most common trade-based money laundering techniques used to move money. This reflects the fact that the primary focus of most customs agencies is to stop the importation of contraband and ensure that appropriate import duties are collected. Thus, customs agencies generally monitor exports less rigorously than imports.

It is also worth noting that the more complex the good being traded, the greater the difficulty that customs agencies will have in identifying over- and under-invoicing and correctly assessing duties or taxes. In part, this is because many customs agencies do not have access to data and resources to establish the "fair market" price of many goods. In addition, most customs agencies do not share trade data with other countries and therefore see only one side of the transaction. As such, their ability to identify incorrectly priced goods is often limited to those that are widely traded (and whose prices are widely quoted) in international markets.

2. Multiple Invoicing of Goods and Services

Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different

financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions. In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that there is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.

3. Over- and Under-Shipments of Goods and Services

In addition to manipulating export and import prices, a money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so-called "phantom shipment" are routinely processed. Banks and other financial institutions may unknowingly be involved in the provision of trade financing for these phantom shipments.

(i) Over- and Under-Shipment of Goods – An Example

Company E (a domestic exporter) sells 1 million widgets to Company F (a colluding foreign importer) at a price of $2 each, but ships 1.5 million widgets. Company F pays Company E for the goods by sending a wire transfer for $2 million. Company F then sells the widgets on the open market for $3 million and deposits the extra $1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company E's instructions.

Alternatively, Company G (a foreign exporter) sells 1 million widgets to Company H (a colluding domestic importer) at a price of $2 each, but only ships 500,000 widgets. Company H pays Company G for the goods by sending a wire transfer for $2 million. Company G then pays $1 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company H's instructions.

4. Falsely Described Goods and Services

In addition to manipulating export and import prices, a money launderer can misrepresent the quality or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

(i) Falsely Described Goods – An Example

Company I (a domestic exporter) ships 1 million gold widgets worth $3 each to Company J (a colluding foreign importer), but invoices Company J for 1 million silver widgets worth $2 each. Company J pays Company I for the goods by sending a wire transfer for $2 million. Company J then sells the gold widgets on the open market for $3 million and deposits the extra $1 million (the difference between the invoice value and the actual value) into a bank account to be disbursed according to Company I's instructions.

Alternatively, Company K (a foreign exporter) ships 1 million bronze widgets worth $1 each to Company L (a colluding domestic importer), but invoices Company L for 1 million silver widgets worth $2 each. Company L pays Company K for the goods by sending a wire transfer of $2 million. Company K then pays $1 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced value and the actual value) into a bank account to be disbursed according to Company L's instructions.