GOVERNMENT OF BARBADOS

ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION GUIDELINE

For

Licensees and Registrants

Under

The Corporate and Trust Service Providers Act, 2015-12

The Private Trust Companies Act, 2012-22

The Trusts (Miscellaneous Provisions) Act, 2018-49

And

The Foreign Currency Permits Act, 2018-44

International Business Unit

In conjunction with the Anti-Money Laundering Authority

Revised: October, 2021

TABLE OF CONTENTS

ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION GUIDELINE

I. PURPOSE OF GUIDELINE

1. The purpose of the Guideline is to provide guidance to all licensees and registrants of the International Business Unit 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.

2. 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 Unit and is updated to reflect the changes in the MLFTA. The definitions appearing in the MLFTA apply *mutatis mutandis* to this Guideline.

II. MONEY LAUNDERING AND FINANCING OF TERRORISM AND PROLIFERATION

Money Laundering:

3. 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:
   - to conceal the true ownership and origin of criminal proceeds;
   - to maintain control over them; and
   - to change their form.

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

   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.

   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.

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

5. 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. The FATF Recommendations places obligations on countries as it relates to terrorist financing in the context of national cooperation and coordination (Recommendation 2), confiscation and provisional measures (Recommendation 4), and targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6). The latter is applicable to all United Nations Security Council resolutions (UNSCRs) applying targeted financial sanctions relating to the financing of terrorism. The IBU's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting terrorism.

Proliferation Financing of Weapons of Mass Destruction

6. The FATF working definition of PF "refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations"[1]. The FATF Recommendations places obligations on countries as it relates to PF in the context of assessing risk and applying a risk-based approach (Recommendation 1), national cooperation and coordination (Recommendation 2), and targeted financial sanctions related to proliferation (Recommendation 7). The latter is applicable to all UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction. The IBU's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation.

III. INTERNATIONAL INITIATIVES

7. The Financial Action Task Force (FATF) was established in 1989 by the seven major industrialized countries of the world and other developed countries to

[1] FATF 2012 Best Practices Paper to Recommendation 2: Information Sharing and Exchange Related to Financing of Proliferation, among Relevant Authorities at the Domestic Level.

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

8. The **FATF Forty Recommendations** were revised in February 2012, and renamed the **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations**. The Recommendations were since updated in February 2013 R.37 & R.40 (mutual legal assistance and other forms of international cooperation); October 2015 (Interpretative Note to R.5 on foreign terrorist fighters); June 2016 (R.8 and its Interpretative Note on non-profit organizations); October 2016 (Interpretative Note to R.5 on terrorist financing offence); June 2017 (Interpretive Note to R.7 on targeted financial sanctions related to proliferation); November 2017 (R.21 on tipping-off and confidentiality and Interpretive Note to R.18 on internal controls and foreign branches and subsidiaries); February 2018 (R.2 on national cooperation and coordination); and October 2018 (R.15 on new technologies); and October 2020 (R. 1 and R. 2 on proliferation financing). The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. The growing body of work includes Guidance on *AML/CFT/CPF-related Data & Statistics*; *Combating the Abuse of Non-Profit Organizations*; *Transparency and Beneficial Ownership*; *Politically Exposed Persons*; *Risk Based Approach to Prepaid Card, Mobile Payments and Internet-Based Payment Services*; *Risk-Based Approach to Combating Money Laundering and Terrorist Financing; Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction; and Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

IV. LEGISLATIVE AND REGULATORY FRAMEWORK

9. 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**:**
   - Drug Abuse (Prevention and Control) Act, 1990-14, Cap.131;
   - Drug Abuse (Amendment) (Prevention and Control) Act;
   - Proceeds and Instrumentalities of Crime Act, 2019;
   - Mutual Assistance in Criminal Matters Act, Cap.140A;
   - Anti-Terrorism Act, Cap. 158;
   - Anti-Terrorism (Amendment) Act, 2019[2];
   - Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23;
   - Money Laundering and Financing of Terrorism (Prevention and Control)

[2] There are consequential amendments to the MLFTA.

(Amendment) Act, 2019;
- Trafficking in Persons Prevention Act, 2016; and
- Criminal Assets Recovery Fund Act, 2016.

10. This framework is supported by the International Business Unit, 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.

Offences

11. Section 5(1) of the Money Laundering and Financing of Terrorism (Prevention and Control) Act states that a person engages in money laundering where:
- The person engages, directly or indirectly, in a transaction that involves money or other property or a benefit that is proceeds of crime; or
- 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.

V. REGIONAL INITIATIVES

The Caribbean Financial Action Task Force

12. 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.

13. 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.

VI. THE ANTI-MONEY LAUNDERING AUTHORITY

14. 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.

15. 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.

VII. SCOPE AND APPLICATION OF GUIDELINE

16. This Guideline[3] provides guidance on the expectations of the International Business Unit (IBU) concerning the activities of licensees and registrants (otherwise referred to as "Institutions") of the IBU. 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.

17. This Guideline applies to all institutions and these institutions must ensure that, at a minimum, this guidance is also implemented in their branches and subsidiaries abroad and where permitted in the host country, ensure that these operations apply the higher of local and host standards. Institutions should inform the International Business Unit if the host laws and regulations prohibit the implementation of this Guideline, and take appropriate additional measures to address ML/TF/PF risks.

18. 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 within the meaning of the Trusts (Miscellaneous Provisions) Act 2018-49;
    ii. a person who operates an insurance business within the meaning of the *Insurance Act*;
    iii. a market actor, self-regulatory organization, participant and issuer of securities within the meaning of the *Securities Act*;

[3] For the purposes of this Guideline, general references to money-laundering should be interpreted as references to money-laundering and/or the financing of terrorism and proliferation.

iv. a mutual fund and mutual fund administrator within the meaning of the *Mutual Funds Act* or any person who manages a mutual fund;
v. a licensee under the *Financial Institutions Act*;
vi. a building society within the meaning of *the Building Societies Act*;
vii. a credit union within the meaning of the *Co-operative Societies Act;*
viii. a friendly society within the meaning of the *Friendly Societies Act*;
ix. a foundation within the meaning of the *Foundations Act, 2013 (Act 2013-2)*;
x. a private trust company with the meaning of the *Private Trust Companies Act, 2012 (Act 2012-22)*
xi. a foreign sales corporation within the meaning of the Barbados Foreign Sales Corporation Act; and
xii. a society with restricted liability within the meaning of the *Societies With Restricted Liability Act*.

VIII. GROUP PRACTICE

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

- ensure that such branches or subsidiaries observe this Guideline and apply the higher of local and host standards;
- keep all such branches and subsidiaries informed as to current group policy;
- ensure that special attention is paid to foreign branches and subsidiaries that do not or insufficiently apply the FATF Recommendations;
- inform the IBU and the Reporting Authority when a foreign branch or subsidiary is unable to observe appropriate AML/CFT/CPF measures due to prohibitions by local laws, regulations or other measures; and
- 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.

If the host country does not permit the proper implementation of AML/CFT/CPF measures, financial groups are required to apply appropriate additional measures to manage the ML/TF/PF risks, and inform their home supervisors on the AML/CFT/CPF gaps in the host country and the measures taken to mitigate the risks. The IBU will then make a determination on the required course of action where additional measures are not sufficient. This would include placing additional controls, such as requesting the financial group to close its operations in the host country.

20. For institutions that are part of the same financial group that rely on a third party that is part of the same financial group, the group should:

- apply CDD and record keeping requirements, in line with FATF Recommendations 10-12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18;

- be aware that the implementation of the CDD and record keeping requirements and AML/CFT/CPF programmes is subject to supervision at a group level by a competent authority; and
- adequately mitigate any higher country risk by the group's AML/CFT/CPF policies.

21. Where institutions have a number of related legal entities included in its structure, i.e. unit, branches, and subsidiaries, the Board and Senior Management should have a clear understanding of the legal and operational risks that may be inherent in the structure.

22. The Board and Senior Management should understand the interconnections and intra-group transactions in order to identify oversee and manage the potential risks to the institution. Therefore, sound and effective measures and systems should be put in place to facilitate the generation and exchange of information within the group, and with regulators.

IX. INTERNAL CONTROL AND PROCEDURES

The Duty of Vigilance

23. 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.

24. Thus the duty of vigilance consists mainly of the following elements:
- Verification;
- Risk Assessment
- Ongoing Due Diligence
- Recognition of suspicious transactions;
- Reporting of suspicion;
- Keeping of records; and
- Training.

X. THE ROLE OF THE BOARD AND SENIOR MANAGEMENT

25. Institutions must see AML/CFT/CPF as part of their overall risk management strategy. Money laundering, terrorist financing and financing of proliferation expose an institution to transaction, compliance and reputation risk. For institutions convicted of money laundering or terrorist financing, there are considerable costs. Therefore, institutions should establish an effective AML/CFT/CPF programme that minimises these risks and potential costs.

26. The Board of Directors has ultimate responsibility for the effectiveness of the institution's AML/CFT/CPF framework. Section 5(2)(b) of the MLFTA establishes that a financial institution engages in money laundering where the financial institution/non-financial business entity/ professional fails to take reasonable steps to implement or apply procedures to control or combat money laundering. The Board has an oversight role designed to ensure inter alia that there is compliance with all the relevant laws and regulations and international standards. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

27. Directors and senior management should be aware that:

(a) The use of a group wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the institution and compliant with Barbadian law, regulations and guidelines. Failure to ensure compliance by the institution with the requirements of the MLFTA may result in significant penalties for directors and the institution (See Appendix 1);

(b) Institutions that are part of a group should implement group-wide AML/CFT/CPF programmes that encompass branches and subsidiaries. Such programmes should include:

i. policies and procedures for sharing information required for the purposes of CDD and ML/FT/PF risk management;
ii. the provision, at group-level compliance, audit, and/or AML/CFT/CPF functions, of a customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes. This includes information and analysis of transactions and activities which appear unusual (if such analysis was done). This could include an STR, its underlying information or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group level functions when relevant and appropriate for risk management;
iii. The monitoring of significant customer relationships and their transaction activity on a consolidated basis;
iv. The monitoring of significant customer relationships and their transaction activity on a consolidated basis;
v. The different risk factors posed by each line of business and customers;
vi. The sharing of information on the identity of customers and their transactions and activities across the entire group; and
vii. adequate safeguards on the confidentiality and use of information exchanged including the prevention of tipping-off.

(c) Subsidiaries and branches of institutions including those domiciled outside of Barbados are expected to, at a minimum, comply with the requirements of Barbados MLFTA and this Guideline; and

(d) Where some of an institution's operational functions are outsourced, the institution retains full responsibility for compliance with local laws, regulations and guidelines.

28. Directors should therefore demonstrate their commitment to an effective AML/CFT/CPF programme by:
(a) Understanding the statutory duties placed upon them, their staff and the entity itself;
(b) Approving AML/CFT/CPF policies and procedures that are appropriate for the risks faced by the institution. Evidence of consideration and approval of these policies should be reflected in the board minutes;
(c) Appointing an individual within the organisation for ensuring that the institution's AML/CFT/CPF procedures are being managed effectively; and
(d) Seeking assurance that the institution is in compliance with its statutory responsibilities as it relates to AML/CFT/CPF. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems.

29. 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 IBU or any related Self-Regulating body. Institutions' programmes should also observe higher/lower risks identified in risk assessments conducted by the International Business Unit or in a national risk assessment and take appropriate enhanced or simplified measures. (See Para. 101 on Reduced Customer Due Diligence)

30. 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.

Risk-Based Approach

31. All institutions should develop anti-money laundering policies and procedures capturing the above, and commensurate with:
    - the size and the nature and complexity of activities;
    - the complexity volume and size of transactions;
    - the degree of risk associated with each area of operation;
    - the type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP);
    - type of product/service;
    - delivery channels;(e.g. whether internet banking, wire transfers etc.)
    - 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);
    - the internal audit and regulatory findings; and
    - value of customer accounts and frequency of transactions

XI. CUSTOMER DUE DILIGENCE

32. For the purposes of this Guideline, the licensee should seek to identify the customer and all those who exercise control over the account/business arrangement. A customer includes:
    i. A person or entity that maintains an account with the licensee;
    ii. A person or entity on whose behalf an account is maintained i.e. beneficial owner. Beneficial owner refers to the 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.

        Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

33. There may be doubt as to the natural person(s) with controlling ownership interest; or there is no natural person(s) exerting control through ownership interests. In such cases, the licensee should identify those natural person(s) exercising control of the legal person or legal arrangement through other means. Where no natural person is identified by the aforementioned, the licensee should identify the relevant natural persons in senior managing positions or those exercising ultimate effective control over legal persons and arrangements, respectively:

    (a) The beneficiaries of business transactions conducted by professional intermediaries such as lawyers, accountants, notaries, business introducers or any other professional service providers; or

(b) Any person or entity connected with a business transaction that can pose a significant risk to the licensee, including persons establishing business arrangements, purporting to act on behalf of a customer or conducting business transactions.

34. 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.

35. Where there is a suspicion that a transaction relates to money laundering or the financing of terrorism, institutions should be cognizant of tipping off a customer when conducting due diligence. The institution should make a business decision whether to execute the transaction as the case may be, but a suspicious report should be submitted to the Authority.

VERIFICATION SUBJECT

Individuals

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

37. 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.

Partnerships

38. Partnerships and unincorporated businesses should meet the relevant requirements set out in Paras. 52 - 59. The licensee should identify each partner as well as immediate family members with ownership control. In addition to providing the identification documentation for partners/controllers and authorised signatories, where a formal partnership arrangement exists, the licensee may obtain a mandate from the partnership authorising the opening of an account.

Corporate Customer/Companies (including corporate trustees)

39. All persons and institutions must identify the beneficial owner and implement reasonable measures for verifying the identity of 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.

40. To satisfy itself as to the identity of the customer, the institution should obtain:

(a) Name of corporate entity;
(b) Principal place of business and registered office;
(c) Mailing address;
(d) Contact telephone and fax numbers;
(e) Identity information on the beneficial owners of the entity. This information should extend to identifying those natural person(s) who ultimately own and control the company and should include anyone who is giving instructions to the licensee to act on behalf of the company. However,
    i. If the company is publicly listed on a recognised stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required; and
    ii. If the company is privately owned, identity should be sought on persons with a minimum of 20% shareholding.
(f) Identity information on directors and officers who exercise effective control over the business and are in a position to override internal procedures/control mechanisms and, in the case of bank accounts, the signatories to the account. This is particularly necessary where no natural person is identified;
(g) Description and nature of business;
(h) Certified copy of the certificate of incorporation, organisation, registration or continuance, as the case may be, or any other certificate that is evidence of the creation, registration or continuance of the body corporate, society or other legal person as such, officially authenticated where the body corporate, society or other legal person was created in another country; and
(i) any other relevant documents or information

Other institutions

41. 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).

TIMING AND DURATION OF VERIFICATION

42. 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:
- carrying out the verification itself, or
- by relying on the verification of others in accordance with these Guidelines.

43. 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.

44. 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.

45. 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 Compliance Officer.

46. 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:
- satisfy himself/herself that such account is held in the name of the applicant for business at or before the time of payment, and
- 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.

METHODS OF VERIFICATION

47. 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.

48. 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.

49. Verification is a cumulative process. Except for one-off transactions, 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.

50. File copies of documents must be retained.

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

Individuals

52. 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.

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

54. The relevance and usefulness in this context of the following personal information must be considered:
- full name(s) used
- date and place of birth
- nationality
- 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
- occupation and name of employer (if self-employed, the nature of the self-employment)
- specimen signature of the verification subject official.

55. In this context “current permanent address” means the verification subject’s actual residential address as it is an essential part of identity.

56. To establish identity, the following documents are considered to be the best possible, in descending order of acceptability:
- telephone and fax number
- current valid passport
- National identity card
- Armed Forces identity card
- driving license which bears a photograph
- Documents sought must be pre-signed.

57. Documents which are easily obtained in any name should not be accepted uncritically. Examples include:
- birth certificates
- an identity card issued by the employer of the applicant even if bearing a photograph
- credit cards
- business cards
- national health or insurance cards
- provisional driving licenses
- student union cards

58. 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.

59. If the verification subject is an existing customer of an institution referenced at Para. 87, 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.

Companies

60. 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:
- Certificate of Incorporation,
- 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,
- Memorandum and Articles of Association;
- 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;
- Copies of Powers of Attorney or other authorities given by the directors in relation to the company;
- a signed director's statement as to the nature of the company's business.

61. 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

62. The relevance and usefulness of obtaining the following (or their foreign equivalent) should be carefully considered as part of the verification procedure:
- the partnership agreement, and
- information listed above under Para. 54 in respect of the partners and managers relevant to the application for business.

RESULT OF VERIFICATION

Satisfactory

63. 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

64. 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 Compliance Officer should make a report to the Reporting Authority.

ENHANCED DUE DILIGENCE

65. 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.

66. Licensees are also required to observe the list of countries published by any competent authority which lists countries that are non-compliant or do not sufficiently comply with FATF recommendations. Refer to the **FATF: High Risk & Non-Cooperative Jurisdictions**[4] **and any lists of high-risk jurisdictions provided by the Competent Authority from time to time**. In order to mitigate the risks, licensees should apply appropriate countermeasures to any country that appears on the list or when called upon to do so by FATF and CFATF or independently of any call to do so. Such countermeasures may include:

(a) Requiring financial institutions to apply specific elements of enhanced due diligence;
(b) Prohibiting financial institutions from establishing subsidiaries, branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant subsidiary, branch or representative office would be in a country that does not have adequate AML/CFT/CPF systems;
(c) Limiting business relationships or financial transactions with the identified country or persons in that country;
(d) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process;
(e) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned; and,

[4] http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc

(f) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

67. The policy framework of an institution should therefore include a description of the types of customers that are likely to pose a higher than average risk and procedures for dealing with such applications. High-risk customers should be approved by senior management and stringent documentation, verification and transaction monitoring procedures should be established. Applying a risk-based approach, enhanced due diligence for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:
    (a) An evaluation of the principals;
    (b) A review of current financial statements;
    (c) Verification of the source of funds;
    (d) Verification of source of wealth;
    (e) The conduct of reference checks;
    (f) Checks of electronic databases;
    (g) Review of relevant country assessment reports; and
    (h) Periodic reporting to the Board about high risk accounts.

68. Institutions perform their duty of vigilance by having in place systems that enable them to:
    - determine (or receive confirmation of) the true identity of customers requesting their services through the use of reliable, independent source documents, data or information;
    - understand and as appropriate obtain information on the purpose and intended nature of the business relationship and source of the funds;
    - 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;
    - identify the beneficial owners whether by declaration by the customer or through investigation;
    - 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;
    - 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
    - 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;

- keep records for the prescribed period of time;
- train key staff;
- liaise closely with the Reporting Authority on matters concerning vigilance policy and systems;
- 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
- ensure that internal auditing and compliance departments regularly monitor the implementation and operation of vigilance system.

69. Types of situations requiring enhanced due diligence include, but are not limited to, the below:

Trust Clients & Other Legal Arrangements

70. Institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf 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.

71. At a minimum, the institutions should obtain the following -
(a) Name of trust;
(b) Nature/type of trust;
(c) Country of establishment;
(d) Identity of the trustee(s), settlor(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and the names or classes of beneficiaries;
(e) Identity of person(s) with powers to add beneficiaries, where applicable; Identity of the person providing the funds, if not the ultimate settlor; and
(f) Any other natural person exercising effective control over the trust (including through a chain of control/ownership).

72. For any other types of legal arrangements, the identity of persons in equivalent or similar positions.

73. 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. 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 institution should verify beneficiaries before the first distribution of assets. Further, institutions 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.

74. 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.

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

76. Institutions should inform the IBU and the FIU when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of this Guideline.

Non-Profit Organisations (NPOs)

77. The FATF has adopted a functional definition of a NPO based on those activities and characteristics of an organisation which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. Consequently, a NPO is defined as a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

78. NPOs differ in size, income, structure, legal status, membership and scope. NPOs can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity. Institutions should therefore, apply a risk-based approach to NPOs and apply effective and proportionate measures.

79. The FATF further notes that not all NPOs are high risk, and some may represent little or no risk at all. It may be possible that existing measures are sufficient to address the current FT risk to the NPO sector identified in a country, although periodic reviews may identify new or evolved FT risks over time. This is important consideration for institutions in their implementation of a risk-based approach. It means that a "one size fits all" approach to all NPOs is not appropriate in how institutions manage business relationships with customers who are NPOs. To assess the risk, an institution should focus inter alia on:
    (a) Purpose, ideology or philosophy;
    (b) Geographic areas served (including headquarters and operational areas);
    (c) Organisational structure;
    (d) Donor and volunteer base;
    (e) Funding and disbursement criteria (including basic beneficiary information);
    (f) Record keeping requirements; and

(g) Its affiliation with other NPOs, Governments or groups.

80. The institution should also include the following in the identity records:
1) Evidence of registration of the home and local operation, where applicable;
2) Identity of all signatories to the account; and
3) Identity of board members and trustees, where applicable.

81. As part of the verification process, institutions should confirm that the organisation is registered under the appropriate laws and with the tax authorities and should carry out due diligence against publicly available terrorist lists. As part of ongoing monitoring activity, institutions should examine whether funds are being sent to high-risk countries. Institutions should bear in mind that there is legitimate and important NPO activity in high risk areas and conflict zones, occasioned by the difficulty of providing assistance to those in need.

Non-Face To Face Customers

82. The rapid growth of financial business by electronic means increases the scope for non-face -to-face business and increases the risk of criminal access to the financial system. Customers may use the internet, the mail service or alternative means because of their convenience or because they wish to avoid face-to-face contact. Consequently, institutions should pay special attention to risks associated with new and developing technologies. Customers may complete applications but institutions should satisfy the requirements in this section before establishing a business relationship.

83. When accepting business from non-face-to-face customers, in order to prove to its satisfaction that the individual is who that individual claims to be, institutions should:

- Obtain documents certified by approved persons;
- Ensure that all company documents are signed by the Company Secretary;
- Request additional documents to complement those which are required for face-to-face customers, including more than one photo bearing ID;
- Make independent contact with the customer, for example by telephone on a listed business or other number; and
- Request third party introduction e.g. by an introducer.

84. In addition, the institution may:
(a) Carry out employment checks (where applicable) with the customer's consent through a job letter or verbal confirmation on a listed business or other number;
(b) Require the first payment to be carried out through an account in the customer's name with another bank subject to equivalent customer due diligence standards; and
(c) Obtain any other information deemed appropriate.

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

86. Where an institution or its subsidiary initiates transactions in its role as a securities broker or in the sale of mutual funds without establishing face-to-face contact and obtaining all of the relevant documentation, the institution should make all efforts to obtain such information within a reasonable timeline. 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 the established timeframe, may trigger the termination of the transaction; and
    (c) Consider submitting a suspicious report.

Introduced Business

87. An institution may rely on other regulated third parties to introduce new business in whole or in part but the ultimate responsibility remains with the institution for customer identification and verification. An institution should:
    (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 practices at least equivalent to those required by Barbados law and the institution itself;
    (b) Satisfy itself about the quality and effectiveness of supervision and regulation in the introducer's country of domicile (refer to 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 the FATF Recommendation 11;
    (c) Obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;
    (d) Satisfy itself that an introducer continues to conform to the criteria set out above (e.g. conduct periodic reviews);
    (e) Consider terminating the relationship where an introducer fails to provide the requisite customer identification and verification documents; and
    (f) Consider terminating the relationship with an introducer who is not within the institution's group, where there are persistent deviations from the written agreement.

88. When a prospective customer is introduced from within an institution's financial 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 institution should however, retain copies of the identification records in accordance with the requirements in the MLFTA. Institutions should obtain written confirmation from a group member confirming completion of verification.

Professional Service Providers

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

90. 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 institution must identify each beneficial owner. Where funds are co-mingled, the institution must also identify the beneficial owners. Subject to the IBU'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. Institutions should apply the criteria in the Section entitled Introduced Business in conducting due diligence on providers.

91. Institutions should observe guidance from the FIU regarding attorney-client accounts.

Politically Exposed Persons (PEPS)

92. 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.

93. 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 institutions, enhanced due diligence is recommended when dealing with PEPs.

94. 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.

95. Institutions must 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, institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

96. The requirements for all types of PEP should also apply to family members or close associates[5] of such PEPs.

97. The FATF Recommendations categorize PEPs as follows:
- Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, 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;
- 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;
- 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.

Virtual Asset Service Provider (VASP)

98. The FATF defines:
"Virtual asset" as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other

[5] Family members are individuals who are related to a PEP other directly (consanguinity) or through marriage or similar (civil) forms of partnership. Close associates are individuals who are closely connected to a PEP, either socially or professionally.

financial assets that are already covered elsewhere in the FATF Recommendations; and

"VASP" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies;
- Exchange between one or more forms of virtual assets;
- Transfer 21 of virtual assets;
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

When establishing and maintaining relationships with a VASP, a licensee should:

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

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

iii. 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.

Corporate Vehicles

99. Barbados law prohibits companies from issuing shares in bearer form. Where an institution decides that companies with nominee shareholders represent an acceptable business risk, they must exercise care in conducting transactions. Institutions must ensure they can identify the beneficial owners of such companies and should immobilize bearer shares and bearer share warrants as a means of monitoring the identity of such companies by, for example, requiring custody by:
(a) The institution, or its subsidiary, regulated affiliate, parent or holding company;
(b) A recognized regulated financial institution in a jurisdiction with equivalent AML/CFT/CPF standards; and
(c) Requiring the prior approval before shares can be exchanged.

Higher Risks Countries

100. Certain countries are associated with predicate crimes such as drug trafficking, fraud, and corruption and consequently may pose a higher potential risk to institutions. Conducting business relationships with customers who are either citizens of or domiciled in such countries may expose the institution to reputational

risks. Institutions are encouraged to consult publicly available information to ensure that they are aware of countries/territories, which may pose a higher risk.

REDUCED CUSTOMER DUE DILIGENCE

101. An institution's policy document should clearly define the risk categories/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 a risk level that qualifies for this treatment. Institutions should apply:
(a) Policies, controls and procedures approved by senior management are implemented to manage and mitigate the risk identified;
(b) The implementation of controls are monitored and enhanced, where necessary;
(c) Enhanced measures are implemented to mitigate higher risks, where identified.

RETROSPECTIVE DUE DILIGENCE

102. Where the identity information held on existing customers does not comply with the requirements of this Guideline, institutions should develop a risk-based programme for ensuring compliance. Institutions should:
(a) Record their non-compliant business relationships, noting what information or documentation is missing;
(b) Establish a framework for effecting retrospective due diligence, including the setting of deadlines for the completion of each risk category. The timing of retrofitting can be linked to the occurrence of a significant transaction, a material change in the way that an account is operating, or doubts about previously obtained customer due diligence data; and
(c) Establish policies for coping with an inability to obtain information and documentation, including terminating the relationship and making a suspicious report.

DECLARATIONS

103. 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.

104. 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.

105. The following points of guidance will apply according to:

- the legal personality of the applicant for business (which may consist of a number of verification subjects); and
- the capacity in which he/she is applying.

106. 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.

XII. TRAINING

107. 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/CPF 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.

108. An ongoing AML/CFT/CPF 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.

109. 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).

110. 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.

111. 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.

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

113. 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:
- 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;
- vigilance policy and vigilance systems;
- the recognition and handling of suspicious transactions;
- new techniques and trends in money laundering and financing of terrorism
- other pieces of anti-money laundering legislation identified under the Barbados Anti-Money Laundering Regime at the beginning of these notes; and
- any Code of Conduct issued by industry associations.

114. 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.

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

XIII. TRAINING PROGRAMMES

116. 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:

New employees

117. Generally training should include:
- the company's instruction manual;
- a description of the nature and processes of laundering;

- 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;
- 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 Compliance Officer (or equivalent).

Specific appointees

118. **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 Compliance 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.

119. 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 Compliance Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

120. **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:
- the *Proceeds of Crime Act*, the *Money Laundering (Prevention and Control) Act* and Regulations issued thereunder;
- procedures relating to the service of production and restraint orders;
- internal reporting procedures; and
- the requirements of verification and records.

XIV. UPDATES AND REFRESHERS

121. 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.

XV. COMPLIANCE AND AUDIT

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

123. The Compliance Officer should:

i. Undertake responsibility for developing compliance policies;
ii. Develop a programme to communicate policies and procedures within the entity;
iii. Monitor compliance with the licensee's internal AML programme;
iv. Receive internal reports and consider all such reports;
v. Issue, in his/her own discretion, external reports to the Authority as soon as practicable after determining that a transaction warrants reporting;
vi. Monitor the accounts of persons for whom a suspicious report has been made;
vii. Establish and maintain on-going awareness and training programmes for staff at all levels;
viii. Establish standards for the frequency and means of training;
ix. Report at least annually to the board of directors (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat money laundering and the financing of terrorism;
x. Review compliance policies and procedures to reflect changes in legislation or international developments;
xi. Participate in the approval process for high-risk business lines and new products, including those involving sharing; and
xii. Be available to discuss with IBU or the FIU matters pertaining to the AML/CFT function.

124. The internal audit department should carry out reviews to evaluate how effectively compliance policies are being implemented. Such reviews should be carried out on a frequency consistent with the licensee's size and risk profile. The review process should identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions.

125. The IBU recognises, however, that the designation of a Compliance Officer or the creation of an internal audit department may create difficulties for some small licensees. Where the licensee is part of a larger regulated group, the Group Compliance Officer or Group Internal Audit may perform the compliance and/or

internal audit services subject to the prior approval of the IBU. Where this is not possible, a licensee may, subject to IBU's agreement, outsource the operational aspects of the compliance or internal audit function to a person or firm that is not involved in the auditing or accounting functions of the licensee. Notwithstanding, the responsibility for compliance with the MLFTA and the Guideline remains that of the licensee and the requirements of this section will extend to the agent. A licensee should have a local control function with the same level of independence as the Compliance Officer and be in a position to readily respond to the IBU and FIU on AML/CFT issues.

XVI. THE DUTY OF VIGILANCE OF EMPLOYEES

126. 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*.

127. 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.

XVII. THE CONSEQUENCES OF FAILURE

128. 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.

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

130. 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*.

131. 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*.

XVIII. RECOGNITION OF UNUSUAL/SUSPICIOUS TRANSACTIONS

132. 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.

133. 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.

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

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

XIX. REPORTING OF SUSPICION

135. 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.

136. 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 Compliance Officer.

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

138. 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 Compliance Officer.

139. On receipt of a report concerning an unusual transaction, the Compliance 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.

140. If the Compliance Officer decides that the information does substantiate a suspicion of laundering or terrorist financing, he is required to disclose this information promptly. If the Compliance 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.

XX. REPORTING TO THE REPORTING AUTHORITY

141. If the Compliance Officer decides that a disclosure should be made, a Suspicious Transaction Report, in standard form should be sent to the Reporting Authority.

142. If the Compliance 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.

143. 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.

144. 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.

145. 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:
- the date of the report;
- the person(s) to whom the report was forwarded;
- a reference by which supporting evidence is identifiable; and
- receipt of acknowledgment from the Reporting Authority.

146. Where a suspicious report has been filed with the Reporting Authority, and further unusual or suspicious activity pertaining to the same customer or account arises, licensees should file additional reports with the Authority. Additionally, the Director must be notified that a suspicious/unusual report has been filed with the Reporting Authority by an Institution in the prescribed form.

See Guidance Note on the Preparation and Submission of High Quality Suspicious Transaction/Activity Reports.

Freezing and Unfreezing

147. In addition, pursuant to the United Nations Resolutions on terrorist financing and the financing of proliferation, licensees should freeze any funds or other assets held for individuals or entities so designated by a terrorist designation order or counter-proliferation order in respect to listed persons. Orders may be communicated electronically or in the Official Gazette and local newspapers. Institutions are required to submit a report to the identified Competent Authority, which should include the total sum of frozen assets. The obligation to freeze is extended to all funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, of designated persons or entities, as well as funds or assets of persons and entities on behalf of, or at the direction of, designated persons or entities. Where a terrorist designation order or counter-proliferation order has been lifted. Institutions should have a mechanism in place to release the assets previously frozen.

See the Guidelines on Targeted Financial Sanctions for Financial Institutions and Designated Non-Financial Business Entities and Professionals.

XXI. KEEPING OF RECORDS

148. To demonstrate compliance with the MLFTA and to allow for timely access to records by the IBU 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:

- 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.
- 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.
- 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.

149. Licensees should also maintain records on internal and external reports. These should include:

i. All reports made by staff to the Compliance Officer;
ii. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;
iii. Consideration of those reports and of any action taken;
iv. Reports by the Compliance officer to senior management and board of directors;
v. Reports to the Reporting Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and
vi. Reports to the Reporting Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.

150. 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

151. 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.

XXII. CONTENTS OF RECORDS

152. Records relating to verification must generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject; and
- 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:
- details of personal identity, including the names and addresses, of:
- the customer;
- the beneficial owner of the account or product;
- any counter-party;
- details of securities and investments transacted including:
- the nature of such securities/investments;
- valuation(s) and price(s);
- memoranda of purchase and sale;
- source(s) and volume of funds;
- destination(s) of funds;
- memoranda of instruction(s) and authority(ies)
- book entries;
- custody of title documentation;
- the nature of the transaction;
- the date of the transaction;
- the form (e.g. cash, cheque) in which funds are offered and paid out.

153. Records relating to accounting must generally comprise:
- underlying documentation, such as invoices, contracts, etc. and should reflect details of
- all sums of money received and expended and the matters in respect of which the receipt and expenditure takes place;
- all sales and purchases and other transactions; and
- the assets and liabilities of the licensee or registrant.

154. 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:
- an original hard copy;
- microform; or
- electronic data.

155. 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.

156. 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.

157. 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.

XXIII. REGISTER OF ENQUIRIES

158. 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:
- the date and nature of the enquiry; and
- details of the account(s) involved should be maintained for a period of at least 5 years.

XXIV. FIDUCIARY SERVICES

159. 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;
- acting as corporate and/or individual trustee;
- providing the services of a registered office or otherwise acting as a person authorized to accept service or correspondence
- formation and/or administration of Barbados and/or foreign-registered companies;
- provision of corporate and/or individual directors;
- opening and/or operating bank accounts on behalf of clients.

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

XXV. VERIFICATION

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

162. 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;

- in the course of company formation, verification of the identity of beneficial owners.

- 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.

XXVI. CLIENT ACCEPTANCE PROCEDURES

Procedures for Professional Service Clients "PSC"

163. 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.

164. 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.

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

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

167. 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.

Procedures for End User Clients "EUC"

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

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

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

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

172. 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.

173. 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.

174. 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 Unit.

Additional Requirements Where Fiduciary Services are provided

175. 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.

176. 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:
- copies of minutes of meetings of shareholders;
- copies of minutes of meetings of directors;
- copies of minutes of meetings of committees;
- copies of registers of directors, officers and shareholders; and
- copies of registers of mortgages, charges and other encumbrances.

177. 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.

XXVII. OFFENCES AND PENALTIES IMPOSED UNDER THE MLFTA

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

Appendix 1: Summary of Money Laundering and Terrorism Sanctions and Offences
Appendix 2: Declaration of Source of Funds/Wealth
Appendix 3: Summary of Administrative Sanctions
Appendix 4: Approved Persons for Certification of Customer Information
Appendix 5: Virtual Asset Service Provider – Red Flag Indicators

APPENDIX I

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.	Conviction on indictment - $100,000.	Section 23 (2) MLFTA
	Failure of a licensee to maintain business transactions records.	Conviction on indictment - $100,000.	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 permission.	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	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

Area	Description of Offence/Breach	Description of Fine/Sanction	Section of Legislation
programs			
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
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	Subject to trial and	Section 44

Area	Description of Offence/Breach	Description of Fine/Sanction	Section of Legislation
	(corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	punishment accordingly.	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
	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 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 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(s)……

……

……

OFFICER COMPLETING TRANSACTION
(Signature & Title)

AUTHORISING OFFICER
(Signature & Title)

APPENDIX 3

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: Suspension of any or all of the activities that the financial institution may otherwise conduct pursuant to the licence of the financial institution; or 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 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.	Section 34 of the MLFTA Section 36 of the MLFTA

APPENDIX 4

APPROVED PERSONS FOR CERTIFICATION OF CUSTOMER INFORMATION

In keeping with Para. 82 on non face-to-face customers, institutions must only accept customer information that has been certified by:

Any of the below persons in Barbados, or their counterparts in jurisdictions with at least equivalent AML/CFT/CPF standards:

- Notary Public
- Member of the Judiciary
- Magistrate
- Attorney-At-Law with a valid practising certificate
- Accountant who is a member of a national professional association
- Senior Banking officer (at least management level)
- Senior Officer of a Consulate/Embassy/High Commission of the country issuing the passport
- *Senior Public Servant -
  *In Barbados, this refers to the:
  - Registrar/Deputy Registrar of Corporate Affairs and Intellectual Property
  - Registrar/Deputy Registrar, Supreme Court
  - Registrar/Deputy Registrar, Land Registry
  - Chief Personnel Officer, Personnel Administration Division
  - Permanent Secretary, Ministry of Home Affairs
  - Permanent Secretary, Chief of Protocol, Ministry of Foreign Affairs
  - Chief/Deputy Chief Immigration Officer
  - Private Secretary to the Governor General
  - Commissioner/Deputy Commissioner/Assistant Commissioner/Senior Superintendent of Police
  - Superintendent/Assistant Superintendent of Prisons
- Any group of persons as prescribed by the International Business Unit

APPENDIX 5

VIRTUAL ASSET SERVICE PROVIDER – RED FLAG INDICATORS[6]

A transaction with multiple indicators and with little or no logical business explanation, could indicate potential criminal activity. This would require further monitoring, examination, and reporting where appropriate.

Transaction size and frequency	• Structuring transactions in small amounts and under the record-keeping or reporting thresholds. • Making multiple high-value transactions. • Transferring virtual assets immediately to multiple virtual asset service providers, including those registered or operated in other countries.
Transaction patterns that are irregular, unusual or uncommon can suggest criminal activity, for example when:	• New users make a large initial deposit to open a new relationship with a virtual asset service provider, inconsistent with the customer profile. • Transactions involve multiple virtual assets, or multiple accounts, without a logical business explanation. • Frequent transfers occur in a certain period of time to the same virtual asset account by more than one person, from the same location or concerning large amounts.
Technological features that increase anonymity	• Transactions involving more than one type of virtual assets particularly those that provide higher anonymity, such as anonymity enhanced cryptocurrency or privacy coins and despite additional transaction fees. • Virtual assets moved from a public, transparent blockchain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin. • Customers that operate as an unlicensed virtual asset service provider on peer-to-peer exchange website.

[6]Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing - September 2020: FATF

	• Abnormal transaction activity of virtual assets from peer-to-peer platform associated wallets with no logical business explanation. • Virtual assets traded to or from wallets that indicated the use of mixing or tumbling services or peer-to-peer platforms.
Geographical Risks These risks also exist if the originator of a transaction or the beneficiary of funds is linked to a high-risk jurisdiction. Indicators of this type of activity include:	• Customer funds originate from, or are sent to, an exchange that is not registered in the country where either the customer or exchange is located. • Customer utilises a virtual asset exchange or foreign-located Money Value Transfer Service in a high-risk country lacking, or known to have inadequate, AML/CFT /CPF regulations for virtual asset entities, including inadequate Customer Due Diligence or Know-Your-Customer measures.