ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM GUIDELINE FOR FINANCIAL INSTITUTIONS LICENSED UNDER THE FINANCIAL INSTITUTIONS ACT, CAP. 324A

Central Bank of Barbados
in conjunction with the Anti-Money Laundering Authority
Revised: November 2021

Table of Contents

ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

1.0 INTRODUCTION

1. The global threats of money laundering, and the financing of terrorism and proliferation of weapons of mass destruction have led financial sector regulators and financial institutions to strengthen their vigilance in support of the efforts of governments to counter these threats and to minimise the possibility that their jurisdictions or institutions becoming involved. Effective enforcement of policies to deter money laundering, and the financing of terrorism and proliferation of weapons of mass destruction, should, inter alia, enhance the integrity of the financial system and reduce incentives for the commission of crime within the jurisdiction.

2. The Central Bank of Barbados (Bank), in furtherance of its responsibility for the regulation and supervision of licensees under the Financial Institutions Act, Cap. 324A (FIA), has issued several revisions to its AML/CFT Guideline to licensees on how they can fulfil their obligations in relation to the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA).

3. This revised Guideline is being issued in conjunction with the Anti-Money Laundering Authority (Authority) pursuant to its powers under Section 26 of MLFTA and is updated to reflect the changes in local legislation, including the MLFTA, as well as the FATF Recommendations. The definitions appearing in the MLFTA apply mutatis mutandis to the Guideline.

4. The development and implementation of effective customer due diligence systems and monitoring mechanisms are essential to help combat money laundering and the financing of terrorism and proliferation. This Guideline sets out the expectations of the Bank and the Authority in relation to the minimum standards for anti-money laundering and the combating of the financing of terrorism (AML/CFT) and combating of the financing proliferation practices by all licensees and, together with the MLFTA, it will form an integral part of the framework used by the Bank in assessing how licensees implement their AML/CFT policies.

5. Section 22 of the MLFTA obligates all licensees to comply with this Guideline. The Guideline contains both advisory and obligatory requirements. Advisory matters are expressed by way of the phrase "the licensee or licensees may" and financial institutions are permitted to implement alternative but effective measures in these circumstances. Mandatory requirements are expressed using the phrase "the licensee or licensees should". Administrative sanctions for non-compliance with the Guideline are found at Section 34 of the Act.

2.0 APPLICATION

6. This Guideline[1] applies to all entities that are licensed under the FIA[2][3]. Licensees (including parent companies or financial holding companies for banking groups) should ensure that, at a minimum, this Guideline is also implemented in their branches and majority-owned subsidiaries abroad and, where permitted in the host country, ensure that those operations apply the higher of local and host standards. Licensees should inform the Bank and the Authority if the host laws and regulations prohibit the implementation of this Guideline; and take appropriate additional measures to address the ML/FT risks.

7. While other financial sector regulators have issued their own guidance notes to their sectors **(See Appendix 1)**, the Bank recognises that other persons and entities may also be vulnerable to money laundering and the financing of terrorism and proliferation. These persons and entities interface directly with licensees. It is recommended that they consider the issues embodied in this Guideline and, to this end, they may also avail themselves of the relevant portions of this Guideline.

3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM & PROLIFERATION

3.1 Money Laundering

8. Money laundering has been defined as the act or attempted act to disguise the source of money or assets derived from criminal activity. It is the effort to transform "dirty" money, into "clean" money. The money laundering process often involves:

i. The **placement** of the proceeds of crime into the financial system, sometimes by techniques such as structuring currency deposits in amounts to evade reporting requirements or co-mingling currency deposits of legal and illegal enterprises;
ii. The **layering** of these proceeds by moving them around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail; and
iii. **Integrating** the funds into the financial and business system so that they appear as legitimate funds or assets.

3.2 Financing of Terrorism

9. Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner. A successful terrorist group, much like a criminal organization, is generally able to obtain sources of funding and develop means of obscuring the links

[1] 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 financing of proliferation.
[2] The International Financial Services Act, Cap. 325 (IFSA) was repealed by the Financial Institutions (Amendment) Act, 2018. Effective January 1, 2019, licensees which were licensed under the IFSA are deemed to be licensed under Part IIIB of the FIA.
[3] Effective January 1, 2019, the Financial Institutions (Amendment) Act, 2018 made provision for a money or value transmission service provider (other than a bank) to be licensed under Part III of the FIA.

between those sources and the uses of the funds. While the sums needed are not always large and the associated transactions are not necessarily complex, terrorists need to ensure that funds are available to purchase the goods or services needed to commit terrorist acts. In some cases, persons accused of terrorism may commit crimes to finance their activities and hence transactions related to terrorist financing may resemble money laundering. 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 Bank's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting terrorism.

3.3 Financing of Proliferation (FP)

10. The FATF working definition of FP "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"[4]. The FATF Recommendations places obligations on countries as it relates to FP 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 Bank's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation.

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

4.0 INTERNATIONAL INITIATIVES

11. 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 (Interpretive Note to R.5 on foreign terrorist fighters); June 2016 (R.8 and its Interpretive Note on non-profit organizations); October 2016 (Interpretive 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); October 2018 (R.15 on new technologies)); June 2019 (Interpretive Note to R.15 on new technologies); October 2020 (R.1 & R.2 and the Interpretive Notes on assessing risk and applying a risk-based approach & national cooperation and coordination); and June 2021 (Interpretive Note to R.15 to clarify the applicability of proliferation financing risk assessment and mitigation requirements to virtual asset activities and service providers). 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-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 for Money or Value Transfer 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;*
- *Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers;*
- *Proliferation Financing Risk Assessment and Mitigation.*

Additionally, Principle 29 of the Basel Committee (Basel) Core Principles for Effective Banking Supervision, requires a bank to have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities. Financial institutions should keep abreast of developments in the international standard and refine their programmes accordingly.

12. Other useful references are provided in **Appendix 2** of the Guideline as well as the Annexes in FATF Guidance documents.

5.0 LEGISLATIVE AND REGULATORY FRAMEWORK

13. 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 include:

- 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, 2015 and 2019[5];
- Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23;
- Money Laundering and Financing of Terrorism (Prevention and Control) (Amendment) Act, 2019; and
- Criminal Assets Recovery Fund Act, 2016.

14. The MLFTA indicates that a financial institution engages in money laundering if it fails to take reasonable steps to implement or apply procedures to control or combat money laundering and it confers responsibility for the supervision of financial institutions[6] to the Authority, which was established in August 2000. A Financial Intelligence Unit (FIU) has been established as the office of the Authority. As the office of the Authority and as a member of the Egmont Group of FIUs, the FIU's responsibilities include:

i. Receiving suspicious or unusual transactions reports from Financial Institutions (FIs) and Designated Non-Financial Business Entities and Professionals (DNFBPs);
ii. Analysing suspicious or unusual transactions reports;
iii. Instructing FIs and DNFBPs to take steps that would facilitate an investigation; and
iv. Providing training to FIs and DNFBPs in respect of record keeping obligations and reporting obligations under the MLFTA.

15. Where a licensee is uncertain about how to treat an unusual or suspicious transaction, it is strongly urged to speak directly to the FIU for preliminary guidance and then make a report as appropriate. Where the FIU suspects on reasonable grounds that a transaction involves the proceeds of crime, the FIU will send a report for further investigation to the Commissioner of Police.

16. The Bank, the supervisory and regulatory agency for institutions licensed under the FIA, assesses these licensees' AML/CFT framework and compliance with the MLFTA through periodic onsite inspections and on-going offsite monitoring. Where deficiencies are identified in policy framework or operations of the control framework for managing the licensee's AML/CFT programme, the Bank will

[5] There are consequential amendments to the MLFTA.
[6] Offences and penalties under the MLFTA are set out in **Appendix 3**.

agree with the licensee on a time period to address the shortcomings. However, if the Bank is concerned by the seriousness of non-compliance and/or the lack of responsiveness to previous findings, the Bank will enforce its powers under Section 11(1)(d), Section 28 (Part III), Section 41B (Part IIIA) and Section 41I (Part IIIB) of the FIA (as amended); or Sections 33 to 36 of the MLFTA (See Section 37).

17. In addition, the Bank is required by law to provide any information that it has in its possession, which the FIU deems useful for an investigation that is being conducted for the purposes of the MLFTA.

18. From time to time, the Bank, in conjunction with the AMLA, will amend this Guideline but licensees should, as part of their risk management practices, stay current with emerging developments as they relate to AML/CFT and upgrade their AML/CFT programme where necessary.

6.0 THE ROLE OF THE BOARD AND SENIOR MANAGEMENT

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

20. The Board of Directors has ultimate responsibility for the effectiveness of the licensee's AML/CFT framework. Section 5(2)(b) of the MLFTA establishes that a financial institution engages in money laundering where the financial institution 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.

21. Directors and senior management should be aware that:

1. The use of a group wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the licensee and compliant with Barbadian law, regulations and guidelines. Failure to ensure compliance by the licensee with the requirements of the MLFTA may result in significant penalties for directors and the licensee **(See Appendix 3)**;

2. Licensees that are parent companies or financial holding companies for banking groups should implement group-wide AML/CFT programmes that encompass branches and majority owned subsidiaries. Such programmes should include:

a. Policies and procedures for sharing information required for the purposes of CDD and ML/FT risk management;
b. The provision, at group-level compliance, audit, and/or AML/CFT functions, of a customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This includes information and analysis of transactions and activities which appear unusual (if such analysis was done). Similarly, branches and subsidiaries should receive such information from these group level functions when relevant and appropriate for risk management; and
c. Adequate safeguards on the confidentiality and use of information exchanged, including the prevention of tipping-off.

3. Majority owned subsidiaries and branches of licensees including those domiciled outside of Barbados are expected to, at a minimum, comply with the requirements of Barbados MLFTA and this Guideline; and

4. Where some of licensee's operational functions are outsourced, the licensee retains full responsibility for compliance with local laws, regulations and guidelines.

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

a. Understanding the statutory duties placed upon them, their staff and the entity itself;
b. Approving AML/CFT policies and procedures that are appropriate for the risks faced by the licensee. 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 licensee's AML/CFT procedures are being managed effectively; and
d. Seeking assurance that the licensee is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems. See Section 10.0.

23. Senior management is responsible for the development of sound risk management programmes and for keeping directors adequately informed about these programmes and their effectiveness. These programmes should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments. Licensees should formally document policies, which at a minimum, irrespective of whether the licensee receives funds from third parties or not, should provide for:

i. The development of internal policies, procedures and controls for inter alia:

a. The opening of customer accounts and verification of customer identity;
b. Establishing business relations with third parties (including custodians, fund

managers, correspondent banks, business introducers);
c. Determining business relationships and transactions that the licensee will not accept [also see Section 7.4.9(vi)];
d. The timely detection of unusual and suspicious transactions, and reporting to the Authority;
e. Internal reporting; and
f. Record retention.

ii. The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, and research of unusual transactions and reporting of suspicious activities;
iii. An on-going training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;
iv. Designation of a compliance officer at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program, receive internal reports and issue suspicious transaction reports to the Authority; See Sections 20 and 23 of the MLFTA.
v. Establishment of management information/reporting systems to facilitate aggregate and group wide monitoring;
vi. An effective independent risk-based oversight function to test and evaluate the compliance program; and
vii. Screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the licensee from being used for criminal activity.

24. Policies should be periodically reviewed for consistency with the business model, product and service offering, and the licensee's risk appetite. Special attention should be paid to new and developing technologies. In this regard, licensees should (a) identify and assess ML/FT risks arising from new products/services and delivery channels; new business practices and new or developing technologies for new and existing products and (b) manage and mitigate such risks. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

6.1 Risk-Based Approach[7]

25. The Bank recognises the diversity of the institutions it regulates and it will seek to establish that, overall, processes appropriate to institutions are in place and operating effectively. All licensees should therefore design an AML/CFT framework that satisfies the needs of their institution, taking into account inter alia:

i. The nature and scale of the business;

[7] In keeping with The FATF Recommendations, examples are not mandatory elements of the standards and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

ii. The complexity, volume and size of transactions;
iii. The degree of risk associated with each area of operation;
iv. Type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group);
v. Type of product/service (e.g. whether private banking, one-off transaction, mortgage);
vi. Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);
vii. 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);
viii. The internal audit and regulatory findings; and
ix. Value of customer accounts and frequency of transactions.

26. Licensees should also observe higher/lower risks identified in risk assessments undertaken by the Bank and the National Risk Assessment and take appropriate enhanced or simplified measures.

27. In keeping with Section 17 of the MLFTA, licensees should apply customer due diligence standards on a risk sensitive basis depending on the type of customer, business relationship or transaction. Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems. Alternatively, licensees should apply enhanced due diligence to customers (Section 7.4) where the risk of being used for money laundering or terrorist financing is high.

28. Licensees should document a risk-based approach in their AML/CFT programmes. This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

29. Licensees are required to:

(a) document their risk assessments;
(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
(c) keep these assessments up to date; and
(d) have appropriate mechanisms to provide risk assessment information to the Bank.

30. 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. As part of this exercise, licensees should consider risk variables, either singly or in combination, which may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

a. The purpose of an account or relationship.

b. The level of assets to be deposited by a customer or the size of transactions undertaken.
c. The regularity or duration of the business relationship.

31. While each licensee will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks. In addition to "Red Flags" appended to this Guideline, typologies of money laundering and terrorist financing schemes are available[8] to assist in risk categorisation.

32. Licensees should ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories and that the requisite due diligence is being followed. In addition, licensees should periodically review their risk categories as typologies evolve on practices by money launderers and terrorists.

6.2 Proliferation Financing Risk Assessment and Mitigation

33. Licensees should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks. Licensees should take appropriate steps to manage and mitigate identified proliferation financing risks, which may be done within existing targeted financial sanctions framework and/or compliance programmes.

34. Licensees should always understand their proliferation financing risks and document proliferation financing risk assessments to:

(a) Demonstrate their basis;
(b) Keep the assessment up to date; and
(c) Have appropriate mechanisms to provide information to the Bank.

35. The nature and extent of any proliferation risk assessment should be appropriate to the size and nature of the business. The nature of risk mitigation measures will depend on the source and degree of risks and should be commensurate with the level of risk. These measures could include:

a. Improved onboarding processes for customers (including beneficial owners);
b. Enhanced customer due diligence procedures;
c. Effective maintenance of customer master data;
d. Regular controls to ensure effectiveness of procedures for sanctions screening; and
e. Leveraging the existing compliance programmes (including internal controls) to identify potential sanctions evasion.

[8] For example, www.fatf-gafi.org.

7.0 CUSTOMER DUE DILIGENCE

36. Customer due diligence is an essential element of the effort to prevent the financial system from being used to perpetrate money laundering and terrorist financing. Licensees are ultimately responsible for verifying the identity of their customers. In this regard, licensees should not accept anonymous accounts or accounts in fictitious names. If licensees maintain numbered accounts, they should ensure compliance with this Guideline.

37. As part of their due diligence process, licensees should:

1) Establish procedures for obtaining identification information on new customers so as to be satisfied that a prospective customer is who he claims to be;
2) Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset[9] of a business relationship. This process should include, where appropriate:

    A. Taking reasonable measures to understand the ownership and control structure of the customer;
    B. Obtaining reliable, data or information from an independent source on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and
    C. Discontinuing the transaction, if customer documentation information is not forthcoming at the outset of the relationship.

3) Employ enhanced due diligence procedures for high risk customers or transactions (Section 7.4);
4) Update identification records, on a risk-focussed basis, to ensure that all existing customer records are current and valid and conform to any new requirements (Section 7.6);
5) Monitor account activity throughout the life of the business relationship in accordance with Section 16 of the MLFTA; and
6) Review the existing records if there is a material change in how the account is operated or if there are doubts about previously obtained customer identification data.

38. 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.

[9] For the purpose of this Guideline, the outset of the relationship is the earlier of acceptance of the signed application/proposal, or the first receipt of funds from the customer.

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.

39. 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 such as, but not limited to:

- Opening of deposit accounts;
- Entering into fiduciary transactions;
- Renting safe-deposit boxes;
- Requesting safe custody facilities; and
- Occasional transactions exceeding thresholds as discussed below or linked transactions under this benchmark, and all occasional wire transfers.

40. Section 2 of the MLFTA defines an occasional transaction as a financial or other relevant transaction other than one that is conducted or to be conducted in the course of an existing business arrangement and includes a wire transfer. An occasional transaction may also include:

a. Encashment of cheques drawn on the licensee;
b. Exchange of coins for cash;
c. Purchase of foreign currency for holiday travel; and
d. Currency exchanges e.g. bureau de change and cambios.

41. Licensees should undertake due diligence on, inter alia:

- Occasional wire transfers over BDS$2,000 or its equivalent in foreign currency; and
- All currency exchange transactions over BDS$2,000 or its equivalent in foreign currency.

42. The extent of identity information and verification of occasional transactions below these thresholds[10] is dependent on the materiality of the transaction and the degree of suspicion.

43. At a minimum, a licensee should:

A. Identify and verify[11] the persons conducting occasional transactions below the threshold cited above. (See Section 7.4.9 on wire/funds transfers);
B. Maintain an effective system to monitor for abuse of occasional transactions; and
C. Establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

44. In effecting the due diligence process, licensees should:

i. Whenever possible, require prospective customers to be interviewed in person. Exceptions to this are outlined in Sections 7.4.3 and 7.4.4;
ii. In verifying customer identity, use independent official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to opening the account or establishing the business relationship. Identification documents which do not bear a photograph or signature and which are easily obtainable (e.g. birth certificate) are not acceptable as the sole means of identification. Customer identity can be verified using a combination of methods such as those listed at **Appendix 4**. Verification may involve the use of external electronic databases;
iii. In instances where original documents are not available, only accept copies that are certified by an approved person. See **Appendix 5**. Approved persons should print their name clearly, indicate their position or capacity together with a contact address and phone number;
iv. If the documents are unfamiliar, take additional measures to verify that they are genuine e.g. contacting the relevant authorities; and
v. Determine through a risk analysis of the type of applicant and the expected size and activity of the account, the extent and nature of the information required to open an account. Examples of documentation for different types of customers are set out in Sections 7.1 to 7.5.

45. Generally, licensees should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, where it would be essential not to interrupt the normal conduct of business (e.g. non face-to-face business and securities transactions), verification may be completed after establishment of the business relationship. However, a reasonable timeline for completing the verification process should be established. Should this be determined to be an acceptable risk, licensees should adopt risk management procedures with respect to the conditions

[10] See Section 9.0 for discussion on profiling and business transaction limits.
[11] At a minimum, identification information should consist of the customer's name and address, which is verified by valid photo-bearing ID with a unique identifier.

under which a customer may utilise the business relationship prior to verification[12]. If the requirements are not met, and it is determined that the circumstances give rise to suspicion, the licensee should make a report to the Authority (See Section 9.0).

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

7.1 Personal Customer

47. A licensee should obtain relevant information on the identity of its customer and seek to verify some of the information on a risk basis, through the use of reliable, independent source documents, data or information to prove to its satisfaction that the individual is who that individual claims to be. See Section 2 of the MLFTA. The basic information should include:

a. True name and permanent residential address;
b. Valid photo-bearing identification, with unique identifier, (e.g. passport, national identification card, driver's licence);
c. Date and place of birth and nationality (if dual, should be indicated);
d. Occupation and business or principal activity;
e. Contact details e.g. telephone number, fax number and e-mail address;
f. Purpose of the account; and
g. Signature.

48. In addition, the licensee may obtain any other information deemed appropriate and relevant e.g. source of funds and estimated account turnover.

49. The licensee should determine the degree of verification to be undertaken on a risk basis. In some instances, verification may be satisfied by maintaining current photo-bearing identification with a unique identifier (e.g. passport, national identification card).

50. Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted if certified by persons listed in **Appendix 5.**

7.1.1 Unavailability of Identity Documents

51. There may be circumstances where some types of customers are unable to supply the identity documents at Section 7.1. Such customers include the elderly, the disabled, students, minors and

[12] Procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship.

individuals dependent on the care of others. Licensees may determine what alternate identity documentation to accept and verification to employ. Where applicable, the following should be among documentation obtained:

a) A letter or statement from a person listed at **Appendix 5** that the person is who he/she states;
b) Confirmation of identity from another regulated institution in a jurisdiction with equivalent standards;
c) Confirmation(s) from the student's workplace, school, college or university; and
d) Identity information on the adult opening the account, and a birth certificate, or national registration card for the account holder.

7.2 Corporate Customer

52. To satisfy itself as to the identity of the customer, the licensee 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 (See Section 7.1) 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 private, identity should be sought on persons with a minimum shareholding of 20%.

f. Identity information (See Section 7.1) 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 (see Section 7.0(37)(ii) and bullet e above);
g. Description and nature of business;
h. Purpose of the account, source of funds and the estimated account activity;
i. 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;
j. By-laws and any other relevant documents, and any amendments thereto, filed with the Registrar of Corporate Affairs and Intellectual Property, the Registrar of Co-operatives or

the Registrar of Friendly Societies, as the case may be;

k. Board resolution authorising the opening of the account and conferring authority on signatories to the account; and

l. Recent financial information or audited statements.

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

7.3 Partnership/Unincorporated Business

54. Partnerships and unincorporated businesses should meet the relevant requirements set out in Section 7.1. 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.

7.4 Enhanced Due Diligence

55. A licensee may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A licensee 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. Licensees should observe the "**Improving Global AML/CFT Compliance: Ongoing Process Statements**" and "**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. Refer to the **FATF: High Risk & Other Monitored Jurisdictions**[13] and any lists of high-risk jurisdictions provided by the Competent Authority from time to time.

56. In addition to the above, the Competent Authority may require countermeasures, which are effective and proportionate, to the risks identified from listed countries, either when called upon to do so by the FATF and CFATF or independently of any call to do so. Such countermeasures that the Competent Authority may impose include:

1) Requiring financial institutions to apply specific elements of enhanced due diligence;
2) Prohibiting financial institutions from establishing subsidiaries, branches or representative offices in the country concerned, or otherwise taking into account the fact

[13] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/

that the relevant subsidiary, branch or representative office would be in a country that does not have adequate AML/CFT systems;

3) Limiting business relationships or financial transactions with the identified country or persons in that country;
4) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process;
5) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned; and,
6) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

57. Regarding the policy framework, the licensee 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.

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

7.4.1 Trust Clients & Other Legal Arrangements

59. Licensees should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction is conducted. This applies especially if there are any doubts as to whether or not these clients or customers are acting on their own behalf.

60. At a minimum, the licensee should obtain the following[14] :

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

[14] These minimum requirements apply whether the licensee is a named trustee or is providing services to a trust.

power to appoint or remove the trustee and where possible the names or classes of beneficiaries;

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

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

61. 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 licensee should verify beneficiaries before the first distribution of assets. Further, licensees should verify protectors/controllers the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

62. 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.

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

64. Licensees should inform the Bank and the FIU when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of this Guideline.

7.4.2 Non-Profit Organisations (NPOs)

65. The FATF has adopted a functional definition of an 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, an 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". 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. Licensees should therefore, apply a risk-based approach to NPOs and apply effective and proportionate measures.

66. 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 financial 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 financial institutions manage business relationships with customers who are NPOs. To assess the risk, a licensee 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.

67. The licensee 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.

68. As part of the verification process, licensees 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, licensees should examine whether funds are being sent to high-risk countries. Licensees 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.

7.4.3 Non Face-to-Face Customers

69. 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, licensees should pay special attention to risks associated with new and developing technologies. Customers may complete applications but licensees should satisfy the requirements in this section before establishing a business relationship.

70. 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, licensees should:

A. Obtain documents certified by approved persons listed at **Appendix 5**;
B. Ensure that all company documents are signed by the Company Secretary;

C. Request additional documents to complement those which are required for face-to-face customers, including more than one photo bearing ID;
D. Make independent contact with the customer, for example by telephone on a listed business or other number; and
E. Request third party introduction e.g. by an introducer as noted in Section 7.4.4.

71. In addition, the licensee 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.

72. Where initial checks fail to identify the customer, the licensee 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.

73. Where a licensee 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 licensee should make all efforts to obtain such information within a reasonably timeline. In accepting such transactions, licensees should:

I. Set limits on the number and aggregate value of transactions that can be carried out;
II. Indicate to customers that failure to provide the information within the established timeframe, may trigger the termination of the transaction; and
III. Consider submitting a suspicious report.

7.4.4. Introduced Business

74. A licensee may rely on other regulated third parties to introduce new business in whole or in part but the ultimate responsibility remains with the licensee for customer identification and verification. A licensee 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 licensee itself;
c. 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 Recommendations[15];

d. Obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;
e. Satisfy itself that an introducer continues to conform to the criteria set out above (e.g. conduct periodic reviews);
f. Consider terminating the relationship where an introducer fails to provide the requisite customer identification and verification documents; and
g. Consider terminating the relationship with an introducer who is not within the licensee's group, where there are persistent deviations from the written agreement.

75. When a prospective customer is introduced from within a licensee's group, provided the identity of the customer has been verified by the introducing regulated parent company, branch, subsidiary or associate in line with the standards set out in the Guideline, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. The licensee should however, retain copies of the identification records in accordance with the requirements in the MLFTA. Licensees should obtain written confirmation from a group member confirming completion of verification. **See Appendix 6**.

7.4.5. Professional Service Providers

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

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.

77. Where pooled accounts are managed by:

a. Providers on behalf of entities such as mutual funds and pension funds; or
b. Lawyers or stockbrokers representing funds held on deposit or in escrow for several individuals, and funds being held are not co-mingled (i.e. there are sub-accounts), the licensee should identify each beneficial owner. Where funds are co-mingled, the licensee

[15] For example, refer to country assessment reports available on some websites listed in **Appendix 2**.

should take reasonable measures to identify the beneficial owners. Subject to the Bank's approval, the latter is not required where the provider employs at a minimum, equivalent due diligence standards as set out in this Guideline and has systems and controls to allocate the assets to the relevant beneficiaries. Licensees should apply the criteria at Section 7.4.4 in conducting due diligence on providers.

78. Licensees should observe guidance from the FIU regarding attorney-client accounts.

7.4.6. (a) Politically Exposed Persons (PEPs)

79. Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which licensees may face have led to calls for enhanced due diligence on such persons. The FATF categorises PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organisation[16].

80. Financial institutions should, in relation to foreign PEPs (whether as a customer or beneficial owner), in addition to performing normal customer due diligence measures:

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.

81. With respect to domestic PEPs or persons who are or have been entrusted with a prominent public function by an international organization, in addition to performing normal customer due diligence measures, financial institutions should:

a) Take reasonable measures to determine whether a customer or the beneficial owner is such a person; and
b) In cases of a higher risk business relationship with such persons, apply the measures referred to in paragraphs (b), (c) and (d) above.

[16] The FATF Recommendations categorises PEPs as follows:
Foreign PEP as "individuals who are or have been entrusted with prominent public functions by a foreign country (e.g. Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political parties officials").
Domestic PEP as "individuals who are or have been entrusted domestically with prominent public functions (e.g. Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political parties officials").
Persons who are or have been entrusted with the prominent function by an international organisation refer to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.
The definition of PEP is not intended to cover middle ranking or more junior individuals in the foregoing categories.

82. However, a domestic PEP is subject to the foreign PEPs requirements if that individual is also a foreign PEP through another prominent public function in another country.

83. The requirements for all types of PEP should also apply to family members or close associates[17] of such PEPs.

7.4.6 (b) PEP Status

84. The handling of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits[18].

85. The risk-based approach requires that financial institutions assess the ML/TF risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors are:

a. the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or
b. whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

86. Licensees should therefore consider the above factors when determining the PEP status of its customers.

7.4.7. Corporate Vehicles

87. Barbados law prohibits companies from issuing shares in bearer form. Where a licensee decides that companies with nominee shareholders represent an acceptable business risk, they should exercise care in conducting transactions. Licensees should ensure they can identify the beneficial owners of such companies and should immobilise bearer shares and bearer share warrants[19] as a means of monitoring the identity of such companies by, for example, requiring custody by:

a. The licensee, or its subsidiary, regulated affiliate, parent or holding company;
b. A recognized regulated financial institution in a jurisdiction with equivalent AML/CFT standards; and

[17] ***Family members*** are individuals who are related to a PEP either 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.
[18] Refer to *FATF Guidance on Politically Exposed Persons*
[19] A ***bearer share warrant*** is a document issued by a company certifying that the bearer is entitled to a certain amount of fully paid stock shares.

c. Requiring the prior approval before shares can be exchanged.

7.4.8. (a) Correspondent Banking

88. Correspondent banking relates to the provision of banking services by one bank (correspondent) to another bank, usually domiciled overseas (respondent). A correspondent bank processes &/or executes transactions for third parties i.e. customers of respondent banks; and may also engage in trade finance related services, cash clearing, liquidity management and short term borrowing, foreign exchange or investment in a particular currency. Cross border correspondent banking involving third parties may present enhanced risk, however, there is no requirement for a correspondent bank to conduct due diligence on the customers of their customers.

89. The decision to approve a respondent relationship should depend inter alia on the licensee's assessment of all relevant risk factors, including the nature of the counterpart's business, their money laundering and terrorist financing prevention and detection systems and controls, and the quality of bank supervision and regulation in the counterpart's country. Licensees offering cross-border wire or fund transfers should not conduct correspondent and respondent banking relations with shell banks[20]. Additionally, licensees are required to have a clear understanding of the respective AML/CFT responsibilities of both (i.e. correspondent and respondent) institutions.

90. Licensees that offer correspondent banking services should conduct due diligence on their respondent banks on a risk basis as well as ongoing due diligence to ensure that CDD information and the risk assessment on the counterpart remain up-to-date. Reduced due diligence is acceptable where the respondent bank is listed on a recognized stock exchange; or is a member of the licensee's own financial group and subject to a group AML/CFT programme and consolidated supervision.

91. Where as a correspondent bank, the licensee has determined the need for enhanced due diligence the licensee obtains the following on the respondent bank:

a. Information on ownership and governance;
b. Assessment of the risk profile (consider e.g. the location, nature of major business activities, and whether the bank has been subject to a money laundering or terrorist financing investigation or regulatory action);
c. Satisfy itself that there is an equivalent AML/CFT programme in place;
d. Confirm that the respondent does not maintain business relations with shell banks;
e. Assess of the quality of bank supervision and regulation in the respondent's country;
f. Obtain senior management's approval before establishing the relationship; and

[20] A ***shell bank*** is a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

g. In relation to payable-through-accounts[21], the licensee should confirm that the respondent bank has conducted CDD on the customers having direct access to accounts of the licensee, and that the relevant CDD information is available upon request by the licensee.

7.4.8 (b) MVTS Providers (CDD by other Financial Institutions)

92. The FATF definition of money or value transfer service (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such providers can involve one or more intermediaries and a final payment to a third party, and may include new payment methods.

93. As part of their normal CDD processes, financial institutions should understand the purpose and nature of the intended business relationship e.g. whether the MVTS provider intends to use the account for its own corporate or settlement purposes; or whether it intends to use the account to provide correspondent services to its own customers. In the latter case, where the MVTS provider acts as intermediary for other MVTS providers or is accessing banking or similar services through the account of another MVTS customer, the correspondent bank should consider all of the factors listed above for respondent banks.

94. It is only after considering all relevant risk factors, and on a case by case basis, should a licensee apply enhanced due diligence to a MVTS provider.

7.4.8 (c) Virtual Asset Service Provider (VASP)

95. 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 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;

[21] ***Payable-through-accounts*** refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

- Exchange between one or more forms of virtual assets;
- Transfer[22] 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.

96. 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.

7.4.9 Wire/Funds Transfer[23]

97. For the purposes of this Guideline, wire transfer and funds transfer refer to any transaction carried out on behalf of an originator[24] person through a licensee by electronic means for availability to a beneficiary person at another financial institution. The originator and beneficiary may be the same person. Beneficiary refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

98. When serving as intermediary or beneficiary financial institutions, licensees should:

(a) take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information; and,
(b) have risk-based policies and procedures which include:

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

[22] ***Transfer*** means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.
[23] Agents of MVTS Providers are required to comply with this section, where relevant.
[24] The ***originator*** is the account holder who allows the wire transfer from that account, or where there is no account, the person (natural or legal) that places the order with the ordering financial institution to perform the wire transfer.

99. The degree of enhanced due diligence depends on the licensee's role in the wire transfer and the size and origin or destination of the funds. These circumstances are set out below:

For Ordering Financial Institutions:

i) The licensee should obtain, retain and verify the full originator information, i.e. the originator's name, account number (or unique identifier where the originator is not an account holder), and address[25] for wire transfers in any amount. Verification of existing customers should be refreshed where there are doubts about previously obtained information.

ii) The licensee should include in cross-border wire transfers above the BDS$2,000 threshold full originator and beneficiary information[26]. Batch transfers[27] that include cross-border wire transfers sent by a money/value transfer service provider should be treated as cross-border transfers.

iii) Where the institution is conducting a domestic transfer above the BDS$2,000 threshold, the licensee should include full originator information. However, the licensee may send only the originator's account number (or unique identifier) where full originator information can be made available to:

a. The receiving financial institution and the Bank within three (3) business days of receipt of a request; and
b. Domestic law enforcement authorities upon request.

iv) Licensees should observe requirements at bullets i) and ii) above for all cross-border wire transfers below BDS$2,000.

v) Batch transfers that include cross-border transfers may be treated as domestic wire transfers, provided that the requirements applicable to domestic transfers are met.

vi) Licensees should not execute wire transfers if the criteria above (i to v) are not met.

For Intermediary Financial Institutions:

vii) The licensee should ensure that all originator and beneficiary information from cross-border transfers of any amount, remain with the related transfers. Where difficulties arise in maintaining this information with a related domestic wire transfer, then all information received from the ordering or other intermediary financial institution should be retained for no less than five years in accordance with Section 18 of the MLFTA.

[25] It is permissible to substitute national identity number/customer identity number/date and place of birth.
[26] Beneficiary information should include name of the beneficiary and the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.
[27] In general, only routine wire/funds transfers should be batched.

For Beneficiary Financial Institutions:

viii) For cross border wire transfers of BDS$2,000 and above, licensees should verify the identity of the beneficiary, if the identity has not been previously verified. Information should be maintained in accordance with Section 11.

100. The requirements are not applicable to the following types of payments:

a. Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, the necessary information should be included in the message; and
b. Financial institution-to-financial institution transfers where both the originator and the beneficiary are financial institutions acting on their own behalf.

101. Where a relationship is deemed high risk e.g. located in a high-risk jurisdiction, further to standard due diligence, a licensee should undertake a more detailed understanding of the:

i) AML/CFT programme of the respondent bank and its effectiveness;
ii) Review effectiveness of the respondent's group programme;
iii) Respondent's owners, director and senior managers; and
iv) Ownership structure.

102. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider is required to:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

7.5 Reduced Customer Due Diligence

103. As discussed in Section 6.1, the licensee's policy document should clearly define the risk categories/approach adopted and associated due diligence, monitoring and other requirements. A licensee may apply reduced due diligence to a customer provided it satisfies itself that the customer is of such a risk level that qualifies for this treatment.

7.6 Retrospective Due Diligence

104. Where the identity information held on existing customers does not comply with the requirements of this Guideline, licensees should develop a risk-based programme for ensuring compliance. Licensees should:

i. Record their non-compliant business relationships, noting what information or documentation is missing;
ii. Establish a framework for effecting retrospective due diligence, including the setting of deadlines for the completion of each risk category. The timing of retrofitting can be linked to the occurrence of a significant transaction, a material change in the way that an account is operating, or doubts about previously obtained customer due diligence data; and
iii. Establish policies for coping with an inability to obtain information and documentation, including terminating the relationship and making a suspicious report.

105. Where a licensee deems on the basis of risk and materiality, that it is not practical to retrofit a customer (e.g. the settlor has died; the account is inactive or dormant), exemption of such accounts should be approved by the compliance officer and senior management, ratified by the board and documented on the individual's file.

8.0 AGENT[28] OF MVTS PROVIDERS

106. The nature and structure of agents and their relationships with MVTS providers vary. Agents may include small independent entities with a contractual relationship directly with the MVTS provider to provide services on their behalf. Alternatively, agent networks may operate on a tiered structure where an agent operating on behalf of its established network of entities (e.g. through a chain of retail outlets) enters into a contractual relationship with the MVTS provider.

107. Agent Due Diligence is intended to enable a MVTS provider to ensure that it knows the legal and ownership structure of its agents and that it will be forming business relationships with legitimate and viable agents that will implement or adhere to AML/CFT requirements, program responsibilities, policies and procedures. The MVTS provider's procedures should include these factors:

- Identifying the agent and performing the necessary due diligence, such as, inter alia, length of time in business, whether the agent is representing more than one MVTS provider, ownership structure, financial viability;
- Obtaining appropriate additional information to understand the agent's business such as expected nature and level of transactions, the agent's past record of legal and regulatory compliance;
- Ensuring compliance regime adherence to internal policies and external regulation such as reporting suspicious or attempted suspicious activities, monitoring and record keeping, through AML/CFT compliance program reviews; and
- Conducting ongoing AML/CFT training and new agent AML/CFT training encompassing

[28] The FATF Recommendations define an ***agent*** as "any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider".

applicable AML/CFT requirements, AML/CFT compliance program responsibilities, and MVTS internal policies and procedures.

108. The MVTS provider is exposed to risk when an agent engages in transactions that create a risk for money laundering, terrorist financing, or other financial crime. To mitigate exposure to risk, the MVTS provider should have procedures in place to identify those agents conducting activities that appear to lack commercial purpose, lack justification, or otherwise are not supported by verifiable documentation. MVTS providers are required to develop and implement risk-based policies, procedures, and internal controls that ensure adequate ongoing monitoring of agent activity, as part of the implementation of the AML/CFT program.

109. In applying a risk-based approach to monitoring, the degree of monitoring should be based on the perceived risks, both external and internal, associated with the agent. The degree and nature of agent monitoring will depend on, inter alia, the transaction volume of the agent, the monitoring method being utilised (manual, automated or some combination), and countries where funds are sent. Prompt attention and remediation of risk behaviours should be addressed by appropriate means, and the MVTS provider should implement procedures for handling non-compliant agents, including agent contract terminations.

9.0 UNUSUAL & SUSPICIOUS TRANSACTIONS

110. Suspicious transactions are business transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism offence. These transactions may be complex, unusual or large or may represent an unusual pattern. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or a very high account turnover that is inconsistent with the expected pattern of transactions. In some instances, the origin of the transaction may give rise to suspicion. For examples of "Red Flags" see **Appendix 7**.

111. A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and determination of consistent transaction limits. Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis. 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.

112. Licensees should develop procedures to assist in the identification of unusual or suspicious activity in all types of business transactions, products and services offered (for example wire transfers, credit/debit cards and ATM transactions, lending, trust services and private banking).

113. A licensee should:

A. Develop effective manual &/or automated systems to enable staff to monitor, on a solo, consolidated and group-wide basis, transactions undertaken throughout the course of

the business relationship and identify activity that is inconsistent with the licensee's knowledge of the customer, their business and risk profile; and

B. Determine customer specific limits based on an analysis of the risk profile of customers, the volume of transactions and the account turnover. This may give rise to multiple limits and/or aggregate limits on a consolidated basis.

114. Licensees should not grant blanket exemptions and should:

i. Clearly document their policy for the granting of such exemptions including the qualifying criteria for exemption, officers responsible for preparing and authorizing exemptions, the basis for establishing threshold limits, review of exempt customers and procedures for processing transactions;
ii. Maintain authorised exempt lists showing threshold limits established for each qualifying customer; and
iii. Monitor currency exchanges and international wire transfers.

115. For the purposes of this Guideline, and consistent with Section 2 of the MLFTA, a transaction includes an attempted or aborted transaction.

9.1 Internal Reporting Procedures

116. To facilitate the detection of suspicious transactions, a licensee should:

i. Require customers to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount as the licensee determines, to reasonably ascertain that funds are not the proceeds of criminal activity. **Appendix 8** indicates a specimen of a Declaration Source of Funds (DSOF) form. Where electronic reports are employed instead of the form, they should capture the information included on the Appendix and should be signed by the customer;
ii. Develop written policies, procedures and processes to provide guidance on the reporting chain and the procedures to follow when identifying and researching unusual transactions and reporting suspicious activities;
iii. Identify a suitably qualified and experienced person to whom unusual and suspicious reports are channelled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the Authority (See Section 9.2);
iv. Require its staff to document in writing their suspicion about a transaction; and
v. Require documentation of internal enquiries.

9.2 External Reporting

117. Licensees are required by law to report promptly to the Authority where the identity of the person or entity involved, the transaction or any other circumstance concerning that transaction lead the licensee to have reasonable grounds to suspect that a transaction:

i) Involves proceeds of crime to which the MLFTA applies;
ii) Involves terrorist financing;
iii) Involves the financing of proliferation;
iv) Is of a suspicious or an unusual nature; or
v) Is conducted by, or relates to, a person or entity against whom a terrorist designation order is in force or relates to the property of such a person or entity.

118. Where a suspicious report[29] has been filed with the Authority, and further unusual or suspicious activity pertaining to the same customer or account arises, licensees should file additional reports with the Authority.

119. Freezing and Unfreezing: 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 will be communicated electronically or in the Official Gazette and local newspapers. Financial 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, financial institutions should have a mechanism in place to release the assets previously frozen.

See the detailed Guideline on Targeted Financial Sanctions for Financial Institutions and Designated Non-Financial Business Entities and Professionals (See http://www.centralbank.org.bb/financial-stability-and-financial-regulation/aml-cft).

120. Licensed financial institutions, their directors, officers, employees and agents are protected under the MLFTA from any action, suit or proceedings for breach of any restriction on disclosure of information, if they report suspicious activity in good faith to the Authority, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. See Sections 48(5) and 48(6) of the MLFTA. It is against the law for employees, directors, officers or agents of a licensee to disclose that a suspicious transaction report or related information on a specific transaction has not been reported, is in the process of being reported, or has been reported, to the Authority. These provisions are not intended to inhibit information sharing within financial groups. (See Section 6.0).

121. Reports should be in the format determined by the FIU (See http://www.centralbank.org.bb/financial-stability-and-financial-regulation/aml-cft). However, where a matter is considered urgent, an initial report may be made by contacting the FIU by telephone or encrypted e-mail.

[29] Refer to the *Guidance Note on the Preparation and Submission of High Quality Suspicious Transaction/Activity Reports*

122. Where a person is a client of both the licensee and another group member, and a suspicious report is prepared by the latter, the Barbados FIU should be notified.

10.0 COMPLIANCE AND AUDIT

123. All licensees 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.

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 the Bank 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 Bank 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 financial or mixed conglomerate, the Group Compliance Officer or Group Internal Audit may perform the compliance and/or internal audit services. Where this is not possible, a licensee may, subject to the Bank's agreement, outsource the operational aspects of the compliance or internal audit function to a person or firm that is not involved in the auditing or accounting functions of the 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 and be in a position to readily respond to the Bank and FIU on AML/CFT issues.

11.0 RECORD-KEEPING

126. To demonstrate compliance with the MLFTA and to allow for timely access to records by the Bank or the FIU, licensees should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including customer identification data, business transaction records, internal and external reporting and training records.

127. Licensees should maintain business transaction records for a minimum of **five years** in accordance with Section 18 of the MLFTA.

128. However, it may be necessary for licensees to retain records, until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where:

i. There has been a report of a suspicious activity; or
ii. There is an on-going investigation relating to a transaction or client.

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

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

131. In the case of a merger or acquisition, the licensee should ensure that the records described above can be readily retrieved. Where the records are kept under a contractual arrangement by an entity other than a licensee, the licensee is responsible for retrieving those records before the end of the contractual arrangement.

132. The nature of records that should be retained is set out at Section 2 of the MLFTA, which defines a business arrangement, business transaction and business transaction record.

11.1 Internal and External Records

133. Licensees should maintain records related to unusual and suspicious business transactions for no less than 5 years. 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 Competent Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and
vi. Reports to the Competent Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.

11.2 Training Records

134. In order to provide evidence of compliance with Section 21 of the MLFTA at a minimum, a licensee should maintain the following information:

a) Details and contents of the training programme provided to staff members;
b) Names of staff receiving the training;
c) Dates that training sessions were held;
d) Test results carried out to measure staff understanding of money laundering, terrorist financing and the financing of proliferation requirements; and
e) An on-going training plan.

12.0 TRAINING AND AWARENESS

135. An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analysing potential illicit transactions. Therefore, licensees should establish on-going employee training programmes. Training should be targeted at all employees but added emphasis should be placed on the training of the Compliance Officer and the compliance and audit staff because of their critical role in sensitising the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures. Additionally, front line staff should be targeted so as to enable them to respond appropriately when interacting with the public.

136. Licensees should:

i. Develop an appropriately tailored training and awareness programme consistent with their size, resources and type of operation to enable their employees to be aware of the risks associated with money laundering and terrorist financing, to understand how the institution might be used for such activities, to recognise and handle potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;
ii. Clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious transaction reporting;
iii. Formally document, as part of their anti-money laundering policy document, their approach to training, including the frequency, delivery channels and content;
iv. Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the Reporting Officer to whom they should report unusual or suspicious transactions;
v. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:

   a. New hire orientation;
   b. Operations staff;
   c. Supervisors;
   d. Board and senior management; and
   e. Audit and compliance staff.

vi. Obtain an acknowledgement from each staff member on the training received;
vii. Assess the effectiveness of training[30]; and
viii. Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

12.1 Content and Scope of the Training Programme

137. Regarding the overall training programme, a licensee should cover topics pertinent to its operations and should be informed by developments in international AML/CFT standards. Training should be general as well as specific to the area in which the trainees operate. As staff members move between jobs, their training needs for AML/CFT may change. Training programmes should, inter alia, incorporate references to:

[30] Assessment methods include written or automated testing of staff on training received, use of evaluation forms by recipients of training, confirmation of delivery of training according to plan, and review of the contents of training.

i. Relevant money laundering and terrorism financing laws and regulations;
ii. Definitions and examples of laundering and terrorist financing schemes;
iii. How the institution can be used by launderers or terrorists;
iv. The importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;
v. Effective ways of determining whether clients are PEPs and to understand, assess and handle the potential associated risks;
vi. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;
vii. The completion of unusual and suspicious transaction reports;
viii. Treatment of incomplete or declined transactions; and
ix. The procedures to follow when working with law enforcement or the FIU on an investigation.

13.0 PRE-EMPLOYMENT BACKGROUND SCREENING

138. The ability to implement an effective AML/CFT programme depends in part on the quality and integrity of staff. Therefore, licensees should undertake due diligence on prospective staff members. The licensee should ensure that senior management:

1) Verify the applicant's identity;
2) Develop a risk-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual staff member may warrant additional background screening, which should include verification of references, experience, education and professional qualifications;
3) 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
4) Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

APPENDICES

Appendix 1

Coverage of Activities of Financial Institutions

Although the MLFTA applies to all persons and businesses, additional administrative requirements are placed on financial institutions. According to Part I of MLFTA, a financial institution means:

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

i. a trustee within the meaning of the Trusts (Miscellaneous Provisions) Act, 2018 (Act 2018-49);
ii. a person who operates an insurance business within the meaning of the Insurance Act;
iii. a market actor, self-regulatory organisation, participant and issuer of securities within the meaning of the Securities Act;
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); and
x. a private trust company within the meaning of the Private Trust Companies Act, 2012 (Act 2012-22)

(b) foreign sales corporation within the meaning of the Barbados Foreign Sales Corporation Act; and
(c) a society with restricted liability within the meaning of the Societies with Restricted Liability Act;

Appendix 1 Cont'd

The activities of financial institutions are defined in the **First Schedule** of the MLFTA as follows:

1. Acceptance of deposits and other repayable funds from the public, including private banking.
2. Lending, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting.
3. Financial leasing other than with respect to arrangements relating to consumer products.
4. Money or value transmission services.
5. Issuing and managing means of payment, including credit and debit cards, travelers' cheques, money orders and bankers' drafts, and electronic money.
6. Issuing financial guarantees and commitments.
7. Trading in

(a) money market instruments, including cheques, bills, certificates of deposit and derivatives;
(b) foreign exchange;
(c) exchange, interest rate and index instruments; and
(d) transferable securities.

8. Commodity futures trading.
9. Participation in securities issues and the provision of financial services related to such issues.
10. Individual and collective portfolio management.
11. Safekeeping and administration of cash or liquid securities on behalf of other persons.
12. Investing and administering or managing funds or money on behalf of other persons.
13. Underwriting and placement of life insurance and other investment-related insurance, including insurance intermediation by agents and brokers.
14. Money and currency changing.
15. Any other service of a financial nature.

Appendix 2

Additional References

Name of Organisation	Website Address / Link
Basel Committee on Banking Supervision	http://www.bis.org/bcbs/
Caribbean Financial Action Task Force (CFATF)	https://www.cfatf-gafic.org/
Commonwealth Secretariat	http://www.thecommonwealth.org
Egmont Group for Financial Intelligence Units	http://www.egmontgroup.org
Financial Action Task Force (FATF)	http://www.fatf-gafi.org
Financial Stability Board	http://www.fsb.org
International Association of Insurance Supervisors	http://www.iaisweb.org
International Monetary Fund	www.imf.org
International Organisation of Securities Commission	http://www.iosco.org
Interpol	http://www.interpol.int
Organisation of American States – CICAD	http://www.cicad.oas.org
The Financial Crime Enforcement Network (FINCEN)	http://www.fincen.gov/
The World Bank	http://www.worldbank.org
United Nations	http://www.un.org
United Nations – International Money Laundering Information Network	http://www.imolin.org
United Nations – Security Council Resolutions	http://www.un.org/en/sc/documents/resolutions/
United Nations Office on Drugs and Crime	http://unodc.org
US Department of the Treasury (Resource Center/Terrorism and Illicit Finance/Money Laundering	http://www.treasury.gov
Office of The Comptroller of the Currency	https://www.occ.treas.gov
Wolfsberg Group	http://www.wolfsberg-principles.com/index.html
UNSCR Sanctions List for ISIL (Da'esh) & Al-Qaida	https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
UNSCR Sanctions List Materials	https://www.un.org/securitycouncil/sanctions/1718/materials

Appendix 3(a)

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; is of a suspicious or unusual nature; or is conducted by, or relates to, a person against whom a terrorist designation order is in force or relates to the property of such a person; to the FIU Director.	$100,000 on conviction and indictment	Section 23 (2) MLFTA
	Failure of a licensee to maintain business transactions records.	$100,000 on conviction and indictment	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$10,000 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 Programs	Failure by a financial institution to develop policies and procedures; audit functions; and procedures to audit compliance.	Imposition of a pecuniary penalty (up to $5,000 for any of the circumstances referred to at Section 34(1) of the MLFTA; $500 daily for failure to take a measure or action or cease a behaviour or practice) in accordance with Section 36.	Section 19(2) of the MLFTA

Appendix 3(a) Cont'd

Area	Description of Offence / Breach	Description of Fine / Sanction	Section of Legislation
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) of the MLFTA
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 4 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 6(2) MLFTA
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 44 MLFTA

Appendix 3(a) Cont'd

Area	Description of Offence / Breach	Description of Fine / Sanction	Section of Legislation
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 financial services to persons to be used to carry out an offence as defined in the listed treaties[31] 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

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

Appendix 3 (b)

Summary of Administrative Sanctions

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

Verification Examples

A. Personal Clients

- Confirm the date of birth from an official document (e.g. birth certificate).
- Confirm the permanent address (e.g. utility bill, tax assessment, bank statement, letter from a public notary).
- Contact the customer e.g. by telephone, letter, email to confirm information supplied.
- Confirming the validity of the official documents provided through certification by an authorised person.
- Confirm the permanent and/business residence through credit agencies, home visits.
- Obtain personal references from third parties and existing customers in writing.
- Contact issuers of references.
- Confirmation of employment.

B. Corporate Customers & Partnerships

- Review of current audited information (preferably audited).
- Obtain statements of affairs, bank statements, confirmation of net worth from reputable financial advisers.
- Seek confirmation from a reputable service provider(s).
- Confirm that the company is in good standing.
- Undertake enquiries using public and private databases.
- Obtain prior banking and commercial references, in writing.
- Contact issuers of references.
- Onsite visitations.
- Contact the customer e.g. by telephone, letter, email to confirm information supplied.

C. Trusts and Fiduciary Clients

- Seek confirmation from a reputable service provider(s).
- Obtain prior bank references.
- Access public or private databases.

Appendix 5

Approved Persons for Certification of Customer Information

In keeping with Section 7.4.3 on non face-to-face customers, licensees should 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 standards:

- Notary Public
- *Senior Public Servant
- 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
- Any other group of persons prescribed by the Central Bank of Barbados

*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

Appendix 6

Confirmation of Customer Verification of Identity

Part A - Personal Customers

Full Name of Customer: (Mr/Mrs/Ms):
……..……

Known Aliases:……..……

Identification:……..……..

Current Permanent Address:……..…..……

Date of Birth:……. Nationality:……...

Country of Residence:……..……

Specimen Customer Signature Attached: Yes ☐ No ☐

Part B - Corporate & Other Customers

Full Name of Customer:……..…..…..….....

Type of Entity:……...……...……..

Location & Domicile of Business:..……..……

Country of Incorporation:……...……..…

Regulator / Registrar:……..…

Names of Directors:…….....……

……

Names of majority beneficial owners:…….....

Appendix 6 (cont'd)

Confirmation of Customer Verification of Identity

Part C

We confirm that the customer is known to us. Yes ☐ No ☐

We confirm that the identity information is held by us. Yes ☐ No ☐

We confirm that the verification of the information meets

- the requirements of Barbados law and AML/CFT Guideline. Yes ☐ No ☐

We confirm that the applicant is acting on his own behalf and

- not as a nominee, trustee or in a fiduciary capacity for any other person. Yes ☐ No ☐ N/A ☐

Part D

Customer Group Name:……...

Relation with Customer:……...

Part E

Name & Position of Preparing Officer:……...
(Block Letters)

Signature & Date:……...……...……

Name & Position of Authorising Officer:……..……..
(Block Letters)

Signature & Date:……..……..……

Appendix 7

Red Flags

There are a myriad of ways in which money laundering, terrorist financing or the financing of proliferation may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention. Financial institutions are encouraged to refer to such organisations as the FATF, Egmont Group and United Nations Office on Drugs and Crime for typology reports and sanitised cases on money laundering and terrorist financing schemes, respectively. In addition,

General

If the client:

- Does not want correspondence sent to home address.
- Shows uncommon curiosity about internal systems, controls and policies.
- Over justifies or explains the transaction.
- Is involved in activity out-of-keeping for that individual or business.

If the client:

- Produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Provides insufficient, false, or suspicious information, or information that is difficult or expensive to verify.

Economic Purpose

- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer's business.

Appendix 7 Cont'd

Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past.
- Frequent exchanges small bills for large ones.
- Deposits of small amounts of cash on different successive occasions, in such a way that on each occasion the amount is not significant, but combines to total a very large amount. (i.e. "smurfing").
- Consistently making cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Stated occupation is not in keeping with the level or type of activity (e.g. a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Unusually large deposits or withdrawals of cash by an individual or a legal entity whose apparent business activities are normally carried out using cheques and other monetary instruments.
- Multiple and frequent purchase or sale of foreign currency by a tourist.
- Multiple and frequent large withdrawals from an ATM using a local debit card issued by another financial institution.
- Multiple and frequent large withdrawals from an ATM using debit or credit card issued by a foreign financial institution.

Deposit Activity

- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Multiple transactions are carried out on the same day at the same branch but with an

Appendix 7 Cont'd

apparent attempt to use different tellers.

- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly exhibits significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

Cross-border Transactions

- Deposits followed within a short time by wire transfers to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
- Immediate conversions of funds transfers into monetary instruments in the name of third parties.
- Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family-run banks, shell banks or unknown banks.
- Large incoming or outgoing transfers, with instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account

Appendix 7 Cont'd

relationship with the institution.

- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities having no apparent business connection with client.

Personal Transactions

- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Increased use of safety deposit boxes. Increased activity by the person holding the boxes. The depositing and withdrawal of sealed packages.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

Corporate and Business Transactions

- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Unexplained transactions are repeated between personal and business accounts.

Appendix 7 Cont'd

- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

Lending

- Customer suddenly repays a problem loan unexpectedly, without indication of the origin of the funds.
- Loans guaranteed by third parties with no apparent relation to the customer.
- Loans backed by assets, for which the source is unknown or the value has no relation to the situation of the customer.
- Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.
- Use of standby letters of credit to guarantee loans granted by foreign financial institutions, without any apparent economic justification.

Securities Dealers

- Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.

Accounts Under Investigation

- Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in a court or other competent

Appendix 7 Cont'd

national or foreign authority in connection with fraud, terrorist financing or money laundering.

- Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority with fraud, terrorist financing or money laundering.

Fiduciary Business

- Client seeks to invest a large sum of money with no apparent interest in the details of the product (e.g. mutual fund) and does not enquire about the characteristics of the product and /or feigns market ignorance.
- Corporate client opens account with large sum of money that is not in keeping with the operations of the company, which may itself have recently been formed.
- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.

Employees

- Lifestyle, financial status or investment activity is not in keeping with employee's known income.
- Reluctance to go on vacation, to change job position or to accept a promotion, with no clear and reasonable explanation.
- Employee frequently receives gifts &/or invitations from certain clients, with no clear or reasonable justification.
- Employee hinders colleagues from dealing with specific client(s), with no apparent justification.
- Employee documents or partially supports the information or transactions of a particular client, with no clear and reasonable justification.

Appendix 7 Cont'd

- Employee frequently negotiates exceptions for a particular client(s).

MVTS Business

- Customer is unaware of details surrounding incoming wire transfers, such as the ordering customer details, amounts or reasons.
- Customer does not appear to know the sender of the wire transfer from whom the wire transfer was received, or the recipient to whom they are sending the wire transfer.
- Customer frequents multiple locations to send wire transfers overseas.
- The customer sends wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond with the expected activity of the customer.
- Customer is accompanied by individuals who appear to be sending or receiving wire transfers on their behalf.
- Customer utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.
- Multiple customers have sent wire transfers over a short period of time to the same recipient.
- Large and/or frequent wire transfers between senders and receivers with no apparent relationship.
- Customer sending to, or receiving wire transfers from, multiple customers.

VASPs Business

- 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.
- Transferring virtual assets immediately to multiple virtual asset service providers, including those registered or operated in other countries.

- 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 regulations for virtual asset entities, including inadequate Customer Due Diligence or Know-Your-Customer measures.
- 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.
- Abnormal transaction activity of virtual assets from peer-to-peer platform associated wallets with no logical business explanation.

Appendix 8

Declaration Source of Funds/Wealth

Customer Name or Business:……..

Current Address:……..…..

Account Number:……..

Identification:……..…….....

Amount of Transaction & Currency:

Description/Nature of Business Transaction:

☐ Deposit ☐ Monetary Instrument ☐ Currency Exchange ☐ Wire Transfer ☐ Credit/Debit Card

☐ ATM ☐ Loan ☐ Investment ☐ Trust Settlement / Distribution Other ☐ (Specify)

Source of Funds / Wealth:

…..……..……..…..…

……..…

…..……..……

Supporting Evidence:……..

Customer Signature:……..

Date:……

Transaction Approved? Yes ☐ No ☐

If No, state reason:……...

……..…

……. ……....

OFFICER COMPLETING TRANSACTION (Signature & Title)

AUTHORISING OFFICER (Signature & Title)