ANTI-MONEY LAUNDERING/ COMBATING TERRORIST FINANCING GUIDELINE

For

DEALERS IN PRECIOUS METALS

AND

DEALERS IN PRECIOUS STONES

Anti-Money Laundering Authority
May, 2016

AML/CFT GUIDELINE FOR DEALERS IN PRECIOUS METALS AND DEALERS IN PRECIOUS STONES

TABLE OF CONTENTS

AML/CFT GUIDELINE FOR DEALERS IN PRECIOUS METALS AND DEALERS IN PRECIOUS STONES

ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

Terms Used In This Guideline

AMLA	Anti-money laundering authority
AML/CFT	Anti-money laundering and counter financing of terrorism
CDD	Customer Due Diligence
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
PEP	Politically Exposed Person

1.0 INTRODUCTION

After a series of high level stake holder meetings in 2007, the Financial Action Task Force (FATF) determined that dealers in precious metals and dealers in precious stones should be included among certain non-financial entities to which anti-money laundering measures should apply. In 2008, the FATF published guidance notes for these dealers.

Paragraphs 10 and 11 of that guidance provides as follows:

"10. Recommendation 12 mandates that the requirements for customer due diligence, record-keeping, and paying attention to all complex, unusual large transactions set out in Recommendation 5, 6, and 8 to 11 apply to dealers in precious metals and dealers in precious stones when they engage in any cash transaction with a customer equal to or above USD/EUR 15 000.

11. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions (see paragraph 132) and internal AML/CFT controls, and Recommendation 21 regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, apply to dealers in precious metals and dealers in precious stones when they engage in any cash transaction with a customer equal to or above the applicable designated threshold (USD/EUR 15 000)."

The Barbados Government passed legislation which incorporated this international position into our domestic law. Section 4 of the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA) states that the provisions of the Act applies to the designated non-financial business entities and professionals listed in the Second Schedule as they apply to financial institutions. Paragraph 2 of the Second Schedule names'

> "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."

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 or dealers in precious stones in Barbados, when engaged as set out above.

The definitions appearing in the MLFTA apply mutatis mutandis to the Guideline.

2.0 APPLICATION

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.

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.

Adherence to guidelines issued pursuant to section 26 of the MLFTA is mandatory. It may be noticed, however, that this Guideline contains provisions that are either permissive or advisory, and others that are obligatory. Where action is advised, the enforcing entity is at liberty to apply an alternative course of action, as long as it is equally effective in keeping that entity and the financial system safe.

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 users of it to apply such measures in their business affairs.

3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1 Money Laundering

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

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.

4.0 LEGISLATIVE AND REGULATORY FRAMEWORK

The Government of Barbados has enacted several pieces of legislation aimed at preventing and detecting drug trafficking, money laundering, terrorist financing and other serious crimes. The Acts which are most relevant for the purposes of this Guideline are as follows:

(a) Drug Abuse (Prevention and Control) Act, Cap. 131;
(b) Proceeds of Crime Act, Cap. 143;
(c) Mutual Assistance in Criminal Matters Act, Cap. 140A;
(d) Anti-Terrorism Act, 2002-6
(e) Anti-Terrorism (Amendment) Act, 2015, and;
(f) Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23.

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.

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. A Financial Intelligence Unit (FIU) has been established to carry out AMLA's supervisory function over financial institutions and DNFBPs.

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.

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.

5.0 THE ROLE OF THE DEALER IN PRECIOUS METALS OR STONES

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 the appendix in this Guideline.

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.

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.

5.1 When is a dealer a dealer?

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, broches, watches, etc.

5.2 Threshold

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 ($15,000.00) where cash is used.

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.

5.3 Inclusion and exclusion

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.

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.

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.

5.4 Meaning of manufacturing jewellery

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.

Manufacturing jewellery excludes the following:

- The sole packaging or repackaging of jewellery;
- The repair of jewellery;
- The sizing or resizing of jewellery;
- The sole engraving, chasing, or etching of jewellery.

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.);
- A manufacturer that only sells to or purchases from manufacturers, wholesalers or retailers.

6.0 RISK-BASED APPROACH

The MLFTA provides for the application of a risk-based approach to combating money laundering and the financing of terrorism. 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.

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.

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 client (e.g. whether ownership is highly complex, whether the client is a PEP, whether the client's employment income supports business activity, whether client is known to the justice system);
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 precious metal or stones originated in a jurisdiction where there is illegal mining or where mining operations

may be under the control of financiers of terrorism, whether the client is subject to regulatory or public disclosure requirements); and

vi. Value of business and frequency of transactions.

Dealers are required to regularly review their AML/CFT 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.

6.1 Types of Risk

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

6.1.1 Geographic Risk:

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 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.

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.

Jurisdictions with certain characteristics pose risks. Jurisdictions with AML/CFT 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 standards are problematic. Dealers must investigate the persons or entities with which they do business, as well as where they do business.

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 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 organisations or criminal organisations operate within a country, especially in small and artisan mining areas.
- Whether there is ready access from a country to nearby competitive markets or processing operations, e.g. gold mined in Africa is more frequently refined in South Africa, the Middle East or Europe rather than in the United States, and a proposal to refine African gold in the United States would be unusual and higher risk.
- Whether, based on credible sources, appropriate AML/CFT laws, regulations and other measures are applied and enforced in a country.
- The level of enforcement of laws addressing corruption or other significant organized criminal activity.
- Whether sanctions, embargoes or similar measures have been directed against a country.

6.1.2 Customer Risk and Counterparty Risk

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.

6.1.3 Retail Customer Risk

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 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. 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.

6.1.4 Business Counterparty Risk

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 banks in other countries.
- Involves third parties in transactions, either as payers or recipients of payment or product, 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, or other intermediaries, see the paragraph above.
- Uses cash in its transactions with the dealer in precious metals or dealer in precious stones, or with his own counterparties in a nonstandard manner.
- Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
- Is a politically exposed person (PEP).

6.2 Mitigating Risk

Dealers should implement appropriate measures and controls to mitigate the potential money laundering and terrorist 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 criteria. Appropriate measures and controls may include:

- General training for appropriate personnel on money laundering and terrorist 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.

7.0 KNOW YOUR CUSTOMER/CUSTOMER DUE DILIGENCE (CDD)

When Purchasing

The Identify Your Counterparty/Customer activity within a dealer's AML/CFT 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

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.

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.

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.

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.

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.

7.1 Politically Exposed Persons (PEPs)

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 organisation. 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 organisation PEPs: persons who are or have been entrusted with a prominent function by an international organisation, 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.

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.

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

8.0 RECORD-KEEPING

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.

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.

8.1 Training Records

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 dealers and staff;
b) Names of staff receiving the training;
c) Dates that training sessions were attended or held; and
d) An on-going training plan.

9.0 TRAINING AND AWARENESS

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analysing potential illicit transactions. Therefore, 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 sensitising the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures. Additionally, front line staff should be targeted so as to enable them to respond appropriately when interacting with the public.

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 recognise and handle potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;

(ii) Clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious transaction reporting;

(iii) Formally document, as part of their anti-money laundering policy document, their approach to training, including the frequency, delivery channels and content;

(iv) Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the Reporting Officer to whom they should report unusual or suspicious transactions;

(v) Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:
   a) New hire orientation;
   b) Operations staff;
   c) Supervisors;
   d) Board and senior management; and
   e) Audit and compliance staff.

(vi) Obtain an acknowledgement from each staff member on the training received;

(vii) Assess the effectiveness of training; and

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

9.1 Content and Scope of the Training Programme

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

(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.

10.0 COMPLIANCE FUNCTION

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.

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.

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.

10.1 Internal Reporting Procedures

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

(i) Require clients or customers to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount as the dealer determines, to reasonably ascertain that funds are not the proceeds of criminal activity. Appendix 3 indicates a specimen of a Declaration Source of Funds (DSOF) form. Where electronic reports are employed instead of the form, they should capture the information included on the Appendix and should be signed by the customer;
(ii) Develop written policies, procedures and processes to provide guidance on the reporting chain and the procedures to follow when identifying and researching unusual transactions and reporting suspicious activities;
(iii) Identify a suitably qualified and experienced person to whom unusual and suspicious reports are channelled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the FIU;
(iv) Require its staff to document in writing their suspicion about a transaction; and
(v) Require documentation of internal enquiries.

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

10.2 External Reporting - Reporting Suspicious Activity

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; or
(iii) Is of a suspicious or an unusual nature.

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.

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.

APPENDICES

APPENDIX 1

Summary of Money Laundering and Terrorism Sanctions and Offences

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

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

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

APPENDIX 2

Suspicious Transaction Report Form

CONFIDENTIAL

SUSPICIOUS/UNUSUAL TRANSACTION REPORT

PLEASE TYPE INFORMATION OR WRITE IN BLOCK LETTERS

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

THE DIRECTOR, FINANCIAL INTELLIGENCE UNIT
ANTI-MONEY LAUNDERING AUTHORITY
P.O. BOX 1372 Bridgetown, Barbados
FACSIMILE NO. (246) 436-4756
Email: **amla@sunbeach.net**
For urgent reporting – Tel. (246) 436-4734/5

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

PART A – Initial Information

1. ☐ Completed Transaction ☐ Attempted/Aborted Transaction

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

☐ NO
(Skip to No.4)

☐ YES
☐ Correction
☐ Follow-up

3. If yes, original Report's date ___ ___ ___ (D M Y)

4. Reporting date ___ ___ ___ (D M Y)

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

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

Part B – Identity of Customer 1

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

4. …….. Alternative Names/Spelling
5. …… …… Address(es)

6. ……..... Nationality/(ies)
7. …… Date of Birth (D/M/Y)

8. Identifier #1
☐ ID Card
☐ Passport
☐ Driver's License
☐ Other……
9. …… ID No.(1)
10. ……. Place of Issue

11. Identifier #2
☐ ID Card
☐ Passport
☐ Driver's License
☐ Other …….
12. ……. ID No.(2)
13. ……. Place of Issue

14. ……. Occupation
15. …….. Employer

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

…….

Telephone # (Include area Code) (C)

17. ……. ……
Email Address(es) Email address(es)

18. …….. ☐ Personal
Account Number(s) ☐ Corporate
☐ Trust
☐ Other ……..

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

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

CUSTOMER 2

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

4. ……. 5. ……
Alternative names/Spelling
……
Address(es)

6. ……. 7. ……
Nationality/(ies) Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card 9. ……
☐ Passport ID No.(1)
☐ Driver's License 10. …….
☐ Other ……. Place of Issue

11. Identifier #2 ☐ ID Card 12. …….
☐ Passport ID No.(2)
☐ Driver's License 13. ……
☐ Other …… Place of Issue

14. ……. 15. ……..
Occupation Employer

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

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

17. ……. …….
Email Address(es) Email address(es)

18. …….. ☐ Personal
Account Number(s) ☐ Corporate
☐ Trust
☐ Other ……..

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

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

Customer 2 applies where there is a transfer between customers.

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

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

4. ……. 5. ……
Alternative- Entity's name

……
Address(es)

6. ……. 7. ……
Nationality/(ies) Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card ☐ Certificate of Incorporation
☐ Passport ☐ Registration for Business Name
☐ Driver's License
☐ Other ……

9. …….. 10. …….. 11. ……
ID No.(1) Place of Issue Occupation/Type of Business

12. ……... 13. ……. ……...
Employer Telephone (#1)- area code (H) Telephone (#2) - area code (W)

……
Telephone (#3)- area code (C)

14. …….. ……
Email Address #1 Email Address #2

15. ……
Account Number(s)

16. …….
State if a/c joint, other signatories, etc

PART D – Transaction Details

1. Type of Transaction

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

2. Date(s) of transaction(s) | | | |
D M Y

3. …….
Amount & Currency

4. ……..
BBD $ Equivalent

5. …….
Name of drawer/Ordering Customer

6. ……..
Name of Payee/beneficiary

7. …….
Other bank involved, other Country

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

PART E – Grounds for Suspicion

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

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

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

PART E2

If additional information is attached, please tick box ☐

PART E3

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

……
……
……
……
……
……
……

PART F - Details of financial institution/place of transaction

1. ……
Organisation

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

3. …….
Name and Title of Reporting Officer

4. …….
Signature of Reporting Officer

5. ……..
Dealers internal reference number

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

APPENDIX 3

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*)