Compliance Unit
Anti-Money Laundering Authority

Anti-Money Laundering/Combating the Financing of Terrorism/Countering Proliferation Financing Guideline

for

ACCOUNTANTS

October 2021

Table of Contents

Terms Used

AMLA	Anti-Money Laundering Authority
AML/CFT/CPF	Anti-Money Laundering/Counter Financing of Terrorism/ Countering Proliferation Financing
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Business Professionals
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
MLFTA	Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach

1.0 Introduction

1.1 Background

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. Experience and careful study have taught that the threats of money laundering and the financing of terrorism extend beyond the traditional financial entities which have been receiving attention for control of these activities. It is, therefore, necessary for certain Designated Non-Financial Businesses and Professions (DNFBPs) to be regulated so as to keep them safe from these nefarious activities, and to protect the legitimate financial system from illegitimately acquired funds that could find their way into the financial system via these non-financial entities.

3. The Compliance Unit (Unit) of the Anti-Money Laundering Authority was created by legislative amendment of the Money Laundering and Financing of Terrorism (Prevention & Control) Amendment No. 2 Act 2019-58 (MLFTA). The entities in the Second Schedule of the MLFTA as DNFBPs for the purpose of our anti-money laundering and counter financing of terrorism infrastructure as set out in the Second Schedule of the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA) include:

"An independent accountant engaged in any of the following:

a) the purchase, sale or other disposal of real property;
b) the management of the money, securities or other assets of a customer;
c) the management of bank savings or securities accounts;
d) the organization of contributions for the creation, operation or management of bodies corporate;
e) the creation, operation or management of legal persons or arrangements; or
f) the purchase or sale of business entities.

4. Effective use and enforcement of policies that are directed at deterring money laundering and the financing of terrorism gives authenticity and integrity to those areas in which they are applied. This is beneficial to those particular sectors as well as the entire financial sector.

5. The MLFTA empowers the Anti-Money Laundering Authority (AMLA), pursuant to Section 26, to issue guidelines with respect to these activities. This Guideline is so issued for the guidance of persons and entities operating as accountants in Barbados, when engaged as set out above. The definitions appearing in the MLFTA apply mutatis mutandis to the Guideline.

6. The essential ingredient in an effective anti-money laundering system is an efficient know your customer due diligence system. Everything in this Guideline is founded on this understanding and is aimed at equipping accountants to apply such measures in their business affairs.

1.2 Purpose of Guideline

7. The purpose of the Guideline is to provide guidance to all Accountants on how they can fulfil their obligations in relation to the MLFTA and in doing so comply with the anti-money laundering and financing of terrorism and proliferation requirements of the Recommendations of the Financial Action Task Force (FATF). The Guideline should be read in conjunction with the MLFTA.

8. This Guideline, which is being issued by the Anti-Money Laundering Authority ("Authority") pursuant to its powers under Section 26 of MLFTA, replaces any previously issued Guideline of the Authority and is updated to reflect the changes in the MLFTA and updated guidance of the FATF.

9. Administrative sanctions for non-compliance with the guideline are found at section 34 of the MLFTA Act as the relate to DNFBPS as defined in the Second Schedule of the MLFTA.

2.0 Application

10. This Guideline applies to all persons and entities operating as accountants, whether as business owners or as sole practitioners, when they are performing the functions set out above. It is expected to be followed by principals and their agents.

11. The legal requirements apply to an independent accountant as they do to a firm, partnership or corporate arrangement. Therefore, "accountant" means a sole practitioner, partner, or employed professional within a professional firm. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

12. Some accountants may be able to conclude that based on the services they provide, they do not have any specific AML/CFT/CPF obligations as they do not prepare for, or carry out any of the functions set out above. However even though specific AML/CFT/CPF obligations may not apply to an accountant, it is consistent with the overall ethics and best practices of the profession for all accountants to ensure that their services are not being misused, including by criminals. Accordingly, accountants should carefully consider what they need to do to guard against that risk, in order not to be unwittingly involved in ML/TF.

13. This Guideline shall be considered in the context of applicable professional privilege and professional secrecy rules. Privilege/professional secrecy is a protection to the client, and a duty of accountant to protect client information or advice from being disclosed. In situations where accountants are claiming professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules.

3.0 Money Laundering and Financing of Terrorism and Proliferation

3.1 Money Laundering

14. 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

15. 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 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.

16. It is worth emphasizing that while money laundering is concerned with funds generated from unlawful sources, funds used for terrorist activities are often legitimate in nature. The source of funds is, therefore, not the sole consideration for agents. The conversion of assets into money and the subsequent direction of that money must be observed.

17. As information changes, the United Nations publish lists of terrorist or terrorist organizations. Financial institutions and designated non-financial businesses and professionals are required to remain abreast of this information and check their databases against these lists. Should any person or entity on the lists be clients, that information should be immediately communicated to the FIU and the Commissioner of Police.

18. The FATF Recommendations place obligations on countries as they relate to terrorist financing in the context of national cooperation and coordination, confiscation and provisional measures and targeted financial sanctions related to terrorism and terrorist financing. The latter is applicable to all United Nations Security Council resolutions (UNSCRs) applying targeted financial sanctions relating to the financing of terrorism. The AMLA'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

19. The FATF defines proliferation financing as "*the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*[1]". Proliferation of weapons of mass destruction can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles). The AMLA's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation. See the detailed Guidelines on TF and PF Financial Sanctions obligations.[2]

[1] http://www.fatfgafi.org/topics/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

[2] Refer to Guidelines on Targeted Financial Sanctions for FIs and DNFBPs.

4.0 International Initiatives

20. 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 (Mutual Legal Assistance and other forms of International Cooperation); October 2015 (Interpretative Note on Foreign Terrorist Fighters); June 2016 (Note on Non-profit Organizations); October 2016 (Interpretative Note on Terrorist Financing Offence); June 2017 (Interpretive Note on Targeted Financial Sanctions related to proliferation); November 2017 (on Tipping-off and Confidentiality and Interpretive Note on internal controls and foreign branches and subsidiaries); February 2018 (on National Cooperation and Coordination); and October 2018 (on New Technologies) and October 2020 (on Proliferation Financing). The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. Accountants should keep abreast of developments in the international standard and refine their programmes accordingly.

5.0 Legislative and Regulatory Framework

21. 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. The Acts and Guideline which are most relevant for the purposes of this Guideline are as follows:

- Drug Abuse (Prevention and Control) Act, 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, Cap158;
- Anti-Terrorism (Amendment) Act, 2015 and 2019;
- 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

22. Section 4 of the MLTFA provides that it applies to the DNFBPs set out in the Second Schedule as it does to financial institutions. Section 3 of the Second Schedule includes independent accountants engaged in specified activities. This means that the legislative infrastructure which applies to the traditional financial institutions, also applies to the DNFBPs.

23. 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 to the AMLA, which was established in August 2000. The Financial Intelligence Unit is centralised, independent, authority, which receives and analyses information from the financial sector and DNFBP sectors and makes disclosures to law enforcement authorities.

24. As the operational arm of the AMLA, the FIU's responsibilities, inter alia, include:

(i) Receiving suspicious or unusual transactions reports from financial institutions;
(ii) Investigating suspicious or unusual transactions reports;
(iii) Instructing supervised entities to take steps that would facilitate an investigation; and
(iv) Providing training in respect of record keeping obligations and reporting obligations under the MLFTA.

25. Where an accountant is uncertain about how to treat an unusual or suspicious transaction, he/she is strongly urged to speak directly to the FIU for preliminary guidance and then make a report as appropriate.

6.0 Gatekeepers

26. Gate keepers are businesses or professionals that are able to provide access into the financial system, including accountants. They have the ability to allow illicit funds into the financial system, whether knowingly or not. This informs why it is necessary to regulate their activities for anti-money laundering purposes, although they are not financial institutions.

6.1 The Role of the Accountant

27. Accounting professionals serve as gatekeepers since they have the ability to furnish access (knowingly or unknowingly) to the financial system through the various functions they perform that might help the criminal with funds to move or conceal them.

28. Professional expertise that accountants provide may be important to a money laundering enterprise. For example, accounting expertise is needed to set up complex illicit transactions, and to unravel them, especially where organized crime is involved.

29. Accountants must see anti-money laundering policies and procedures as part of their operational practice. The consequences of participation in money laundering activity, or failing to prevent one's practice from being used in furtherance of this activity, are severe. Practitioners should refer to the penalties provisions of the MLFTA or Appendix 1 of this Guideline.

30. Often, fraud and money laundering are carried out by people who know more about the accounting systems and other practices than many auditors or police investigators. Under Barbados' MLFTA, accountants are brought under the umbrella of the anti-money laundering infrastructure in the same way as other DNFBPs. Accountants like other DNFBPs, must therefore apply the provisions of the MLFTA in the same way as financial institutions. As is the case with attorneys, accountants must keep client records, conduct know your client due diligence and make suspicious transaction reports to the FIU when there is a need to do so.

31. It is worth emphasizing that the anti-money laundering responsibilities of an accountant arise only in the circumstances set out in the legislation and not to the general practice of all aspects of legal practice.

32. Even though individual accountants and accounting firms may be able to conclude that specific AML/CFT/CPF obligations do not apply to them, ethical standards require them to ensure that their services are not being misused, including by criminals, and they should carefully consider what they need to do to guard against that risk.

7.0 Risk-based Approach

33. The MLFTA provides for the application of a risk-based approach to combating money laundering and the financing of terrorism and proliferation. The RBA to AML/CFT/CPF means that countries, competent authorities and DNFBPs including accountants, should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT/CPF measures effectively and efficiently, to mitigate and manage the risks.

34. Key elements of a RBA can be summarised as follows:

(i) **Risk Identification and Assessment** - *identifying ML/TF risks facing a firm, given its customers, services, countries of operation, also having regard to publicly*

available information regarding ML/TF risks and typologies

*(ii)***Risk Management and Mitigation** - *identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks*

(iii) **Ongoing Monitoring** - *putting in place policies, procedures and information systems to monitor changes to ML/TF risks*

(iv) **Documentation** - *documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks*

35. The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT/CPF controls should apply.

36. Implementing a RBA requires that accountants have a sound understanding of the ML/TF risks and are able to exercise good professional judgement. Above all, accountants and the leadership of accounting firms should recognise the importance of a culture of compliance across the organization and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organization. This requires the 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on ML/TF risks, both at the country and institutional levels, and to develop procedures and systems.

37. In this regard, accountants are encouraged to pay close attention to their practice and apply defensive measures that are in proportion to the risk faced at any particular time. In the interest of clarity, accountants should deploy defensive resources only where there is a threat of money laundering or financing of terrorism and proliferation. Further, the extent of that deployment should be a function of the extent of the risk faced.

38. As general guidance, the following considerations should be at the base of all due diligence actions:

39. Accountants are required to regularly review their AML/CFT/CPF systems and test them for effectiveness. Records should be reviewed to ensure that all existing customer records are current and valid. Wherever beneficial ownership information is required, it must be borne in mind that the true beneficial owner is the ultimate beneficial owner. The ultimate beneficial owner is the natural person who controls or benefits from the assets of the business.

40. For accountants identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions where they operate, and the effectiveness of their controls in place, will require the investment of resources and training.

7.1 Risk Identification and Assessment

41. Potential ML/TF risks faced by accountants will vary according to many factors including the activities undertaken by them, the type and identity of the client, and the nature and origin of the client relationship. When applying the RBA, accountants and accounting firms should bear in mind that specified activities have been found to be more susceptible to ML/TF activities because they involve the movement or management of client assets; this susceptibility may be heightened when these activities are conducted on a cross-border basis. These specified activities are set out in Schedule 2 of the MLFTA.

42. Accountants should perform a risk assessment of clients at the inception of a client relationship. Such risk assessment may well be informed by findings of the NRA and any other information which may be relevant to assess the risk level particular to their accounting practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Accountants may also refer to FATF Guidance on indicators and risk factors[3]. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important.

7.2 Categories of Risk

43. Accountants may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling accountants, where required, to subject each client to reasonable and proportionate risk assessment.

44. The most commonly-used risk categories are:

a) country or geographic risk;
b) client risk; and
c) risk associated with the particular service offered (Transaction Risk).

45. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the accountant and/or accounting firm. These criteria, however, should be

[3] Refer to FATF Guidance for a Risk-Based Approach for the Accounting Profession

considered holistically and not in isolation. Accountants, based on their individual experiences and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

7.2.1 Country or Geographic Risk

46. Barbados promotes itself as an important financial centre for business persons from many diverse parts of the world. Our wide spread of double taxation treaties is ample evidence of this. Further, real estate in Barbados is an attractive asset for persons. It is to be expected, therefore, that the services of accountants will be in high demand as many millions of dollars pass through this sector every year.

47. Jurisdictions with certain characteristics pose risks. Jurisdictions with AML/CFT/CPF regimes that fall below acceptable standards may be regarded as high risk. Jurisdictions which support terrorist activities or are known for significant political corruption are also high risk.

48. There is no universally agreed definition by competent authorities that prescribes whether a particular country or geographic area (including the country within which the accountant practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information on ML/TF risks. Geographic risks of ML/TF may arise in a variety of circumstances, including from the domicile of the client, the location of the transaction or the source of wealth or the funds.

49. Accountants 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 business from such countries. Accountants should observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, from listed countries and to observe the list of countries published by any competent authority which lists countries that are non-compliant or do not sufficiently comply with FATF recommendations[4].

50. Accountants should therefore have regard to where a transaction or request for their services originated, but also whether a high-risk jurisdiction is an intermediate stage in the financing or ownership arrangement.

51. In addition, an accountant may be required to apply countermeasures, which are effective and proportionate, to the risks identified from listed countries, either when called upon to do so by the

[4] Refer to FATF Guidance on High Risk and Non-Cooperative Jurisdictions

FATF and CFATF or independently of any call to do so. Such countermeasures that the Competent Authority may impose include:

1) Requiring DNFBPs to apply specific elements of enhanced due diligence;
2) Prohibiting DNFBPs from establishing subsidiaries, branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant subsidiary, branch or representative office would be in a country that does not have adequate AML/CFT/CPF systems;
3) Limiting business relationships or financial transactions with the identified country or persons in that country;
4) Prohibiting DNFBPs 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 businesses or professions 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.

7.2.2 Client Risk

52. Determining the potential ML/TF risks posed by a client or category of clients is critical to the development and implementation of an overall risk-based framework. Based on their own criteria, accounting firms and accountants should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment.

53. There are several issues that may point to a high risk client, including:

- Industries or sectors where opportunities for ML/TF are particularly prevalent.
- The structure or nature of the entity or relationship makes it difficult to identify the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions.
- PEPs and/or their family members and close associates.
- Companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- Cash intensive businesses including money transfer services, casinos and other gaming institutions, dealers in precious metals and non-profit or charitable organizations, where such clients are themselves subject to and regulated for a full range of AML/CFT/CPF

requirements consistent with the FATF Recommendations, this will aid to mitigate the risks.

- Reluctance to provide relevant information or the accountant having reasonable grounds to suspect that the information provided is incorrect or insufficient.

7.2.3 Transaction Risk

54. An overall risk assessment of clients should also include determining the potential risks presented by the services being offered by accountants, who provide a broad and diverse range of services. The context of the services being offered or delivered is fundamental to a RBA. When determining the risks associated with the provision of services related to specified activities, consideration and appropriate weight should be given to transaction risks including:

- Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- Transactions that are capable of concealing beneficial ownership from competent authorities.
- Transactions where it is readily apparent to the accountant that there is inadequate consideration, where the client does not provide legitimate reasons for the transaction.
- Large cash transactions. While rules and regulations governing the financial sector are designed to detect situations where large amounts of cash are being introduced, accountants should keep this factor in mind when evaluating whether a transaction seems suspicious.
- Immediate resale of property. Especially if the sale entails a significant increase or decrease in the price compared to the prior purchase price, without a reasonable explanation.
- Non-cash transactions through the use of inter-company transfers within a group to disguise the audit trail.
- Any other activities which demonstrate suspicious behavior and do not make professional or commercial sense based on the norms in the industry and the normal course of business.

7.3 Mitigating Risk

55. Accountants should implement appropriate measures and controls to mitigate the potential ML/TF risks for those clients that, as the result of a RBA, are determined to be higher risk. These measures should be tailored to the specific risks faced, both to ensure the risk is adequately addressed. Paramount among these measures is the requirement for Accountants and appropriate staff to be adequately trained to identify and detect relevant changes in client activity by reference to risk-based criteria.

56. The presence of a single risk factor, or even multiple factors, does not necessarily mean that the client is engaging in money laundering or financing terrorism and proliferation activities. Accountants should be familiar with these risk factors, and exercise sound judgment based on their knowledge of the relevant industry, and when a combination of these factors truly raises a red flag, know the proper action to take.

57. In light of this, it is crucial that accountants develop a sound risk management policy that they will follow in all transactions. This policy should document what customer information is required to facilitate a transaction. It should also set out in what circumstances business would be declined.

8.0 Know Your Client/Customer Due Diligence (CDD)

58. CDD measures should allow accountants to establish with reasonable certainty the true identity of each client. Due diligence procedures should apply in circumstances where accountants are preparing for or carrying out the activities listed in the Second Schedule of the MLTFA.

59. CDD is a critical component of the role all accountants can play in helping to identify and combat money laundering and terrorist and proliferation financing. Knowing one's client does not mean knowing the client's name and address. This can only be satisfied by understanding the client's business and his/her desired relationship with the accountant's professional service.

60. Accountants are required to apply each of the following CDD measures:

(i) identification and verification of the client's identity;
(ii) identification of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner;
(iii) understanding the purpose and nature of the business relationship; and
(iv) on-going due diligence on the relationship

61. In effecting the due diligence process, accountants should:

(i) Whenever possible, require prospective clients to be interviewed in person.
(ii) In verifying client identity, use independent official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to 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. Client 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 establish a relationship. Examples of documentation for different types of clients are set out in Appendix 4.

62. Generally, funds should not be accepted from prospective clients unless the necessary verification has been completed. However, in exceptional circumstances, verification may be completed after establishment of the business relationship. A reasonable timeline for completing the verification process should be established. If after verification efforts there is still discomfort, a report should be made to the FIU. "Funds", in this regard, does not refer to an initial consultation fee.

63. In cases where red flags are present, the agent should apply increased levels of CDD, which could include the following:

1) Obtain additional information, a driver's license, passport or other reliable identification document, to confirm the true identity of the client.
2) If a legal entity is involved, such as a corporation, take additional measures to identify who actually controls or owns the entity and take risk based measures to verify the identity of the owner. This is commonly referred to as beneficial ownership information.
3) Obtain other appropriate information based on experience and knowledge to understand the client's circumstances and business.

64. In addition, depending on the size of the firm, it may be appropriate to notify and discuss with senior management the higher risk client or a particular situation that raises red flags, and to monitor the relationship if there are a series of transactions with the client.

8.1 Personal Clients

65. Accountants should obtain relevant information on the identity of their personal clients and seek to verify the relevant information on a risk basis, through the use of reliable, independent source documents, data or information to prove to their 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 business; and
g. Signature.

66. Accountants 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). 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.

8.2 Unavailability of Identity Documents

67. There may be circumstances where some clients are unable to supply the identity documents. Such clients include the elderly, a minor, the disabled and individuals dependent on the care of others. Accountants 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.

8.3 Corporate Clients

68. To satisfy itself as to the identity of the client, accountants should obtain:

a. Name of corporate entity;

b. Principal place of business and registered office;
c. Mailing address;
d. Contact telephone and fax numbers;
e. Identity information on the beneficial owners of the entity. This information should extend to identifying those who ultimately own and control the company and should include anyone who is giving instructions to the agent to act on behalf of the company. However,
    i. If the company is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required;
    ii. If the company is a private, identity should be sought on persons with a minimum of 20% shareholding.
f. Identity information on directors and officers who exercise effective control over the business and are in a position to override internal procedures / control mechanisms;
g. Description and nature of business;
h. Certified copy of the certificate of incorporation, organization, 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;
i. By-laws and any other relevant documents, and any amendments thereto, filed with the Registrar of Corporate Affairs and Intellectual Property, the Financial Services Commission or the Registrar of Friendly Societies, as the case may be;
j. Board resolution authorizing the business activity and conferring authority on signatories to the transaction, where appropriate; and
k. Recent financial information or audited statements, depending on the nature of the transaction.

69. In addition, accountants may obtain any other information deemed appropriate. For example, one 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. One 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.

8.4 Partnership/Unincorporated Business

70. Partnerships and unincorporated businesses should meet the relevant requirements set out in Section 8.1. Each partner as well as immediate family members with ownership control should be identified. Ownership control exists where a partner or an investor in the business enterprise, or an immediate family member (spouse, child, parent, sibling) has at least ten percent interest in the business, or the power to control the direction of the business. In addition to providing the identification documentation for partners/controllers and authorized signatories, where a formal partnership arrangement exists, the accountant may obtain a mandate from the partnership authorizing the business to be undertaken.

8.5 Trusts

71. Trust business is usually regarded as inherently risky because of the confidentiality associated with these entities. To satisfy itself as to the identity of the client, the accountant should obtain:

a. Name of trust;
b. Nature / type of trust;
c. Country of establishment;
d. Identity of the trustee(s), settlor(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;
e. Identity of person(s) with powers to add beneficiaries, where applicable;
f. Identity of the person providing the funds, if not the ultimate settler;
g. Verify beneficiaries before the first distribution of assets;
h. Verify protectors/controllers at 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;
i. 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.
j. Verify the identity of the trust by obtaining a copy of the creating instrument and other amending or supplementing instruments.

8.6 Professional Service Providers

72. Professional service providers act as intermediaries between clients and the professionals providing services to those clients. 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, accountants should:

(i) Adequately assess any risk and monitor the relationship for suspicious or unusual activity;
(ii) Understand the intended business, including the anticipated transaction volume, 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.

8.7 Politically Exposed Persons (PEPs)

73. Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which accountants who deal with them may face, have led to calls for enhanced due diligence on such persons. The Financial Action Task Force (FATF) categorizes PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organization[5]. These categories of PEPS are defined as follows:

- Foreign PEPs: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- Domestic PEPs: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- International organization PEPs: persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.
- 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.

[5] Refer to FATF Guidance on Politically Exposed Persons

74. Accountants should, in relation to foreign PEPs (whether as a client/customer or beneficial owner), in addition to performing normal due diligence measures:

a. Have appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;
b. Take reasonable measures to establish the source of wealth and source of funds; and
c. Conduct enhanced ongoing monitoring of the business relationship.

75. 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 due diligence measures, accountants should:

a. Take reasonable measures to determine whether a client 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) and (c) above.

76. 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.

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

8.8 Reduced Client/Customer Due Diligence

78. Accountants may apply reduced due diligence to a client provided they are satisfied that the client is of such a risk level that qualifies for this treatment. Such circumstances are set out below:

Where an indication to conduct business is made by:

a. An entity licensed under the International Financial Services Act or the Financial Institutions Act;
b. An entity registered under the Securities Act or the Mutual Funds Act;
c. An entity licensed under the Insurance Act or Exempt Insurance Act;
d. An entity licensed under the Cooperatives Society Act, Friendly Societies Act or Building Societies Act;
e. The Government of Barbados; or
f. A statutory body.

79. Where, owing to the perceived risk, reduced due diligence is applied in any circumstance other than those set out in this section, Accountants must first consider and approve this decision. Evidence of this process must be recorded and stored for the statutory period required after the end of the business relationship.

9.0 Record-Keeping

80. To demonstrate compliance with the MLFTA and to allow for timely access to records by the FIU, accountants 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. Business transaction records should be maintained for a minimum of five years in accordance with section 18 of the MLFTA. However, it may be necessary to retain records, until such time as advised by the FIU or High Court, for a period exceeding the statutory period, beginning from the date of termination of the last business transaction, where:

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

81. 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.

9.1 Internal and External Records

82. Accountants 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 Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and
vi. Reports to the Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.

9.2 Training Records

83. Accountants are required to provide training and awareness programmes and to maintain an on- going training programme for themselves and all persons working in their businesses. In order to provide evidence of compliance with Section 21 of the MLFTA, at a minimum, the following information must be maintained:

a. Details and contents of the training programme attended by practitioners and staff;
b. Names of staff receiving the training;
c. Dates that training sessions were attended or held; and
d. Results of any testing included in the training programmes;
e. An on-going training plan.

10.0 Compliance and Audit Function

84. Accountants must establish procedures for ensuring compliance with legal requirements as set out in relevant legislation and this Guideline to demonstrate that they are able to identify suspicious activity.

85. A sole practitioner has the responsibility of personally carrying out all required due diligence activities, unless this function is contracted out. However, the practitioner remains responsible for the compliance function.

86. With respect to an accounting firm, a compliance officer at the level of management must be appointed. This is to ensure that this officer has access to all relevant internal information without having to seek clearance in each case. Where the compliance function is contracted out, the firm remains responsible for the function.

87. An independent review should be carried out to evaluate how effectively compliance policies are being implemented. Such reviews should be carried out on a frequency consistent with the size and risk profile of the practice/business. The review process should identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions.

88. It is recognised that the appointment of a Compliance Officer or the creation of an internal audit department may create difficulties for some small entity, where this is not possible an accountant may subject to the Compliance Unit's agreement, contract out the compliance or

internal audit function to a person or firm that is not involved in the auditing or accounting functions of the accountant's practice/business.

89. Where the compliance and/or audit function is contracted out, the entity remains responsible for the function and shall be in a position to readily respond to the Compliance Unit and the FIU on AML/CFT/CPF issues.

10.1 Internal Reporting Procedures

90. To facilitate the detection of suspicious transactions, accountants should:

(i) Require clients to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount as the practitioner determines, to reasonably ascertain that funds are not the proceeds of criminal activity. Appendix 6 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 client;
(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, at management level, 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
(iv) Require staff to document in writing their suspicion about a transaction;
(v) Require documentation of internal enquiries; and
(vi) Keep a record of all reports made to authorities and responses to enquiries made for the statutory period.

91. Persons operating as sole practitioners are expected to apply these steps to the extent that they are relevant.

10.2 External Reporting - Reporting Suspicious Activity

92. Accountants are required by law to report forthwith to the FIU where the identity of the person involved, the transaction or any other circumstance concerning that transaction lead the practitioner to have reasonable grounds to suspect that a transaction:

(i) Involves proceeds of crime to which the MLFTA applies;
(ii) Involves the financing of terrorism;
(iii) Involves the financing of proliferation; or
(iv) Is of a suspicious or an unusual nature.

93. Accountants are advised to monitor suspicious activity, but there is an obligation to report activity that satisfies the threshold for inconsistency with normal behaviour. After a reasonable time, a transaction, or series of transactions, should be cleared of suspicion, and if this cannot be done with a clear conscience, a report should be made to the FIU.

94. A Suspicious Transaction Report form should be completed and submitted to the FIU for analysis. Once reported, nothing should be done to indicate to any person that such a report was made. There are legal consequences for tipping off a person that an investigation is about to commence or has commenced or that a report was made to the FIU. Bear in mind that tipping off may be inadvertent and could take place through the loose handling of information.

95. An accountant, their employees or 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 FIU, 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.

96. It is against the law for partners, employees, or agents of a DNFBP to disclose that a suspicious transaction report or related information on a specific transaction has been reported, is in the process of being reported, or is about to be reported, to the FIU.

Appendices

Summary of Money Laundering and Terrorism Sanctions and Offences

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
Reporting Obligations	Failure to make a report on a transaction involving proceeds of crime, the financing of terrorism or is of a suspicious or unusual nature to the FIU Director.	$100,000 on directors jointly and severally and /or 5 years imprisonment	Section 23 (2) MLFTA
	Failure to maintain business transactions records.	$100,000 on directors jointly and severally	Section 18(4) MLFTA
	Failure of a person to report transfers out of Barbados or transfers Barbadian currency or foreign currency into Barbados, of more than BDS$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 to develop policies and procedures; audit functions; and procedures to audit compliance.	Imposition of a pecuniary penalty (up to $5,000 for any of the circumstances referred to at section 34(1) of the MLFTA; $500 daily for failure to take a measure or action or cease a behaviour or practice) in accordance with section 36.	Section 19(2) of the MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
Information Gathering & Investigations	Failure to comply with any instruction issued or request made by the FIU Director.	The licence of the financial institution may be suspended.	Section 30(5) of the MLFTA.
Onsite Inspections	Failure to comply with an instruction or request made by an authorised officer or Regulatory Authority.	The licence of the financial institution may be suspended.	Section 31(4) of the MLFTA
Interference in the Line of Duty	The obstruction, hindrance, molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	$50,000 or imprisonment of 2 years or both.	Section 42 MLFTA
Directives	Contravention of the Act but circumstances do not justify taking action under sections 34, 35 or 36 of the MLFTA.	Issuance of directives by the Anti-Money Laundering Authority or Regulatory Authority to cease and desist.	Section 33 of the MLFTA.
Money Laundering Offences	Engagement in money laundering.	Summary conviction - $200,000 or 5 years imprisonment or both. Conviction on indictment - $2,000,000 or 25 years imprisonment or both. Forfeiture of licence for financial institution.	Section 6 (1) MLFTA Sections 35 & 46(1)
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 4 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 6(2) MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 44 MLFTA
Disclosure of Information	Disclosure of information on a pending money laundering investigation. Falsifying, concealing, destruction or disposal of information material to investigation or order.	$50,000 or 2 years imprisonment or both	Section 43(b) MLFTA
	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[6] 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

[6] 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.

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.

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 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 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.

- 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 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.
- 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.

Virtual Assets (VA)

- Configure VA transactions for small amounts or amounts below record keeping or reporting thresholds.
- Making multiple high-value transactions
- Depositing VAs to an exchange and then often immediately
- Accepting funds suspected of being stolen or fraudulent

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.

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:……...

……

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 lawand AML/CFT/CPF Guideline. **Yes □ No □**

We confirm that the applicant is acting on his own behalf and - not as a nominee, trustee or in afiduciary 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:…….

Approved Persons For Certification of Customer Information

In keeping with Section 7.4.3 on non-face-to-face customers, entities 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/CPF standards:

- Notary Public
- *Senior Public Servant
- Member of the Judiciary
- Magistrate
- Accountant 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 group of persons prescribed by the Compliance Unit

*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

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*)