GOVERNMENT OF BARBADOS

GUIDELINE

FOR THE DETECTION AND PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM AND PROLIFERATION IN BARBADOS

For

Licensees and Registrants

Under

The Corporate and Trust Service Providers Act, 2015-12

The International Business Companies Act, Cap.77

The Societies With Restricted Liability Act, Cap. 318B

The Private Trust Companies Act, 2012-22

The Foundations Act 2013-2

And

The International Trusts Act, Cap. 245

International Business Division

In conjunction with the Anti-Money Laundering Authority

December, 2016

TABLE OF CONTENTS

Guideline for the Detection and Prevention of Money Laundering and Financing of Terrorism and Proliferation

INTRODUCTION

1. PURPOSE OF GUIDELINE

The purpose of the Guideline is to provide guidance to all licensees and registrants of the International Business Division on how they can fulfil their obligations in relation to the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA) and in doing so comply with the anti-money laundering and financing of terrorism and proliferation requirements of the Recommendations of the Financial Action Task Force (FATF). The Guideline should be read in conjunction with the MLFTA.

This Guideline, which is being issued in conjunction with the Anti-Money Laundering Authority ("Authority") pursuant to its powers under Section 26 of MLFTA, replaces any previous Guidance Notes of the International Business Division and is updated to reflect the changes in the MLFTA. The definitions appearing in the MLFTA apply *mutatis mutandis* to this Guideline.

2. MONEY LAUNDERING.

The term "money laundering" refers to all acts used to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. It is an attempt to convert "dirty money" to "clean money". There are three features common to persons engaged in this criminal conduct, namely that they seek:

(a) to conceal the true ownership and origin of criminal proceeds;
(b) to maintain control over them; and
(c) to change their form.

There are three stages of money laundering, which may occur in sequence but often overlap:

(1) **Placement** is the physical disposal of criminal proceeds, commonly in the form of cash which the criminal wishes to place in the financial system. Placement may be achieved through the placing of illicit cash on deposits at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt.

(2) **Layering** is the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy.

(3) **Integration** is the stage in which criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

Financing of Terrorism:

Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner through the use or threat of action. Successful terrorist groups may operate much like criminal organizations and are generally able to obtain sources of funding and develop means of concealing the links between those sources and the uses of the funds. This practice is intended to ensure that funds are available to facilitate the objectives of the terrorists. Consequently, money-laundering techniques are often employed in concealing terrorist financing.

Proliferation:

There are challenges posed by the threat of the proliferation of weapons of mass destruction (WMD). International efforts have been undertaken to co-ordinate participating states' actions, consistent with national legal authorities and relevant international law (e.g. United Nation Security Council Resolution 1540) and frameworks, to stop proliferation related trade in WMDs, related materials and delivery systems.

3. LEGISLATIVE AND REGULATORY FRAMEWORK

The Government of Barbados has enacted several pieces of legislation aimed at preventing and detecting drug trafficking, money laundering, terrorist financing and other serious crimes. These comprise**:**

(a) Drug Abuse (Prevention and Control) Act, 1990-14, CAP131;

(b) Proceeds of Crime Act, 1990-13, CAP143

(c) Mutual Assistance in Criminal Matters Act, 1992, CAP140A;

(d) Anti-Terrorism Act, 2002-6; Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23; and

(e) Transnational Organized Crime (Prevention and Control) Act, 2011.

This framework is supported by the International Business Division, which is responsible for international business entities licensed under the International Business Companies Act the Societies with Restricted Liability Act, the International Trust Act, the Corporate and Trust Service Providers Act, the Foundations Act and the Private Trust Companies Act.

4. OFFENCES

Section 5(1) of the Money Laundering and Financing of Terrorism (Prevention and Control) Act states that a person engages in money laundering where:

(a) The person engages, directly or indirectly, in a transaction that involves money or other property or a benefit that is proceeds of crime; or

(b) The person receives, possesses, conceals, disposes of, or brings into or sends out of Barbados any money or other property that is proceeds of crime.

It is not necessary for the original offence from which the proceeds stem to be committed in Barbados, so long as it would have been an offence had it taken place within Barbados.

5. INTERNATIONAL AND REGIONAL INITIATIVES

5.1 THE FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) was established in 1989 by the seven major industrialized countries of the world and other developed countries to combat money laundering. The FATF seeks to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. To achieve this objective, the FATF has developed Recommendations to establish a global standard. In 1990, the FATF issued its first 40 Recommendations to be implemented to fight money laundering and these recommendations were subsequently revised in 1996, 2001, 2003 and most recently in 2012. They have been renamed the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations.

5.2 THE CARIBBEAN FINANCIAL ACTION TASK FORCE

The Caribbean Financial Action Task Force (CFATF) is a regional organization, which had its genesis out of the Financial Action Task Force (FATF). This organization has as its mandate ensuring that the supervisory and regulatory practices are such within the Caribbean that they act as a deterrent to money laundering and financing of terrorism and proliferation and in cases where it does occur that it can be detected. Barbados is a member of the CFATF.

In order to assess the status of the anti-money laundering framework of their member countries, both the FATF and the CFATF undertake detailed reviews referred to as mutual evaluations. Barbados has had three rounds of mutual evaluations and the 3rd mutual evaluation report of Barbados was adopted in May 2008.

6. OTHER INTERNATIONAL ORGANISATIONS

Barbados is a member of the Group of International Finance Centre Supervisors as well as a member of the International Association of Insurance Supervisors and the International Organization of Securities Commissioners which have also been engaged in setting standards for anti- money laundering.

7. THE ANTI-MONEY LAUNDERING AUTHORITY

The Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 confers responsibility for the supervision of financial institutions to the Anti-Money Laundering Authority ("the Authority") which was officially established in August 2000.

In accordance with Section 9(1), the executive functions of the Authority are carried out by the Financial Intelligence Unit (FIU) which is headed by a Director. The Director is responsible for the general administration of the Money Laundering and Financing of Terrorism (Prevention and Control) Act. The Financial Intelligence Unit carries out the Authority's supervisory functions including the collecting, analyzing and disseminating of suspicious or unusual transactions reports from financial institutions and where necessary discloses such information to judicial and law enforcement authorities for prosecution. As it is a requirement for financial institutions to report all suspicious and unusual transactions to the Unit, it therefore serves as the central authority connecting the financial and law enforcement sectors.

8. SCOPE OF GUIDELINE

The Guideline provides guidance on the expectations of the International Business Division (IBD) concerning the activities of licensees and registrants (otherwise referred to as "Institutions") of the IBD. All institutions must develop their internal compliance systems and procedures and ensure that they are effective and up to date, so enabling them to effectively implement their duty of vigilance.

Although the *Money Laundering and Financing of Terrorism (Prevention and Control) Act* applies to all persons and businesses engaged in specified activities, additional administrative requirements are placed on a financial institution which is defined as;

(a) a person who conducts as a business one or more of the activities listed in the First Schedule of the MLFTA and includes:

(i) a trustee of an international trust within the meaning of the International Trusts Act who is resident in Barbados within the meaning of that Act;

(ii) an exempt insurance company within the meaning of the *Exempt Insurance Act*;

(iii) a person who operates an insurance business within the meaning of the *Insurance Act*;

(iv) a market actor, self-regulatory organization, participant and issuer of securities within the meaning of the *Securities Act*;

(v) a mutual fund and mutual fund administrator within the meaning of the *Mutual Funds Act* or any person who manages a mutual fund;

(vi) a licensee under the *Financial Institutions Act*;

(vii) a person who provides an international financial service within the meaning of the *International Financial Services Act*;

(viii) a building society within the meaning of *the Building Societies Act*;

(ix) a credit union within the meaning of the *Co-operative Societies Act;*

(x) a friendly society within the meaning of the *Friendly Societies Act*;

(xi) a foundation within the meaning of the *Foundations Act, 2013 (Act 2013-2)*;

(xii) a private trust company with the meaning of the *Private Trust Companies Act, 2012 (Act 2012-22)*

(b) a foreign sales corporation within the meaning of the Barbados Foreign Sales Corporation Act;

(c) an international business company within the meaning of the *International Business Companies Act*; and

(d) a society with restricted liability within the meaning of the *Societies With Restricted Liability Act*.

GROUP PRACTICE

Where a group whose headquarters is in Barbados operates branches or controls subsidiaries in another jurisdiction, it should:

(a) ensure that such branches or subsidiaries observe this Guideline and apply the higher of local and host standards;

(b) keep all such branches and subsidiaries informed as to current group policy;

(c) ensure that special attention is paid to foreign branches and subsidiaries that do not or insufficiently apply the FATF Recommendations;

(d) inform the IBD and the Reporting Authority when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures due to prohibitions by local laws, regulations or other measures; and

(e) ensure that each branch or subsidiary informs itself as to its own local reporting point equivalent to the Reporting Authority (Financial Intelligence Unit) in Barbados and that it is conversant with procedures for disclosure.

9. INTERNAL CONTROL AND PROCEDURES

9.1 THE DUTY OF VIGILANCE

Institutions must be constantly vigilant in deterring criminals from making use of any of the facilities described above for the purpose of money laundering or the financing of terrorism & proliferation. The task of detecting crime falls to law enforcement agencies. While financial institutions may on occasion be requested or, under due process of law, may be required to assist law enforcement agencies in that task, the duty of vigilance is necessary to avoid assisting the process of laundering and to react to possible attempts at being used for that purpose.

Thus the duty of vigilance consists mainly of the following elements:

(a) Verification;

(b) Risk Assessment

(c) Ongoing Due Diligence

(d) Recognition of suspicious transactions;

(e) Reporting of suspicion;

(f) Keeping of records; and

(g) Training.

Risk-Based Approach

All institutions should develop anti-money laundering policies and procedures capturing the above, and commensurate with:

(a) the size and the nature and complexity of activities;

(b) the complexity volume and size of transactions;

(c) the degree of risk associated with each area of operation;

(d) the type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP);

(e) type of product/service (e.g. whether international trust, or corporate and trust service provider);

(f) delivery channels;(e.g. whether internet banking, wire transfers etc.)

(g) geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking or corruption, whether the customer is subject to regulatory or public disclosure requirements);

(h) the internal audit and regulatory findings; and

(i) value of customer accounts and frequency of transactions

Senior management is responsible for the development of sound, up-to-date risk management programmes which are to be formally documented. They are also required to keep directors adequately informed about these programmes and their effectiveness.

The approach in designing these programmes requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. Risk should be assessed in relation to the customer base, products and services, delivery channels and geographic areas and ratings (e.g. low, medium, high) identified along with assigned actions for each rating type. Institutions are also required to implement appropriate mechanisms to provide this risk assessment information to the IBD or any related Self-Regulating body. Institutions' programmes should also observe higher/lower risks identified in risk assessments conducted by the International Business Division or in a national risk assessment and take

appropriate enhanced or simplified measures. (See Section 13 on Reduced Customer Due Diligence)

In keeping with Section 17 of the MLFTA, licensees and registrants, should apply customer due diligence standards on a risk sensitive basis depending on the type of customer, business relationship or transaction. Enhanced due diligence should be applied where the risk of being used for money laundering or terrorist financing is high. Reduced due diligence is acceptable for example, where information on the identity of the beneficial owner is publicly available or where checks and controls exist elsewhere in national systems.

Enhanced Due Diligence

An institution may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. An institution should 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. Institutions are required to observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, and financial institutions from listed countries.

Institutions perform their duty of vigilance by having in place systems that enable them to:

(a) determine (or receive confirmation of) the true identity of customers requesting their services through the use of reliable, independent source documents, data or information;

(b) understand and as appropriate obtain information on the purpose and intended nature of the business relationship and source of the funds;

(c) understand, record and retain information about the ownership and control structure of the customer where the customer is an entity whether financial or non-financial;

(d) identify the beneficial owners whether by declaration by the customer or through investigation;

(e) conduct ongoing due diligence on the business relationship, control structure, ownership and transaction 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, including, where necessary, the source of funds;

(f) update identification records and conduct retrospective due diligence on a risk-focused basis to ensure that all existing customer records are current and valid and conform to any new requirements

(g) recognize and report suspicious transactions to the Reporting Authority; in this respect any person who voluntarily discloses information to the Reporting Authority arising out of a suspicion or belief that any money or other property represents the proceeds of criminal conduct is protected by law under section 48(6) of the *Money Laundering and Financing of Terrorism (Prevention and Control) Act*, from being sued for breach of any duty of confidentiality;

(h) keep records for the prescribed period of time;

(i) train key staff;

(j) liaise closely with the Reporting Authority on matters concerning vigilance policy and systems;

(k) disclose to or allow timely access by the Competent Authority of current and all relevant information about the beneficial ownership and control of companies upon request; and

(l) ensure that internal auditing and compliance departments regularly monitor the implementation and operation of vigilance system.

10. TRAINING

In order to maximize vigilance and be adequately equipped to mitigate the threat of money laundering, financing of terrorism and proliferation, financial institutions should establish on-going employee training programs. Training should be targeted at all employees but added emphasis should be placed on the training of the compliance and audit staff because of their critical role in educating the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures. The appointment of a compliance officer at the management level is also a requirement of the compliance management arrangements for these institutions. Additionally, front office staff should be especially trained so as to enable them to respond appropriately when interacting with the public.

An ongoing AML/CFT training program should be implemented which is custom built to meet the needs of the specific business and the risks associated with that type of operation. The methods of money laundering, terrorist financing and proliferation are always evolving and changing as criminals try to stay ahead of the authorities. Consequently training must always reflect new techniques and trends in money laundering and the latest best practices and standards in order to stay abreast of this ever-changing area of criminal behavior.

This will make staff better able to identify suspicious behavior and transactions, identify high-risk business activities and clients such as Politically Exposed Persons (PEP).

Staff should have access to a compliance training manual and the relevant laws as part of their education in this area and these documents must be periodically updated to reflect any changes that have taken place. Periodic audits should also be done to determine whether the ongoing training is being effective in achieving the desired goals.

In order to maintain the integrity of the compliance regime and prevent misuse of the institution for criminal activity, it is essential that high standards be observed when hiring employees. The requisite due diligence should be undertaken on prospective staff with a risk based approach employed based on the position to be filled and the level of responsibility and access to sensitive information involved.

As an essential part of training, operational and other key staff members should receive a copy of the institution’s current compliance manual(s).

Institutions have a duty to ensure that key staff receive sufficient training to alert them to the circumstances whereby they should report customers/clients and/or their transactions to the internal compliance officer. Such training should include making key staff aware of the basic elements of:

(a) the *Money Laundering and Financing of Terrorism (Prevention and Control) Act*, the *Proceeds of Crime Act*, and any Regulations made and issued thereunder, and in particular the personal obligations of key staff thereunder, as distinct from the obligations of their employers thereunder;

(b) vigilance policy and vigilance systems;
(c) the recognition and handling of suspicious transactions;
(d) new techniques and trends in money laundering and financing of terrorism
(e) other pieces of anti-money laundering legislation identified under the Barbados Anti-Money Laundering Regime at the beginning of these notes; and
(f) any Code of Conduct issued by industry associations.

The effectiveness of a vigilance system is directly related to the level of awareness engendered in key staff both as to the background of international crime against which the Proceeds of Crime Act and anti-money laundering legislation have been enacted and these Guidelines issued, and as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

An effective, independent risk-based audit function should also be implemented to test and evaluate the system of vigilance.

10.1 TRAINING PROGRAMMES

While each institution should decide for itself how to meet the need to train members of its key staff in accordance with its particular commercial requirements, the following programs will usually be appropriate:

10.1.1 New employees

Generally training should include:

(a) the company's instruction manual;
(b) a description of the nature and processes of laundering;
(c) an explanation of the underlying legal obligations contained in the *Proceeds of Crime Act*, the *Money Laundering (Prevention and Control) Act* and any Regulations made or Code of Practice issued thereunder;
(d) an explanation of vigilance policy and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the Reporting Officer (or equivalent).

10.1.2 Specific appointees

Point of Contact staff

The first point of contact with money launderers is often with front office staff and their efforts are vital to the implementation of vigilance policy. They must be made aware of their legal responsibilities and the vigilance systems of the institution, in particular, the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Reporting Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with. This applies to account opening/new customer and new business staff/processing and settlement staff.

All such staff also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Reporting Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

10.1.3 Administration/operations supervisors and managers

A higher level of instruction covering all aspects of vigilance policy and systems must be provided to those with the responsibility for supervising or managing staff. This should include:

(a) the *Proceeds of Crime Act*, the *Money Laundering (Prevention and Control) Act* and Regulations issued thereunder;
(b) procedures relating to the service of production and restraint orders;
(c) internal reporting procedures; and
(d) the requirements of verification and records.

UPDATES AND REFRESHERS

It will also be necessary to make arrangements for updating and refresher training at regular intervals to ensure that key staff remain familiar with and are updated as to their responsibilities.

10.2 THE REPORTING OFFICER

All institutions are required to appoint a Reporting Officer as the point of contact with the Reporting Authority in the handling of cases of suspicious customers and transactions. The Reporting Officer must be a senior member at the management level with the necessary authority and independence to ensure compliance with these Guidelines.

An institution should have a Reporting Officer who is resident in Barbados and who must be in a position to readily respond to the Regulator and FIU on AML/CFT issues. The Reporting Officer is the point of contact between the institution and the Financial Intelligence Unit as well as the Regulator. Institutions large enough to have a compliance or fraud department will be required to appoint a Reporting Officer from within one of these departments.

However, where the institution is part of a larger regulated group or entity, the Group Reporting Officer or Group Internal Audit may perform the reporting function, once approved by the Regulator.

Where this is not possible, an institution may, subject to the Regulator's approval, outsource the operational aspects of the compliance or internal audit function to an independent person or firm that is not involved in the auditing or accounting functions of the institution.

Notwithstanding, the responsibility for compliance with the MLFTA and this Guideline remains that of the institution.

In-depth training concerning all aspects of the relevant laws, vigilance policy and systems will be required for the Reporting Officer. In addition, the Reporting Officer will require

extensive initial and continuing instruction on the validation and reporting of unusual and suspicious transactions and on the feedback arrangements.

11. THE DUTY OF VIGILANCE OF EMPLOYEES

It cannot be stressed too strongly that all employees are at risk of being or becoming involved in criminal activity if they are negligent in their duty of vigilance and they should be aware that they face criminal prosecution if they commit any of the offences under the *Proceeds of Crime Act* and the *Money Laundering and Financing of Terrorism (Prevention and Control) Act*.

Licensees should undertake due diligence on prospective staff members. This includes:

a) Verifying 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.

c) Maintain an on-going approach to screening for specific positions, as circumstances change, or for a comprehensive review of departmental staff over a period of time. Internal policies and procedures should be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing staff; and

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

11.1 THE CONSEQUENCES OF FAILURE

For the institution involved, the first consequence of failure in the duty of vigilance is likely to be commercial. Institutions which, however unwittingly, become involved in money laundering, risk the loss of their good market name and position and the incurring of non-productive costs and expenses.

The second consequence may be to raise issues of supervision and fit and proper standing.

The third consequence is the risk of criminal prosecution of the institution for the commission of an offence under the *Money Laundering and Financing of Terrorism (Prevention and Control) Act* and the *Proceeds of Crime Act*.

For the individual employee it should be self-evident that the consequences of failure are not dissimilar to those applicable to institutions. The employee's good name within the industry is likely to suffer and he or she may face the risk of prosecution for the commission of an offence under the *Money Laundering and Financing of Terrorism (Prevention and Control) Act* and the *Proceeds of Crime Act*.

OFFENCES AND PENALTIES IMPOSED UNDER THE MLFTA

Please refer to **Appendix 1** for a full description of the offences and penalties imposed for non-compliance with the provisions of the Act.

11.2 CUSTOMER DUE DILIGENCE

For the purpose of this Guideline an institution must implement all reasonable measures to determine the ultimate beneficial ownership information on all verification subjects before submission of applications for licensing. This is especially important where intermediaries such as lawyers, financial planners or advisors, accountants, business introducers or other professional service providers purport to act on behalf of a customer.

Ultimately the licensee is responsible for verifying the identity of their customers and must establish procedures for obtaining identification information on all new customers so as to be satisfied that the identification given is correct. At a minimum all reasonable measures must be used to verify and document the identity of the customer or account holder from the beginning of a business relationship.

11.3 Declarations

It should be noted that a licensee or registrant cannot conduct due diligence on themselves as this would clearly be a conflict of interest and would not satisfy international best practice standards as reflected in the FATF Recommendations.

As a consequence, a licensee or registrant is prohibited from declaring themselves as “fit and proper” to conduct business in Barbados. Such declarations must be made by an independent third-party who is held liable at law for having stated that they have conducted the requisite due diligence prior to making the declaration.

The following points of guidance will apply according to:

(a) the legal personality of the applicant for business (which may consist of a number of verification subjects); and

(b) the capacity in which he/she is applying.

Institutions are required to carry out verification in respect of all of the parties authorized to access the account. Where there are underlying principals, however, the true nature of the relationship between the principals and the account signatories must also be established and appropriate enquiries performed on the former, especially if the signatories are accustomed to acting on their instruction. In this context “principals” should be understood in its widest sense to include, for example, beneficial owners, settlors, controlling shareholders, directors, beneficiaries etc., but the standard of due diligence will depend on the exact nature of the relationship.

11.4 Politically Exposed Persons (PEPs)

Additionally, institutions are required to have an appropriate system to determine whether the verification subject is a Politically Exposed Person (PEP) whether foreign or domestic. A PEP is an individual, family member of an individual or a socially or professionally connected person to the individual who has or has been entrusted with prominent public function or connected with an international organization.

Because of the potential for abuse of power by public officials for their own enrichment and possible legal and reputational risks which may be faced by licensees, enhanced due diligence is recommended when dealing with PEPs.

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), should be required in addition to performing normal customer due diligence measures, to also:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
(c) take reasonable measures to establish the source of wealth and source of funds; and
(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

The FATF Recommendations categorize PEPs as follows:

(a) Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State

(b) or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;
(c) Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government,

senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

(d) Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

12. VERIFICATION SUBJECT

12.1 Individuals

The verification subject may be the account holder himself or one of the principals to the account.

An individual trustee should be treated as a verification subject unless the institution has completed verification of that trustee in connection with a previous business relationship or one-off transaction and termination has not occurred. Where the applicant for business consists of individual trustees, all of them should be treated as verification subjects.

12.2 Beneficial Ownership of Trusts:

All persons and institutions must implement all reasonable measures to determine the ultimate beneficial ownership information related to any Trust for which they act. This applies to all Settlors, Beneficiaries, Controllers, Trustees, lawyers or any other Service Provider who acts on behalf of the Trust.

At a minimum, the licensee should obtain the following:

(a) Name of trust;
(b) Nature/type of trust
(c) Identity of the trustee(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;

(d) Identity of person(s) with powers to add beneficiaries where applicable, identity of person providing the funds, if not the ultimate settlor; and
(e) Any other natural person exercising effective control over the trust (including through a chain of control/ownership).

Depending on the type or nature of the trust, it may be impractical to obtain to obtain all of the above at the onset of the relationship e.g. unborn beneficiaries. In such cases, discretion should be exercised and documented in a manner consistent with the requirements in this Guideline. In all circumstances, the licensee should verify beneficiaries before the first distribution of assets. Further, licensees should verify protectors/controllers the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

Ongoing due diligence should be applied in the context of changes to 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.

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

12.3 Ownership of Foundations:

All persons and institutions must implement all reasonable measures to determine the ownership information related to any Foundation for which they act. This applies to all Founders, Beneficiaries, Councillors, Guardians, lawyers or any other Service Provider who acts on behalf of the Foundation.

12.4 Partnerships

Institutions are required to treat as verification subjects all partners of an applicant firm which is an applicant for business who are relevant to the application and have individual authority to operate a relevant account or otherwise to give relevant instructions. Verification must proceed as if the partners were directors and shareholders of a company in

accordance with the principles applicable to non-quoted corporate applicants (see below). In the case of a limited partnership, the general partner should be treated as the verification subject. Limited partners need not be verified unless they are significant investors**.**

12.5 Companies (including corporate trustees)

All persons and institutions must implement reasonable measures for identifying and verifying the beneficial owner and those in control of the company, such that they are satisfied that they know their customers. For legal persons (and arrangements) this should include the institution understanding the ownership and control structure of the customer.

12.6 Other institutions

Where an applicant for business is not a firm or company (such as a charity, etc), all signatories who customarily have access to the account must be treated as verification subject(s).

12.7 Intermediaries: Professional Service Providers

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

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

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

(c) 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.

Where pooled accounts are managed by:

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

(b) Lawyers or stockbrokers representing funds held on deposit or in escrow for several individuals, and funds being held are not co-mingled (i.e. there are sub-accounts), the licensee should identify each beneficial owner. Where funds are co-mingled, the licensee should take reasonable measures to identify the beneficial owners. Subject to the Bank's approval, the latter is not required where the provider employs at a minimum, equivalent due diligence standards as set out in this Guideline and has systems and controls to allocate the assets to the relevant beneficiaries. Licensees should apply the criteria at Section 7.4.4 above in conducting due diligence on providers.

Licensees should observe guidance from the Financial Intelligence Unit regarding attorney-client accounts.

13. REDUCED CUSTOMER DUE DILIGENCE

As discussed in Section 9.1, the institution's policy document should clearly define the risk approach and associated due diligence, monitoring and other requirements. An institution may only apply reduced due diligence to a customer provided it satisfies itself that the customer is of such risk level that qualifies for this treatment. The institution's satisfaction should be based on the identification of lower risks, through its internal risk analysis, a national risk assessment or risk analysis by the IBD.

However, where an institution knows or suspects that money laundering or terrorist financing is or may be occurring or has occurred, reduced/simplified concessions as set out below do not apply and the case should be treated as a case requiring refusal and, more important, reporting. Reduced due diligence may be considered where an application to conduct business is made by:

(a) An entity licensed under IFSA or FIA;
(b) An entity registered under the *Securities Act* or the *Mutual Funds Act*;
(c) An entity licensed under the *Insurance Act* or *Exempt Insurance Act*;
(d) An entity licensed under the *Cooperatives Society Act*, *Friendly Societies Act* or *Building Societies Act*;

(e) The Government of Barbados; or

(f) A statutory body.

13.1 INTRODUCED BUSINESS

A licensee may rely on other regulated third parties to introduce new business in whole or in part but ultimately the licensee remains responsible for customer identification and verification. As a safeguard the licensee should:

(a) Have a written agreement that clearly outlines the respective responsibilities of the two parties;

(b) Ensure that the regulated entity or introducer has established Know Your Customer (KYC) practices at least equivalent to those required by Barbados law and the licensee itself;

(c) Be satisfied that the quality and effectiveness of supervision and regulation in the introducer's country of domicile meets the standard set by FATF Recommendations 26, 27 and 28; and satisfy itself that the introducer is regulated, and supervised or monitored for, and has measures in place for compliance with CDD and record-keeping requirements in line with FATF Recommendations;

(d) Obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;

(e) Conduct periodic reviews to ensure that the introducer continues to conform to the criteria set out above;

(f) Consider termination of the relationship where an introducer fails to provide the requisite customer identification and verification documents; and

(g) Consider termination of the relationship with an introducer who is not within the licensee's group, where there are persistent deviations from the written agreement.

When a prospective customer is introduced from within a licensee's group, provided the identity of the customer has been verified by the introducing regulated parent company, branch, subsidiary or associate in line with the standards set out in the Guideline, it is not necessary to re-verify the identification documents unless doubts subsequently arise about

the veracity of the information. The licensee should however, retain copies of the identification records in accordance with the requirements in the MLFTA. Licensees should obtain written confirmation from a group member confirming completion of verification.

13.2 TIMING AND DURATION OF VERIFICATION

Whenever a business relationship is to be formed or a significant one-off transaction is undertaken, the institution should establish the identity of all verification subjects arising out of the application for business either by:

(a) carrying out the verification itself, or

(b) by relying on the verification of others in accordance with these Guidelines.

Where a transaction involves an institution and an intermediary, each needs separately to consider its own position and to ensure that its own obligations regarding verification and records are duly discharged.

The best time to undertake verification is not so much at entry as prior to entry. Verification should, whenever possible, be completed before any transaction is completed, subject to the provisions above. If it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this must be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior manager and the compliance officer may give appropriate authority. This authority should not be delegated. Any such decision must be recorded in writing.

Verification, once begun, should normally be pursued either to a conclusion or to the point of refusal. If a prospective customer does not pursue an application, key staff may (or may not) consider that this is in itself suspicious. In the event that the attempted or aborted transaction is reasonable considered to be suspicious, the transaction must be reported to the Reporting Officer.

In cases of non- face-to-face business where payment is, or is expected, to be made from a bank or other account, the verifier must:

(a) satisfy himself/herself that such account is held in the name of the applicant for business at or before the time of payment, and

(b) not remit the proceeds of any transaction to the applicant for business or his/her order until verification of the relevant verification subjects has been completed.

13.3 METHODS OF VERIFICATION

This Guideline does not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification but seeks to outline the basic mandatory requirements as a matter of good practice.

However, this Guideline is not exhaustive and there may be cases where it would be reasonable to expect an institution to take additional measures to properly satisfy itself that verification has been achieved.

Verification is a cumulative process. Except for one-off transactions as described at 13.0 above, it is not appropriate to rely on any single piece of documentary evidence. The best possible documentation of identification should be required and obtained from the verification subject. For this purpose ‘best possible” is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

File copies of documents must be retained.

The process of verification should not be compromised by the particular type of account or service being applied for.

13.3.1 Individuals

A personal introduction from a known and respected customer (who is not third party regulated by these guidelines) and/or member of key staff is often a useful aid but it would not remove the need to verify the subject in the manner provided in this Guideline. It should

in any case contain the full name and permanent address of the verification subject and as much as is relevant of the information outlined above.

Except in the case of reliable introductions, the institution should, whenever feasible, interview the verification subject in person.

The relevance and usefulness in this context of the following personal information must be considered:

(a) full name(s) used
(b) date and place of birth
(c) nationality
(d) current permanent address including postcode, any address printed on a personal account cheque tendered to open the account, if provided, should be compared with this address
(e) occupation and name of employer (if self-employed, the nature of the self-employment)
(f) specimen signature of the verification subject official.

In this context “current permanent address” means the verification subject’s actual residential address as it is an essential part of identity.
To establish identity, the following documents are considered to be the best possible, in descending order of acceptability:

(a) telephone and fax number
(b) current valid passport
(c) National identity card
(d) Armed Forces identity card
(e) driving license which bears a photograph

Documents sought must be pre-signed.

Documents which are easily obtained in any name should not be accepted uncritically. Examples include:

(a) birth certificates

(b) an identity card issued by the employer of the applicant even if bearing a photograph
(c) credit cards
(d) business cards
(e) national health or insurance cards
(f) provisional driving licenses
(g) student union cards

It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where appropriate documentary evidence of identity and independent verification of address are not possible. In such cases a senior member of key staff could authorize the opening of an account if they are satisfied with the circumstances and must record these circumstances in the same manner and for the same period of time as other identification records.

If the verification subject is an existing customer of an institution referenced at Section 13.1 above, which is acting as intermediary in the application, the name and address of that institution and that institution's personal reference on the verification subject should also be recorded.

13.3.2 Companies

All account signatories should be duly accredited by the company. The relevance and usefulness in this context of the following documents (or their foreign equivalent) should be carefully considered:

(a) Certificate of Incorporation,
(b) the name(s) and address(es) of the beneficial owner(s) and/or the person(s) on whose instructions the signatories on the account are empowered to act,
(c) Memorandum and Articles of Association;
(d) Resolution, bank mandate, signed application form or any valid account opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;

(e) Copies of Powers of Attorney or other authorities given by the directors in relation to the company;

(f) a signed director's statement as to the nature of the company's business.

As legal requirements vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

Partnerships

The relevance and usefulness of obtaining the following (or their foreign equivalent) should be carefully considered as part of the verification procedure:

(a) the partnership agreement, and

(b) information listed above under 13.3 (1) in respect of the partners and managers relevant to the application for business.

13.4 RESULT OF VERIFICATION

Satisfactory

Subject to the keeping of records in accordance with this Guideline and the MLFTA, once verification has been completed further verification checks are periodically needed when transactions are subsequently undertaken. The file of each applicant for business must show the steps taken and the evidence obtained in the process of verifying each verification subject.

Unsatisfactory

In the event of failure to complete verification of any relevant verification subject and where there are no reasonable grounds for suspicion, any business relationship with or one-off transaction for the applicant for business should be suspended and any funds held to the applicant's order returned until verification is subsequently completed (if at all). Funds should never be returned to a third party but only to the source from which they came. If failure to complete verification itself raises suspicion, the Reporting Officer should make a report to the Reporting Authority.

14. RECOGNITION OF UNUSUAL/SUSPICIOUS TRANSACTIONS

A suspicious transaction will often be one which gives rise to reasonable grounds to suspect that it is related to the commission of a money laundering or terrorism offence. It follows that an important pre-condition of recognition of a suspicious transaction is for the institution to know enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual. Unusual transactions are not necessarily suspicious, but should give rise to further enquiry and analysis. In this regard, licensees 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.

This Guideline is not intended to focus on new business relationships and transactions alone. 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 behavior of an account.

Suspicious transactions should be cognizable as falling into one or more of the following categories:

(a) any unusual transaction in the course of some usual financial activity;
(b) any unusually-linked transactions;
(c) any unusual employment of an intermediary in the course of some usual transaction or financial activity;
(d) any unusual method of settlement; or
(e) any unusual or disadvantageous early redemption of an investment product.

15. REPORTING OF SUSPICION

Reporting of suspicion is important as it provides a defence against a possible accusation of assisting in the retention or control of the proceeds of criminal conduct or of acquiring, possessing or using the proceeds of criminal conduct. It should be noted in this context that suspicion of criminal conduct is more than the absence of certainty that someone is innocent. It is rather an inclination that there has been criminal conduct.

Institutions should ensure that the key staff knows to whom their suspicions should be reported; and that there is a clear procedure for reporting such suspicions without delay to the Reporting Officer.

Key staff must be required to report any suspicion of laundering directly to the Reporting Officer.

Employees must comply at all times with the approved vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to their Reporting Officer.

On receipt of a report concerning an unusual transaction, the Reporting Officer must determine whether the information contained in such report, reaches the level of suspicion. If so, a report should be submitted to the Reporting Authority.

If the Reporting Officer decides that the information does substantiate a suspicion of laundering or terrorist financing, he is required to disclose this information promptly. If the Reporting Officer reasonably believes that carrying out customer due diligence procedures will tip-off the customer, he should be permitted not to pursue the procedures and instead should be required to file a Suspicious Transaction Report (STR) promptly. If he is genuinely uncertain as to whether such information substantiates a suspicion, he should nevertheless, report to the Reporting Authority. If in good faith he decides that the information does not substantiate a suspicion, he must record fully the reasons for his decision not to report to the Reporting Authority.

16. REPORTING TO THE REPORTING AUTHORITY

If the Reporting Officer decides that a disclosure should be made, a Suspicious Transaction Report, in standard form found at **Appendix 3** should be sent to the Reporting Authority.

If the Reporting Officer considers that a report should be made urgently (e.g. where the account is already part of a current investigation), initial notification to the Reporting Authority should be made by facsimile.

Where a report is made to the Reporting Authority, the Authority may seek further information from the reporting institution and elsewhere. It is important to note that after a reporting institution makes an initial report in respect of a specific suspicious transaction, that initial report does not relieve the institution of the need to report further suspicions in respect of the same customer or account. The institution should therefore report any further suspicious transactions involving that customer.

Discreet inquiries are made to confirm the basis for suspicion but the customer is never approached. In the event of a prosecution, the source of the information is protected, as far as the law allows. Production orders are used to produce such material for the Court. Maintaining the integrity of the confidential relationship between law enforcement agencies and institutions is regarded to be of paramount importance.

Vigilance systems must require the maintenance of a register of all reports made to the Reporting Authority pursuant to this section. Such register should include such details as:

(a) the date of the report;
(b) the person(s) to whom the report was forwarded;
(c) a reference by which supporting evidence is identifiable; and
(d) receipt of acknowledgment from the Reporting Authority.

17. KEEPING OF RECORDS

To demonstrate compliance with the MLFTA and to allow for timely access to records by the IBD or the Reporting Authority, licensees should establish a document retention policy that provides for the maintenance of a broad spectrum of records including the following:

(a) Entry records: institutions must keep all account opening records, including verification documentation and written introductions, for a period of at least 5 years after termination or, where an account has become dormant, 5 years from the last transaction.

(b) Ledger records: institutions must keep all account ledger records for a period of at least 5 years following the date on which the relevant transaction or series of transactions is completed.

(c) Supporting records: institutions must keep all records in support of ledger entries, including credit and debit slips and cheques, for a period of at least 5 years following the date on which the relevant transaction or series of transactions is completed.

Licensees should also maintain records on internal and external reports. Where an investigation into a suspicious customer or a suspicious transaction has been initiated, the Reporting Authority may request an institution to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where an institution knows that an investigation is proceeding in respect of its customer, it should not, without the prior approval of the Reporting Authority, destroy any relevant records even though the prescribed period for retention may have elapsed.

Accounting Records:

Licensees and registrants must keep reliable accounting records that correctly explain all transactions, enable the financial position to be determined with reasonable accuracy at any time and allow for the preparation of financial statements. The accounting records required to be kept must be preserved for a period of not less than 5 years after the end of the period to which they relate.

18. CONTENTS OF RECORDS

Records relating to verification must generally comprise:

(a) a description of the nature of all the evidence received relating to the identity of the verification subject; and

(b) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Records relating to transactions must generally comprise:

(a) details of personal identity, including the names and addresses, of:

a. the customer;
b. the beneficial owner of the account or product;
c. any counter-party;

(b) details of securities and investments transacted including:

a. the nature of such securities/investments;
b. valuation(s) and price(s);
c. memoranda of purchase and sale;
d. source(s) and volume of funds;
e. destination(s) of funds;
f. memoranda of instruction(s) and authority(ies)
g. book entries;
h. custody of title documentation;
i. the nature of the transaction;
j. the date of the transaction;
k. the form (e.g. cash, cheque) in which funds are offered and paid out.

Records relating to accounting must generally comprise:

(a) underlying documentation, such as invoices, contracts, etc. and should reflect details of

a. all sums of money received and expended and the matters in respect of which the receipt and expenditure takes place;
b. all sales and purchases and other transactions; and
c. the assets and liabilities of the licensee or registrant.

Institutions should keep all relevant records in readily retrievable form and be able to access records without undue delay. A retrievable form may consist of:

(a) an original hard copy;
(b) microform; or
(c) electronic data.

Records held by third parties are not regarded to be in a readily retrievable form unless the institution is reasonably satisfied that the third party is itself a regulated institution, which is able and willing to keep such records and provide same when required.

Institutions should ensure that records held by an affiliate, branch or subsidiary outside Barbados; or head office; that act as an introducer, at a minimum, comply with the requirements of Barbados law and this Guideline.

Where the Reporting Authority requires sight of records which according to an institution's vigilance systems would ordinarily have been destroyed, the institution is nonetheless required to conduct a search for those records and provide as much detail to the Reporting Authority as possible.

19. REGISTER OF ENQUIRIES

An institution must maintain a register of all enquiries made to it by the Reporting Authority. The register should be kept separate from other records and contain at a minimum the following details:

(a) the date and nature of the enquiry; and

(b) details of the account(s) involved should be maintained for a period of at least 5 years.

20. FIDUCIARY SERVICES

For the purpose of this Guideline "fiduciary services" comprise any of the following activities carried on as a business, either singly or in combination: (a) trust services, where provided to an international trust or private trust company;

(a) acting as corporate and/or individual trustee;

(b) providing the services of a registered office or otherwise acting as a person authorized to accept service or correspondence

(c) formation and/or administration of Barbados and/or foreign-registered companies;

(d) provision of corporate and/or individual directors;

(e) opening and/or operating bank accounts on behalf of clients.

A “fiduciary’ is any person duly licensed and carrying on any such business in or from within Barbados. Fiduciaries should comply with this Guideline.

20.1 VERIFICATION

Good practice requires key staff to ensure that engagement documentation (client agreement etc.) is duly completed and signed at the time of entry.

Verification of new clients should include the following or equivalent steps:
where a settlement is to be made or when accepting trusteeship from a previous trustee, the settlor, and/or where appropriate the beneficiaries, should be treated as verification subjects;

(a) in the course of company formation, verification of the identity of beneficial owners.

(b) the documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client’s affairs should include a note of any required further input on verification from any agent/intermediary of the new client, together with a reasonable deadline for the supply of such input, after which suspicion should be considered aroused.

20.2 CLIENT ACCEPTANCE PROCEDURES

20.2.1 Independent Audit Function

A service provider should obtain a separate report on its compliance with the client acceptance and other procedures from an independent person.

20.2.2 Procedures for Professional Service Clients “PSC”

The definition of ‘PSC” is an organization or person, such as a law firm, an accountant, or a similar professional organization which contracts the services of a service provider on behalf of its clients.

A service provider should obtain from each PSC that instructs a service provider, details of the business address, contact communication numbers and principals or professionals involved in the PSC. A service provider should obtain evidence of first hand involvement in the verification of those details.

A service provider should obtain satisfactory sources of reference to provide adequate indication of the reputation and standing of the PSC.

A service provider should retain records for a period of five (5) years following the discontinuation of the service provided to the PSC.

Before a service provider undertakes to form a company, on the instructions of a PSC the service provider should take reasonable steps to ensure that the PSC has adequate due diligence procedures in place.

20.2.3 Procedures for End User Clients "EUC"

The definition of 'EUC" is a client of a service provider who contracts services of a service provider for its own benefit.

A service provider should maintain written procedures to ensure that the identity of each EUC is known.

A service provider should maintain records for a period of five (5) years following the discontinuation of the service provided to the EUC.

A service provider should maintain on its file a reference from a recognized bank in respect of the EUC.

The service provider should maintain on its file a copy of the individual's passport or identity card with photo identification, when instructed by an individual.

A service provider should maintain on its file contact communication numbers and addresses for each EUC and should annually remind the EUC that it should notify the

service provider within a reasonable period of any change of such EUC's communication numbers and addresses and that it should advise the service provider of any changes in share ownership. The latter should be reflected in the share register of any company incorporated on behalf of the EUC.

Where, prior to the coming into force of any enactment or this Guideline a service provider has not obtained communication numbers, addresses, references or passport or identity card with photo identification as referred to herein, the service provider should obtain any such items on the basis of materiality and risk at appropriate times, or by any such period determined by the International Business Division.

20.2.4 **Additional Requirements Where Fiduciary Services are provided**

A service provider should to the extent relevant to the services being provided, maintain on its files. evidence of the opening of bank and investment accounts, and copies of a statement of those accounts.

A service provider should to the extent relevant to the services being provided, maintain on its files in respect of clients for whom it provides fiduciary services:

(a) copies of minutes of meetings of shareholders;
(b) copies of minutes of meetings of directors;
(c) copies of minutes of meetings of committees;
(d) copies of registers of directors, officers and shareholders; and
(e) copies of registers of mortgages, charges and other encumbrances.

The service provider should obtain satisfactory references in accordance with the above on the party giving the instructions for the engrossment or appointment of a new trustee, where such instructions are accepted by a service provider to act as trustee for a trust. The service provider should satisfy itself that assets settled into the trust are not or were not made as part of a criminal or illegal transaction to dispose of assets.

Appendix 1: Summary of Money Laundering and Terrorism Sanctions and Offences
Appendix 2: Declaration of Source of Funds/Wealth
Appendix 3: Suspicious / Unusual Transaction Report.

Appendix 1 - Summary of Money Laundering and Terrorism Sanctions and Offences

Area	Description of Offence / Breach	Description of Fine / Sanction	Section of Legislation
Reporting Obligations	Failure of a financial institution to make a report on a transaction involving proceeds of crime, the financing of terrorism or is of a suspicious or unusual nature to the FIU Director.	$100,000 on directors jointly and severally and/or 5 years imprisonment.	Section 23 (2) MLFTA
	Failure of a licensee to maintain business transactions records.	$100,000 on directors jointly and severally	Section 18(4) MLFTA
	Failure of a person to report transfers out of Barbados or transfers Barbadian currency or foreign currency into Barbados, of more than BDS$1 0,000 without Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24(6) MLFTA
	Failure by a person to report receiving more than BDS$10,000 in Barbadian currency (or foreign equivalent) without the Exchange Control	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24 (6) MLFTA
Internal Policies, procedures, controls; Internal reporting procedures; Internal employee training and awareness programs	Failure by a financial institution to develop policies and procedures; audit functions; and procedures to audit compliance.	Imposition of a pecuniary penalty (up to $5,000 for any of the circumstances referred to at section 34(1) of the MLFTA; $500 daily for failure to take a measure or action or cease a behaviour or practice) in accordance with section 36.	Section 19(2) of the MLFTA
Information Gathering & Investigations	Failure by a financial institution to comply with any instruction issued or request made by the FIU Director.	The licence of the financial institution may be suspended.	Section 30(5) of the MLFTA.
Onsite Inspections	Failure to comply with an instruction or request made by an authorised officer or Regulatory Authority.	The licence of the financial institution may be suspended.	Section 31(4) of the MLFTA

Anti-Money Laundering/Combating Terrorist Financing Guideline, May 2015 International Business Division

Area	Description of Offence / Breach	Description of Fine / Sanction	Section of Legislation
Interference in the Line of Duty	The obstruction, hindrance, molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	$50,000 or imprisonment of 2 years or both.	Section 42 MLFTA
Directives	Contravention of the Act but circumstances do not justify taking action under sections 34, 35 or 36 of the MLFTA.	Issuance of directives by the Anti-Money Laundering Authority or Regulatory Authority to cease and desist	Section 33 of the MLFTA.
Money Laundering Offences	Engagement in money laundering.	Summary conviction - $200,000 or 5 years imprisonment or both. Conviction on indictment - $2,000,000 or 25 years imprisonment or both. Forfeiture of licence for financial institution.	Section 6 (1) MLFTA Sections 35 & 46(1)
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 4 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 6(2) MLFTA
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 44 MLFTA
Disclosure of Information	Disclosure of information on a pending money laundering investigation. Falsifying, concealing, destruction or disposal of information material to investigation or order.	$50,000 or 2 years imprisonment or both	Section 43(b) MLFTA

Area	Description of Offence / Breach	Description of Fine / Sanction	Section of Legislation
	Disclosure or publication of the contents of any document, communication or information in the course of duties under this Act.	$50,000 or 5 years imprisonment or both.	Section 48(3) MLFTA.
Terrorism Offences	Provision or collection funds or financial services to persons to be used to carry out an offence as defined in the listed treaties[19] or any other act.	Conviction on indictment to 25 years imprisonment.	Section 4(1) Anti-Terrorism Act
	Provision of assistance or involve in the conspiracy to commit a terrorist offence.	Conviction on indictment and principal offender punished accordingly.	Section 3 of ATA
	A terrorist offence committed by a person responsible for the management or control of an entity located or registered in Barbados, or otherwise organised under the laws of Barbados.	$2,000,000 notwithstanding that any criminal liability has been incurred by an individual directly involved in the commission of the offence or any civil or administrative sanction as imposed by law.	Section 5 of ATA

[19] Treaties respecting Terrorism: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, International Convention against the taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf and the International Convention for the Suppression of Terrorists Bombings.

Appendix 3(b)

Summary of Administrative Sanctions

Description of Offence	Sanctions Enforceable by the Anti-Money Laundering Authority or Regulatory Authority	Section of Legislation
Failure to meet fitness and propriety standards Failure to comply with or contravene a Guideline issued in accordance with section 26; Failure to comply with a directive given in accordance with section 33 The financial institution is otherwise contravening the Act.	Any of the following: Issue a warning or reprimand to the financial institution, Give such directives as deemed appropriate, Impose on the financial institution, in accordance with section 36, a pecuniary penalty*, or Recommend, in accordance with section 35: (i) Suspension of any or all of the activities that the financial institution may otherwise conduct pursuant to the licence of the financial institution; or (ii) Suspension or revocation of the licence of the financial institution. ***Pecuniary Penalties Enforceable by the Anti-Money Laundering Authority or Regulatory Authority:** Where the Authority is satisfied as to any of the circumstances referred to in section 34(1) in respect of a financial institution, the Authority may, by written notice, impose on the financial institution, a pecuniary penalty not exceeding $5 000. Where by this Act or a Guideline made or directive given under this Act a financial institution is required, by a specified time, to take a certain measure or action or cease a particular activity, behaviour or practice and the Authority is satisfied that the financial institution has failed to do so, the Authority may impose on the institution, in addition to the penalty	Section 34 of the MLFTA Section 36 of the MLFTA

Description of Offence	Sanctions Enforceable by the Anti-Money Laundering Authority or Regulatory Authority	Section of Legislation
	specified in subsection (1), an additional penalty of $500 for every day or part of a day that the institution failed to take the measure or action or cease the particular activity, behaviour or practice.	

Appendix 2 - Declaration Source Of Funds/Wealth

Customer Name Or Business:……..

Current Address:……..

Account Number:…….

Identification:……...

Amount of Transaction & Currency:

Description/Nature of Business Transaction:

□ Loan □ Investment □ Trust Settlement / Distribution Other □ (Specify)

Source of Funds / Wealth:

……..……..…

……

……

Supporting Evidence:……...

Customer

Signature:……

Date:……

Transaction Approved? Yes □ No □

If No, state reason:……

……

……. …….

OFFICER COMPLETING TRANSACTION AUTHORISING OFFICER

(Signature & Title) (Signature & Title)

Appendix 3 - SUSPICIOUS/UNUSUAL TRANSACTION REPORT

CONFIDENTIAL

IMPORTANT: Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to:

THE DIRECTOR, FINANCIAL INTELLIGENCE UNIT,
ANTI-MONEY LAUNDERING AUTHORITY

P.O. BOX 1372 Bridgetown, Barbados

FACSIMILE NO. (246) 436-4756

Email: **amla@sunbeach.net**

For urgent reporting – Tel. (246) 436-4734/5

PLEASE TYPE INFORMATION OR WRITE

IN BLOCK LETTERS

FOR OFFICIAL USE ONLY **FIU Reference No.: ……**

PART A – Initial Information

1. ☐ Completed Transaction ☐ Attempted/Aborted Transaction

2. Is this report a correction or follow-up to a Report previously submitted?

☐ NO
(Skip to No.4)

☐ YES
☐ Correction
☐ Follow-up

3. If yes, original Report's date ____ ____ ____
D M Y

4. Reporting date | | | | | | | | |

D D M M Y Y Y Y

5. Which one of the following reporting entities best describes you:-

---

- ☐ Accountant
- ☐ Attorney-at-Law
- ☐ Bank
- ☐ Cooperative Society
- ☐ Credit Union
- ☐ Corporate &/or Trust Service Provider
- ☐ Dealer in Precious Metals &/ or Stones
- ☐ Finance Company
- ☐ Gaming Institution
- ☐ General Insurance Company
- ☐ International/Offshore Bank
- ☐ Life Insurance Broker/Agent
- ☐ Life Insurance Company
- ☐ Merchant Bank
- ☐ Money Service Business/Money or Value Transmission Services
- ☐ Mutual Fund Administrator/Manager
- ☐ Real Estate Agent
- ☐ Regulator
- ☐ Securities Dealer
- ☐ Trust Company/Corporation
- ☐ Other ……..

Part B – Identity of Customer 1

1. …… Surname

2. ……... Given Name

3. ……. Middle Name(s)

4. …….. Alternative Names/Spelling

5. …… ……. Address(es)

6. ……..... Nationality/(ies)

7. …… Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other……

9. …… ID No.(1)

10. ……. Place of Issue

11. Identifier #2 ☐ ID Card

12. …….

☐ Passport
☐ Driver's License
☐ Other ……

ID No.(2)

13. …….

Place of Issue

14. …….
Occupation

15. ……..
Employer

16. …….
Telephone # (Include area Code) (H)

…….
Telephone # (Include area Code) (C)

…….
Telephone # (Include area code) (W)

.

17. …….
Email Address(es)

……
Email address(es)

18. ……..
Account Number(s)

☐ Personal
☐ Corporate
☐ Trust
☐ Other ……..

19. …….
State if account is joint, other signatories, etc

20. …….
Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

CUSTOMER 2

1. …….. 2. …… 3. ……..
Surname Given Name Middle Name(s)

4. ……. 5. ……

Alternative names/Spelling

……

Address(es)

6. …….
Nationality/(ies)

7. ……
Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other …….

9. ……
ID No.(1)

10. …….
Place of Issue

11. Identifier #2 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other …….

12. …….
ID No.(2)

13. ……
Place of Issue

14. …….
Occupation

15. ……..
Employer

16. …….
Telephone # (Include area Code) (H)

……..
Telephone # (Include area code) (W)

…….
Telephone # (Include area Code) (C)

……..

17. …….
Email Address(es)

…….
Email address(es)

18. ……..
Account Number(s)

☐ Personal
☐ Corporate
☐ Trust
☐ Other ……..

19. ……
State if account is joint, other signatories, etc

20. …….

Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

Customer 2 applies where there is a transfer between customers.

PART C – To be completed only if the transaction was conducted on behalf of another person/entity other than those mentioned in Part B.

1. …….. 2. …….. 3. …….

Surname Given Name Middle Name(s)

4. ……. 5. ……

Alternative- Entity's name

……

Address(es)

6. ……. 7. ……

Nationality/(ies) Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card ☐ Certificate of Incorporation

☐ Passport ☐ Registration for Business Name

☐ Driver's License

☐ Other ……

9. …….. 10. …….. 11. ……

ID No.(1) Place of Issue Occupation/Type of Business

12. …….. 13. ……. ……

Employer Telephone (#1)- area code (H) Telephone (#2) - area code (W)

……

Telephone (#3)- area code (C)

14. …….. ……

Email Address #1 Email Address #2

15. ……

Account Number(s)

16. ……

State if a/c joint, other signatories, etc

PART D – Transaction Details

1. Type of Transaction

☐ Cash Out
☐ Deposit to an account Cash/Cheque
☐ Life Insurance Policy purchased/deposit
☐ Purchase of bank draft
☐ Purchase of Jewelry
☐ Purchase of precious metals/stones
☐ Purchase of Gold
☐ Real Estate Purchase
☐ Securities
☐ Conducted Currency Exchange
☐ Inter-account transfer
☐ Outgoing electronic funds transfer
☐ Purchase of diamonds
☐ Purchase of money order
☐ Purchase of traveller's cheques
☐ Other ……

2. Date(s) of transaction(s) | | | |

D M Y

3. …… 4. ……..

Amount & Currency BBD $ Equivalent

5. …… 6. ……..

Name of drawer/Ordering Customer Name of Payee/beneficiary

7. ……

Other bank involved, other Country

Please provide copies of relevant documents (e.g. bank statements, real estate documents, etc.) for suspicious or unusual activity and identification and verification information.

PART E – Grounds for Suspicion

(Please describe clearly and completely the factors or unusual circumstances that led you to suspect that the transaction(s) involve(s) the proceeds of crime, involve(s) the financing of terrorism, is of a suspicious or unusual nature.)

If the report relates to attempted transaction(s), describe why each one was not completed.

……..

……
……
……
……
……
……
……
……
……
……
……
…

(If insufficient space, please attach a separate sheet.)

PART E2

If additional information is attached, please tick box ☐

PART E3

If identity of the customer has not been established in PART B and they are not known to the officer, give a description (e.g., sex, approximate age, height, built, ethnicity, complexion, etc.)

……
……
……
……
……
……

PART F - **Details of financial institution/place of transaction**

1. …… Organisation

2. …….. Branch where transaction occurred if applicable

3. ……. Name and Title of Reporting Officer

4. …… Signature of Reporting Officer

5. …….. Dealers internal reference number

6. …….. Reporting Officer‘s direct telephone number