Compliance Unit
Anti-Money Laundering Authority

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

for

DEALERS IN PRECIOUS METALS AND STONES

OCTOBER 2021

Table of Contents

Terms of Use iii

1.0 INTRODUCTION 1

1.1 Background 1

1.2 Purpose of Guideline 2

2.0 APPLICATION 2

3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM AND PROLIFERATION 3

3.1 Money Laundering 3

3.2 Financing of Terrorism 3

3.3 Financing of Proliferation 4

4.0 INTERNATIONAL INITIATIVES 4

5.0 LEGISLATIVE AND REGULATORY FRAMEWORK 5

6.0 THE ROLE OF THE DEALER IN PRECIOUS METALS AND STONES 6

6.1 When is a Dealer a Dealer? 6

6.2 Threshold 7

6.3 Inclusion and Exclusion 7

6.3.1 Meaning of Manufacturing Jewellery 8

7.0 RISK-BASED APPROACH 8

7.1 Types of Risk 10

7.1.1 Country or Geographic Risk 10

7.1.2 Customer Risk and Counterparty Risk 13

7.1.3 Retail Customer Risk 13

7.1.4 Business Counterparty Risk 13

7.2 Mitigating Risk 14

8.0 KNOW YOUR CLIENT/CUSTOMER DUE DILIGENCE (CDD) 15

8.1 Politically Exposed Persons (PEPs) 17

9.0 RECORD-KEEPING 18

9.1 Training Records 18

10.0 TRAINING AND AWARENESS 19

10.1 Content and Scope of the Training Programme 20

11.0 COMPLIANCE AND AUDIT FUNCTION 20

11.1 Internal Reporting Procedures 21

11.2 External Reporting - Reporting Suspicious Activity 22

APPENDICES 23

Summary of Money Laundering and Terrorism Sanctions and Offences 24

Red Flags 27

Verification Examples 33

Confirmation of Customer Verification of Identity 34

Approved Persons For Certification of Customer Information 36

Declaration Source of Funds/Wealth 37

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:

> "A dealer in precious metals or precious stones engaged in financial transactions equal to or above the value set out in guidelines of the Authority."

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 dealers in precious metals and stones in Barbados.

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 dealers in precious metals and stones 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 dealers in precious metals and stones 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 directly to all precious metals and precious stones businesses in Barbados. There may be operators of such businesses in Barbados that are subsidiaries of foreign-owned parent companies. Precious metals and stones businesses are expected to ensure that they and their subsidiaries in Barbados have effective controls in place to comply with this Guideline. Where Barbadian businesses have branches or subsidiaries overseas, steps should be taken to alert the management of such overseas branches to the requirements in Barbados in relation to anti-money laundering and counter terrorist financing.

11. Where a local jurisdiction has domestic money laundering legislation, branches and subsidiaries of Barbados businesses operating within that jurisdiction should, as a minimum, act in accordance with the requirements of the local legislation. Where the local legislation and the Guideline are in conflict, the foreign branch or subsidiary should comply with the local legislation and inform the Barbados office immediately of any departure from this Guideline.

3.0 Money Laundering and Financing of Terrorism and Proliferation

3.1 Money Laundering

12. 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

13. 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.

14. 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.

15. 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.

16. 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

17. 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]

4.0 International Initiatives

18. 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). The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. Dealers in Precious Metals and Stones should

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

[2] 3 Refer to Guidelines on Targeted Financial Sanctions for FIs and DNFBPs.

keep abreast of developments in the international standard and refine their programmes accordingly.

5.0 Legislative and Regulatory Framework

19. 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, 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.

20. Section 4 of the MLTFA provides that it applies to the DNFBPs set out in the Second Schedule as it does to financial institutions. This means that the legislative infrastructure which applies to the traditional financial institutions, also applies to the DNFBPs.

21. 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 Anti-Money Laundering Authority (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.

22. 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.

23. Where a dealer 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 The Role of the Dealer in Precious Metals or Stones

24. Dealers are obligated to ensure that their businesses have the capacity to follow the legal requirements as set out in the MLFTA and this Guideline. The consequences of participation in money laundering activity, or failing to prevent one's business from being used in furtherance of this activity, are severe. Dealers should refer to the penalties provisions of the MLFTA or Appendix 1 in this Guideline.

25. The MLFTA expressly provides that its provisions apply to DNFBPs in the same way as it applies to financial institutions. This means that the duties contained in the legislation for financial institutions, also form part of the responsibilities of dealers and other DNFBPs. This requires dealers to keep client records and carry out due diligence procedures in seeking to properly know their customers. They are also duty bound to submit suspicious transaction reports to the FIU when the need arises. In order to make a proper judgment in this regard, they will need to avail themselves of training opportunities so that they may be properly equipped to protect themselves and their businesses.

26. It is worth emphasizing that the anti-money laundering responsibilities of a dealer arise only in the circumstances set out in the legislation, that is, engaged in transactions equal to or exceeding the value set out in this Guideline. It should be borne in mind, however, that this threshold may be reached through accumulated transactions.

6.1 When is a dealer a dealer?

27. A dealer in precious metals and precious stones means an individual or entity that buys or sells precious metals, precious stones or jewellery, in the course of its business activities.

- Precious metals mean gold, silver, palladium or platinum whether in coins, bars, ingots, granules or in any other similar form.
- Precious stones mean diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite.

- Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment, such as earrings, bracelets, rings, necklaces, brooches, watches, etc.

6.2 Threshold

28. After careful consideration of what is known of the business of dealing in precious metals and precious stones in Barbados, the AMLA has decided that the threshold limit above which dealers are required to keep records is set at Fifteen thousand dollars (Bds$15,000.00) where cash is used.

29. This limit was arrived at because, in the considered opinion of the AMLA, it would allow for the conduct of usual business, only triggering the anti-money laundering requirements when the size of a transaction rises to what is likely for the laundering of money in this particular industry in this jurisdiction.

6.3 Inclusion and exclusion

30. This guideline applies to all dealers in precious metals and stones whose business involves the purchase or sale of precious metals or stones in the amount of $15,000.00 in cash in a single transaction. If your business does not deal in transactions of this size, you are exempted from the requirements of this guideline. If, however, it is discovered that a customer is structuring his or her business to avoid the $15,000.00 threshold, the accumulated sums constitute a reportable amount.

31. Transactions made for the following purposes are excluded from the requirements of this guideline:

- Manufacturing jewellery;
- Extracting precious metals or precious stones from a mine;
- Cutting or polishing precious stones.

32. If all or substantially all (at least 90 percent) of your business is related to the above activities, you are not subject to this guideline. However, this changes if you conduct a transaction of $15,000.00 or more with a consumer.

6.3.1 Meaning of manufacturing jewellery

33. Manufacturing jewellery includes the following activities:
- The moulding of precious metals to obtain jewellery;
- The assembling of precious metals, precious stones or pearls to obtain jewellery;
- The blending and mixing of precious metals and alloys to obtain gold, silver, platinum and palladium;
- The applying of coatings (such as gold or silver) or finishes to or on jewellery; and
- Other similar activities.

34. Manufacturing jewellery excludes the following:
- The sole packaging or repackaging of jewellery;
- The repair of jewellery;
- The sizing or resizing of jewellery; and
- The sole engraving, chasing, or etching of jewellery.

35. The following are examples of those who are not subject to the obligations in this guideline:
- A manufacturer that sells at the retail level precious metals, precious stones or jewellery, but only in amounts under $15,000.00 per transaction;
- A retailer that sells jewellery solely made of materials other than precious metals or precious stones (for example, stainless steel, crystal, Murano glass, copper, etc.); and
- A manufacturer that only sells to or purchases from manufacturers, wholesalers or retailers.

7.0 Risk-based Approach

36. 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 dealers in precious metals and stones, 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.

37. 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*

38. 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.

39. In this regard, dealers are encouraged to pay close attention to the conduct of their businesses and apply defensive measures that are in proportion to the risk faced at any particular time. The approach used should be documented.

40. Following a risk-based approach rather than just following set rules, allows dealers to identify the areas of risk that are relevant to them and direct their defensive resources in those areas. This, however, will demand that dealers have a thorough knowledge of their business and the threats that are posed by money laundering and terrorist financing. The decisions taken must be based on the realities of the particular business.

41. In the interest of clarity, dealers should deploy defensive resources only where there is a threat of money laundering or financing of terrorism. Further, the extent of that deployment should be a function of the extent of the risk faced. As general guidance, the following considerations should be at the base of all due diligence actions:

(i) The nature and scale of the business;
(ii) The complexity, volume and size of transactions;
(iii) 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 related business entities);
(iv) Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash transactions);
(v) 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); and

(vi) Value of business and frequency of transactions.

42. Dealers 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.

43. For dealers 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 Types of Risk

44. Dealers may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling dealers, where required, to subject each client to reasonable and proportionate risk assessment. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important. Real estate agents may also refer to FATF Guidance on indicators and risk factors.[3]

45. There are certain types of risk that are of particular importance to dealers since there are peculiar to this line of business:

a) country or geographic risk;
b) customer and counterparty risk;
c) Retail customer risk; and
d) Business counterparty risk

46. 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 dealer-at-law and/or law firm. These criteria, however, should be considered holistically and not in isolation. Dealers-at-law, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

7.1.1 Country or Geographic Risk

47. Barbados is not a producer of precious metals or precious stones. These items are all imported into this country. As a consequence, the circumstances of the jurisdictions which supply these

[3] Refer to FATF Risk-Based Assessment Guidance for Dealers in Precious Metals and stones.

items is of major importance. The challenge faced by dealers in this regard will vary with whether the imported item is coming into Barbados as a raw material directly from a mining country, or whether it is a finished product coming from a third country. These may both pose risks, but the risks may be different.

48. Tourism is the main stay of the Barbados economy. Thousands of persons visit our shores yearly and many of them shop for jewellery and similar items. Further, 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. Many people from abroad live and work here. These are all potential customers of dealers. These people travel with their cultural values and their original jurisdictional ties. These are all factors that must be considered by dealers.

49. 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. Jurisdictions of this type, with low AML/CFT/CPF standards are problematic. Dealers must investigate the persons or entities with which they do business, as well as where they do business.

50. Dealers 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. Real estate agents 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].

51. Factors that should be considered in a determination that a country may or may not pose a higher risk with regard to a proposed transaction in diamonds, jewels or precious metals include:

- For rough diamonds, whether a producing or trading country participates in the Kimberley Process.
- Whether there is known mining or substantial trading of the transaction product – diamonds, jewels or precious metals - in a transaction source country.
- Whether a country would be an anticipated source of large stocks of existing diamonds, jewels or precious metals, based upon national wealth, trading practices and culture (centres of stone or jewel trading, such as Antwerp, Belgium) or unanticipated (large

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

amounts of old gold jewellery in poor developing countries). It should be recognized, however, that gold and silver have cultural and economic significance in a number of developing countries, and very poor people may have, buy and sell these metals.

- The level of government oversight of business and labour in mining and/or trading areas. The extent to which cash is used in a country.
- The level of regulation of the activity.
- Whether informal banking systems operate in a country, e.g. hawalas operate in many developing countries.
- Whether designated terrorist organizations or criminal organizations operate within a country, especially in small and artisan mining areas.
- For rough diamonds, whether a producing or trading country participates in the Kimberley Process.
- Whether there is known mining or substantial trading of the transaction product – diamonds, jewels or precious metals - in a transaction source country.
- Whether a country would be an anticipated source of large stocks of existing diamonds, jewels or precious metals, based upon national wealth, trading practices and culture (centres of stone or jewel trading, such as Antwerp, Belgium) or unanticipated (large amounts of old gold jewellery in poor developing countries). It should be recognized, however, that gold and silver have cultural and economic significance in a number of developing countries, and very poor people may have, buy and sell these metals.
- The level of government oversight of business and labour in mining and/or trading areas. The extent to which cash is used in a country.
- The level of regulation of the activity.
- Whether informal banking systems operate in a country, e.g. hawalas operate in many developing countries.
- Whether designated terrorist organizations or criminal organizations operate within a country, especially in small and artisan mining areas.

52. In addition, a dealer 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 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.

7.1.2 Customer Risk and Counterparty Risk

53. Dealers in precious metals and precious stones operate in a high-value business. Further, dealers in Barbados are not usually producers of any of the precious metals or precious stones in which they deal. Dealers are both purchasers and retailers of these precious items. They, therefore, face risks at both ends of their business.

7.1.3 Retail Customer Risk

54. A retail customer of precious metals or precious stones will, in general, not have a business purpose for a purchase of an article of jewellery, a precious stone of a precious metal. A purchase is likely to be made for purely personal and emotional reasons that cannot be factored into an AML/CFT/CPF risk assessment. Higher risk can be seen, however, in certain retail customer transaction methods:

- Use of cash. It should be recognized, however, that many persons desire anonymity in jewellery purchases for purely personal reasons, or at least the absence of paper records, with no connection to money laundering or terrorist financing.
- Payment by or delivery to third parties. However, not all third party payments are indicative of AML/CFT/CPF. It is relatively common in jewellery purchases that a woman will select an article of jewellery, and a man will later make payment and direct delivery to the woman.
- Structuring. This would involve multiple purchases below the threshold limit.

7.1.4 Business Counterparty Risk

55. Higher risk counterparties include a person who:

- Does not understand the industry in which he proposes to deal, or does not have a place of business or equipment or finances necessary and appropriate for such engagement, or does not seem to know usual financial terms and conditions.

- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
- Has significant and unexplained geographic distance from the dealer in precious metals or dealer in precious stones.
- Uses banks that are not specialised in or do not regularly provide services in such areas, and are not associated in any way with the location of the counterparty and the products.
- Makes frequent and unexplained changes in bank accounts, especially among banksin other countries.
- Involves third parties in transactions, either as payers or recipients of payment orproduct, without apparent legitimate business purpose.
- Will not identify beneficial owners or controlling interests, where this would be commercially expected.
- Seeks anonymity by conducting ordinary business through accountants, lawyers, orother intermediaries, see the paragraph above.
- Uses cash in its transactions with the dealer in precious metals or dealer in preciousstones, or with his own counterparties in a nonstandard manner.
- Uses money services businesses or other non-bank financial institutions for noapparent legitimate business purpose.
- Is a politically exposed person (PEP) and/or is a family members or close associateof a PEP.

7.2 Mitigating Risk

56. Dealers in precious metals and stones should 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.

57. Dealers should implement appropriate measures and controls to mitigate the potential money laundering and terrorist and proliferation financing risk of those customers that are determined to be a higher risk as a result of the dealers' risks assessment. The same measures and controls may often address more than one of the risk criteria identified and it is not necessarily expected that dealers establish specific controls that target each criterion. Appropriate measures and controls may include:

- General training for appropriate personnel on money laundering and terrorist and proliferation financing methods and risks relevant to dealers.
- Targeted training for appropriate personnel to increase awareness of higher risk

customers or transactions.

- Increased levels of know your customer/counterparty (KYC) or enhanced due diligence.
- Escalation within dealer management required for approval.
- Increased monitoring of transactions.
- Increased controls and frequency of review of relationships.

8.0 Know Your Client/Customer Due Diligence (CDD)

58. The process by which the dealer forms a reasonable belief that he/she knows the true identity customer and is then able to assess AML/CFT/CPF risk, is commonly referred to as know-your-customer or customer due diligence (CDD).

When Purchasing

59. The Identify Your Counterparty/Customer activity within a dealer's AML/CFT/CPF programme is intended to enable the dealer in precious metals or the dealer in precious stones to form a reasonable belief that it knows the true identity of each counterparty/customer and the types of transactions the counterparty proposes. A dealer's programme should include procedures to:

- Identify and verify counterparties/customers before establishing a business relationship, such as entering into contractual commitments. This identified natural or legal person or authorized and fully identified agents should then be the only person or persons to whom payment is authorized to be made, or product delivered, unless legitimate and documented business reasons exist, and any third party is appropriately identified and its identity verified.
- Identify beneficial owners and take reasonable measures to verify the identities, such that the dealer is reasonably satisfied that it knows who the beneficial owners are. The measures which have to be taken to verify the identity of the beneficial owner will vary depending on the risk. For legal persons and arrangements this should include taking reasonable measures to understand the ownership and control structure of the counterparty/customer.
- Obtain information to understand the counterparty's/customer's circumstances and business, including the expected nature and level of proposed transactions.

Retail Business

60. A dealer in precious metals or stones is subject to the provisions of this guideline when a retail transaction involves a sum of $15,000.00 or more in cash. A transaction below this threshold does not trigger the Know Your Customer requirements. However, if a dealer becomes aware of a

customer making more than one purchase within a six-month period, regardless of the size of the transaction, the dealer is obligated to verify the identity of the customer and maintain a record.

61. In the circumstances where transactions involving cash equal to or above $15,000.00, the general rule is that counterparties/customers must be subject to the full range of CDD measures. Furthermore, additional Identify Your Counterparty/Customer activity and procedures should be applied to higher risk determinations (such as PEPs or transactions involving higher risk countries). In these cases, for instance, a dealer in precious metals or a dealer in precious stones should implement additional measures and controls to mitigate that risk. This may require increased monitoring of transactions.

62. These steps should be recorded and maintained in a file regarding each counterparty/customer. In circumstances defined by the public authorities where there are lower money laundering or terrorist financing risks, dealers may apply reduced or simplified CDD measures when identifying and verifying the identity of the counterparty/customer and the beneficial owner having regard to the type of counterparty/customer, product or transaction.

63. In other circumstances (i.e. for transactions not involving cash equal to or above $15,000) and where national law does not require otherwise, counterparty/customer identification can, however, be accomplished through broader industry practices and associations that already maintain comparable data to which the authorities have ready access, or by reference to government held databases (registered dealer database, VAT related database, etc.). This will reduce transaction burdens, particularly upon small and mid-size dealers who already rely upon such industry resources to maintain security and high standards in their business practices. For example, in the diamond industry, transactions for rough diamonds are conducted within the scope of the Kimberley Process. Trading in rough diamonds and polished diamonds can occur through sources that are members of the World Federation of Diamond Bourses. Dealers might transparently reference these sources of counterparty/customer identification rather than recreate all identification data in multiple dealer and transaction files.

64. In similar circumstances, other regulatory programmes and/or industry associations may provide similar counterparty information and assurances. Transactions with well-known, longstanding counterparties might also be identified by transparent reference to existing information of a dealer, rather than be recreated. Such streamlined counterparty identification practices should, of course, be limited to transactions with standard trading and bank payment practices that do not give rise to suspicion and concern, and do not in any case fully eliminate the need to apply risk based analysis to transactions, customers, or counterparties.

8.1 Politically Exposed Persons (PEPs)

65. Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which practitioners who deal with them may face, have led to calls for enhanced due diligence on such persons. The Financial Action Task Force (FATF) categorises PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organization. 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.

66. It is appreciated that in a retail environment, the collection of customer information may be impractical. Dealers are, therefore, encouraged to conduct retrospective due diligence and make later reports where necessary.

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

9.0 Record-Keeping

68. To demonstrate compliance with the MLFTA and to allow for timely access to records by the FIU, dealers 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, as well as any analysis done. 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.

69. A record of all large transactions (transactions above the threshold limit) and all suspicious or unusual transactions must be kept. However, if the dealer in precious metals and stones already keeps the relevant information in a record that is readily available, that information need not be kept again.

70. 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 Training Records

71. 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 TRAINING AND AWARENESS

72. An integral element of the fight against money laundering and the financing of terrorism and proliferation is the awareness of those charged with the responsibility of identifying and analyzing potential illicit transactions. Therefore, dealers 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 sensitizing the broader staff complement to AML/CFT/CPF 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.

73. Dealers 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 recognize 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 andsuspicious 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; and

(viii) Provide all staff with reference manuals/materials that outline theirresponsibilities and the institution's policies. These should complement rather than replace formal training programmes.

10.1 Content and Scope of the Training Programme

74. Regarding the overall training programme, a dealer should cover topics pertinent to its operations and should be informed by developments in international AML/CFT/CPF 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/CPF may change.

Training programmes should, inter alia, incorporate references to:

(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.

11.0 Compliance and Audit Function

75. Dealers 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.

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

77. With respect to a corporate or other legal entity, 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 dealer remains responsible for the function.

78. 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.

79. It is recognized that the appointment of a Compliance Officer or the creation of an internal audit department may create difficulties for some small agencies, where this is not possible a dealer 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 dealer's business.

80. Where the compliance and/or audit function is contracted out, the dealer 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.

11.1 Internal Reporting Procedures

81. To facilitate the detection of suspicious transactions, a dealer should:

(i) Require clients or customers to declare the source and/or purpose of funds where a transaction seems unusual 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 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, 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.

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

11.2 External Reporting - Reporting Suspicious Activity

83. Dealers in precious metals and stones 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 dealer 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.

84. Dealers 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.

85. 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.

86. A dealer, 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.

87. 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[5] 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

[5] 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
- 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 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*)