THE COMPLIANCE COMMISSION OF THE BAHAMAS

CODES OF PRACTICE FOR DEALERS IN PRECIOUS METALS AND PRECIOUS STONES

- ANTI-MONEY LAUNDERING
- COUNTERING TERRORIST FINANCING
- COUNTERING PROLIFERATION FINANCING
- OTHER IDENTIFIED RISKS

THE COMPLIANCE COMMISSION
#31 Poinciana House - South
East Bay Street
P. O. Box N-3017
Nassau, The Bahamas
Tel: (242) 604-4331

E-mail: compliance@bahamas.gov.bs
Web address: https://ccb.finance.gov.bs.

Revised - April, 2019
Revised - September, 2020

EXPLANATORY FOREWORD

The Compliance Commission of The Bahamas (the Commission) has powers under section 37 of the Financial Transactions Reporting Act, 2018 (FTRA) to issue Anti-Money Laundering, Countering Terrorism Financing, Countering Proliferation Financing and Other Identified Risks Codes of Practice (the Codes) for financial institutions falling within its supervisory scope. The Codes are essential in providing guidance as to the obligations and standards to be complied with and to be observed by Designated Non-Financial Businesses and Professions (DNFBPs) that are deemed financial institutions and supervised by the Commission. The Codes are to be read in concert with the key legislative laws outlined in Part B II of this document. Copies of all Codes of Practice issued by the Commission are available electronically from the Commission's website at https://ccb.finance.gov.bs.

Obligations imposed by the Codes are enforceable in accordance with section 37 (2) of the FTRA and regulation 8 of the Financial Intelligence (Transactions Reporting) Regulations, 2001 (FI)(TR)R). Financial Institutions that fail to comply with the requirements of the Codes shall be subject to sanctions.

ALL REFERENCES IN THIS DOCUMENT TO ANTI-MONEY LAUNDERING (AML) WILL INCLUDE OBLIGATIONS FOR COUNTERING THE FINANCING OF TERRORISM (CFT), COUNTERING PROLIFERATION FINANCING (CPF) AND OTHER IDENTIFIED RISKS UNLESS THE CONTEXT REQUIRES OTHERWISE.

These Codes of Practice have been issued for Dealers in Precious Metals and Precious Stones. Its purpose is to provide Dealers in Precious Metals and Precious Stones with practical guidance and best practices on how to implement an effective AML compliance and risk-based program in line with relevant legislation. It also supports the regulatory objective of maintaining the reputation of The Bahamas as a first-class international business centre with zero tolerance for criminal activity.

The Commission intends to issue periodic Directives and Guidance Notes to supplement the Codes as changing circumstances dictate.

Finally, the Commission would like to express its gratitude to all those in the profession, representative bodies and stakeholders that contributed to the development of these Codes of Practice.

THE COMPLIANCE COMMISSION OF THE BAHAMAS

Revised – April, 2019

Revised - September, 2020

TABLE OF CONTENTS

A. DEFINITIONS

"AML"	means Anti-Money Laundering. (As indicated earlier, all references in this document to AML will include obligations for Countering the Financing of Terrorism (CFT), Countering Proliferation Financing (CPF) and Other Identified Risks unless the context requires otherwise).
"AML/CFT"	means Anti-Money Laundering / Countering the Financing of Terrorism (also used for Combatting the Financing of Terrorism).
"**AML Law**s"	means The Proceeds of Crime Act, 2018, The Financial Transactions Reporting Act, 2018, The Financial Intelligence Unit Act, 2000 (as amended) the Anti-Terrorism Act, 2018, Financial Transactions Reporting (Wire Transfers) Regulation, 2018, the Anti-Terrorism Regulations, 2019 and all Regulations, Guidelines, Codes and other subordinate instruments made under these Acts. For a complete list of the legislation and citations see ***Appendix A***.
"**ATA**"	means the Anti-Terrorism Act, 2018.
"Beneficial owner"	means: (a) the natural person(s) who ultimately owns or controls a customer/client; (b) the natural person on whose behalf a transaction is being conducted; (c) a natural person who exercises ultimate effective control over a legal person or legal arrangement; and (d) where no natural person is identified under subparagraphs (a), (b) or (c) above, the identity of the natural person who holds the position of senior managing official.
"BICA"	means The Bahamas Institute of Chartered Accountants.
"Cash"	means notes and coins in any currency and includes, postal money orders, travelers' cheques, bankers' drafts, bearer-type negotiable instruments, virtual currency.
"CFATF"	means the Caribbean Financial Action Task Force.
"**CFT**"	means Combating the Financing of Terrorism (also used for Countering the

	Finance of Terrorism).
"CO"	means Compliance Officer.
"**Commission**"	means the Compliance Commission of The Bahamas, established under section 39 of the FTRA (Ch. 368) and continued under section 31 of the new FTRA, 2018.
"CDD" or "Customer due diligence"	means that part of the KYC process where information that comprises facts about a client is gathered by the dealer to assess the extent to which the client exposes the dealer to a range of risks.
"Designated entities"	means individuals or entities and their associates designated as terrorist entities by the Security Council of United Nations. The National Identified Risk Framework Coordinator shall be responsible for maintaining a list of designated entities, among other things.
"Dealer, or company"	refers to a dealer in his capacity as a financial institution pursuant to sections 4(c) of the FTRA i.e., when providing prescribed financial services, unless the context otherwise requires.
"**DNFBP**"	means a designated non-financial businesses and professionals in accordance with Recommendation 28 of the FATF 40 Recommendations and section 4 of the FTRA.
"FATF"	means the Financial Action Task Force.
"Financial institution"	means a person or entity described in section 3 & 4 of the FTRA who or which provides prescribed financial services and on which, have been imposed, AML obligations pursuant to the AML laws.
"FI(TR)R"	means the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended).
"FIU"	means the Financial Intelligence Unit.
"FIUA"	means the Financial Intelligence Unit Act, 2000.
"FTRA"	means the Financial Transactions Reporting Act, 2018.
"FTRR"	means the Financial Transactions Reporting Regulations, 2018.
"Funds"	means any assets or property of any kind, however acquired, including but not limited to currency, bank credits, deposits and other financial resources, travelers' cheques, bank cheques, money orders, promissory notes, shares, non-shareholding interests, securities, bonds, drafts, and letters of credit (Refer to FTRA definition on funds for more details).

"Identified Risks"	means corruption, cybercrime, human trafficking, money laundering, proliferation or financing of weapons of mass destruction, terrorism or financing of terrorism or such other risk as the Minister may prescribe by regulations.
"Inherent Risks"	means the vulnerabilities within the company (for example, the customer base, an activity, or industry) that is susceptible to exploitation to launder proceeds of crime or to fund terrorism.
"International organization"	means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognized by law in member countries and which is not treated as a resident institutional unit of the country in which it is located.
"KYC" or "Know your client/customer"	means the process that allows Dealers in Precious Metals and Precious Stones to know and understand their clients thereby ensuring that they are doing business legally with legitimate entities and individuals before and during the relationship. The combination of the Customer Identification Process (CIP) and the Customer/Enhanced Due Diligence (C/EDD) constitutes the KYC process.
"ML"	means Money Laundering.
"ML/TF"	means Money Laundering and Terrorist Financing.
"MLRO"	means Money Laundering Reporting Officer.
"NRA"	means National Risk Assessment is the process by which a country Identifies and assesses the ML/TF risks for the country.
"Para."	means paragraph.
"PEPs" or "Politically exposed persons"	means:- an individual who is or has been entrusted:- (a) with a domestic prominent public function, inclusive of a head of state or government. Legislator, politician, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official; (b) with a prominent public function by a foreign jurisdiction, inclusive of a head of state or government, legislator, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or senior political party official; and (c) with senior position at an international organization or branch thereof, domestic or foreign, and includes a family member or close associate of a politically exposed person.
"POCA"	means the Proceeds of Crime Act, 2018.

"Prescribed financial services"	means those services defined in sections 4 of the FTRA which make a person or entity, in relation to those services, a financial institution for AML purposes. In the case of a dealer under sections 4(c), those services are where he/she engages in, or carry out transactions for a client concerning matters stipulated in section 4(c) of the FTRA.
"Proliferation"	means the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. This could include, inter alia, technology, goods, software, services or expertise.
"PF" or "Proliferation Financing"	means providing funds or financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.
"RBA"	means Risk-Based Approach.
"Registrants"	means the financial institutions and designated non-financial businesses and professions identified in sections 3 & 4 of the FTRA in particular, Lawyers, accountants, real estate brokers and developers, designated government agencies, jewelers dealing in precious metals and precious stones, persons acting in the capacity of Trustee for which the Commission has AML supervisory responsibility.
"Risk"	All references to risk refer to the risk of money laundering and/or terrorist financing.
"SAR"	means Suspicious Activity Report (used interchangeably with STR).
"STR"	means a suspicious transaction report.
"TF"	means terrorism financing - the financing of terrorist acts, and of terrorists and terrorist organizations.
"UN"	means United Nations.
"UNSCR"	means the United Nations Security Council Resolution(s).
"WMD" or "Weapons of mass destruction"	means a nuclear, biological, or chemical weapons able to cause widespread devastation and loss of life.

Note: Some definitions are drawn from the FATF Recommendations.

B. BACKGROUND

Part B of this document describes the fundamental aspects of money laundering, terrorist financing, proliferation financing, other identified risks and provides some general introductory remarks on the international and regional organizations involved in the global fight against money laundering, terrorist financing and proliferation financing. Brief comments are also given on the obligations placed on countries to comply with international best practices and to ensure the effectiveness of a country's AML/CFT compliance regime. The establishment of a National ML/TF Identified Risk Framework (NIRF) is central to the identification of money laundering and terrorist financing methods across the jurisdiction and to determine how often those methods are used, how effective they are in moving illicit funds and whether there are gaps in the AML/CFT systems and controls. The legislative and regulatory frameworks for AML in The Bahamas have also been outlined for general reference.

Part B also explains the circumstances in which a dealer in precious metals and precious stones, by law, is deemed to be a financial institution along with citing their vulnerabilities; the supervisory framework of the Commission, inclusive of the mandatory registration procedure for all Dealers in Precious Metals and Precious Stones; the transparency of beneficial ownership; the characteristics of the fit and proper test for sound supervisory practices and the risk-based examination process.

Part C of this document highlights the requirements for periodic internal review of AML/CFT systems; the importance of upgrading technological systems, as well as covers the guidelines and procedures for conducting a risk assessment; client identification and verification (KYC); targeted financial sanctions; record keeping; reporting of suspicious transactions; and the Commission's awareness, educational and training programmes.

1. MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION FINANCING AND OTHER IDENTIFIED RISKS

1 MONEY LAUNDERING

1.1 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Its purpose is to allow them to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.

1.2 There is no one single method of laundering money. Methods range from the purchase and resale of real property and luxury items (e.g., cars or jewelry) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, in the case of drug trafficking and some other serious crimes, the proceeds usually take the form of cash, which needs to enter the financial system by some means.

1.3 Despite the variety of methods employed, the laundering process is accomplished in three stages, which may comprise numerous transactions, and which could alert a financial institution to criminal activity: These stages are:

(1) ***placement,*** which is the physical disposal of proceeds derived from illegal activity;

(2) ***layering,*** which involves the separation of illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and

(3) ***integration,*** which is the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

1.4 The three basic steps may occur as separate and distinct phases; they may occur simultaneously or; more commonly, they may overlap. How the basic steps are used depend on the available laundering mechanisms and the requirements of the criminal or his organization.

2. TERRORISM FINANCING

2.1 Unlike money laundering, which focuses on the origin of the funds in question, terrorism financing looks at the destination of the funds, which may in fact originate from a legitimate source.

2.2 Terrorism financing is the method by which "directly or indirectly, unlawfully and willfully, persons provide or collect funds with the intention that the funds should be used or in the knowledge that the funds are to be used, in full or in part, in order to carry out (a) an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the Schedule to the ATA[1]; or (b) any other act intended to cause death or serious bodily injuries to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to refrain from doing any act."[2]

2.3 The United Nations (UN) Security Council Resolution 1267[3] (UNSCR) and its subsequent resolutions has produced a list of designated persons/countries with known or suspected terrorist connections. The Resolutions require countries to freeze, without delay, the funds or other assets and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any person or entity designated by or under the authority of the UNSCR. This list is updated periodically and is forwarded to the UN's contact in each jurisdiction. The National Identified Risk Framework Coordinator (NIRFC) shall be responsible for maintaining a list of designated entities as provided by the UN; ensuring that the list remains current; circulating the list without delay upon receipt to financial institutions; requesting information on whether any designated entity on the list has funds in The Bahamas; and maintaining a consolidated list of all orders issued by the court and circulating the same to all financial institutions. Further, the FIU shall be responsible for furnishing the Attorney General with the information required to facilitate an application under section 45 of the ATA where anyone, as designated on the list, has funds in The Bahamas. Accountants/Firms should refer to section 44 of the ATA for specific details regarding the reporting obligation in accordance with the law.

---

1 Please refer to website.

2 UN 1999 International Convention for the Suppression of the Financing of Terrorism.

3 https://undocs.org/S/RES/1267(1999)
https://www.un.org/securitycouncil/content/resolutions-0 (see for any other subsequent Resolutions).

3 PROLIFERATION & PROLIFERATION FINANCING

3.1 Proliferation financing is providing funds or financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. It involves, in particular, the financing of trade in proliferation sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation.

3.2 Countries, entities and terrorists, seeking to develop weapons of mass destruction (WMD), often try to conceal the fact that the goods, technology and knowledge being procured are intended for the production of weapons.

3.3 The United Nations (UN) under UNSCRs on WMD has also produced a list of designated persons, countries and entities known or suspected in connection with WMD. The Resolutions require countries to freeze without delay, the funds or other assets, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any person or entity designated by, or under the authority of the UNSC. This list is updated periodically and forwarded to the UN's contact in each jurisdiction. Refer to the Compliance Commission's website and the 'Regulatory and Legal Framework' tab along with the UN Orders under the 'Directives and Notices' tab for further information on obligations.

3.4 The objectives of UNSCRs on proliferation of WMD concerning persons and entities designated is to ensure they are identified, deprived of economic resources and prevented from raising, moving and using funds or other assets for the financing or proliferation.

3.5 The dealer should immediately inform the Attorney General & Financial Intelligence Unit of any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions and comply with the procedures in Section 44 of the ATA.

3.6 The dealer must ensure customer/client(s) are not from a nation that is subject to sanctions by the UN or similar prohibition from any other official body that would prohibit the conducting of a transaction.

4 OTHER IDENTIFIED RISKS

4.1 In addition to the above-mentioned predicate offences, other identified risks may include corruption, cyber-crime and human trafficking as outlined in POCA. Corruption refers to any criminal conduct related to bribery, extortion, or misconduct in public office committed by or on behalf of a public officer. Cyber-crime poses a very significant risk to individuals and organizations as it involves the compromise of computer systems such as internet, emails, ransomware and mobile devices etc. Other forms of cyber-crime include hacking, phishing, denial of service attacks, creating and distributing malware, unauthorized data access, corruption, deletion and interception of data and false advertising of products and services on victims' computers. It is worth noting that cyber criminals are constantly working to find innovative and effective means to steal information, data and ultimately money by any means possible. Therefore, an updated computer system and software to safeguard against these types of unauthorized access as well as awareness of online criminal threats and techniques are the best mitigation strategies.

4.2 Human trafficking means trafficking in persons as defined in the Trafficking in Persons (Prevention and Suppression) Act (Ch. 106). According to the FATF report on financial flows from human trafficking published July 2018, it states that human trafficking is estimated to be one of the most profitable proceeds generating crime in the world, with the International Labour Organization estimating that forced labour generates US$150.2 billion per year. It is also stated that human trafficking is one of the fastest growing forms of international crimes.

5. THE GLOBAL FIGHT AGAINST MONEY LAUNDERING

5.1 The Financial Action Task Force (FATF)

5.1.1. The FATF was founded by the Governments of the G7 leading industrialized nations in 1989. The FATF is the international standard setting body for addressing money laundering and terrorist financing. As an inter-governmental body, it develops and promotes global standards and policies, to combat money laundering. Further information on the FATF can be found at www.fatf-gafi.org

5.1.2 The FATF has developed forty (40) Recommendations (Recommendations) to address money laundering and combat terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The Recommendations set out a comprehensive and

consistent framework of measures for AML/CFT and PF initiatives and are designed for universal application. They provide a complete set of counter-measures against money laundering, terrorist financing and proliferation financing covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

5.1.3 Recommendations 22 and 23 require countries to establish an AML supervisory framework to regulate designated non-financial businesses and professions (DNFBPs). Under Recommendation 22 (c), as well as 23 (b) Dealers in Precious Metals and Precious Stones have been identified as DNFBPs where they offer certain prescribed financial services.

5.1.4 Under Bahamian law the implementation of Recommendations 22 and 23 have been implemented through section 4 (c) of the FTRA.

5.1.5 The FATF has also promoted the concept of regional organizations in line with its own structure, whose goals would be to raise awareness of money laundering and terrorism financing and introduce regional evaluation programmes to monitor the implementation and effectiveness of the Recommendations, amongst other things. One such organization is the CFATF as outlined below.

5.2 The Caribbean Financial Action Task Force (CFATF)

5.2.1 The CFATF is an inter-governmental task force, organized as part of the efforts of the FATF to establish regional style bodies patterned after the FATF. The CFATF came into existence as a result of three regional meetings of Governments in 1990, 1992 and 1993. The main objective of the CFATF is to achieve effective implementation of, and compliance with the FATF recommendations to prevent and control money laundering and to combat the financing of terrorism.

5.2.2 At the 1992 meeting the Kingston Declaration called for the establishment of a Regional Secretariat. The Secretariat was established during early 1994, in Trinidad and Tobago, and funded by the FATF donor countries. The Chair of CFATF is rotated annually amongst its members. Further information on the CFATF and its work can be viewed on its website at https://www.cfatf-gafic.org/.

5.2.3 The Bahamas is one of the founding members of CFATF. The CFATF conducts an ongoing programme of the mutual evaluation of members. The last CFATF Mutual Evaluation (MER) of The Bahamas was conducted December 2015. The Report was published in

July 2017. A copy of the report may be seen at www.cfatf-gafic.org/index.php/documents/mutual-evaluation-reports.

6. NATIONAL RISK ASSESSMENT SUMMARY

6.1 FATF (Recommendation 1) places an obligation on countries to conduct a National Risk Assessment (NRA) to identify, assess and understand its money laundering and terrorist financing (ML/TF) risks. The purpose of this assessment is to identify any potential gaps or vulnerabilities in the country's AML regime, which may require the need to amend laws, regulations or policy measures. The assessment also assists government agencies, law enforcement, intelligence agencies, regulators and financial institutions, in allocating and prioritizing AML resources to mitigate risks.

6.2 The Bahamas conducted its first NRA in 2015/2016. The review was a joint effort involving all relevant public and private sector organizations. It required the collection and analysis of ML/TF data to produce a comprehensive report, the results of which are the foundation of the Bahamas' National AML Strategy. The results of the NRA are published on the website of each financial services regulator.

6.3 The NRA impacts the operations of all Financial Institutions in the Bahamas. Financial Institutions are obligated by section 5(1) of the FTRA to conduct a risk assessment for its customers, countries or geographic areas; and products, services, transactions or delivery channels. The assessment should evaluate the impact of the ML/TF risks identified in the Bahamas' NRA, and any regulatory guidance issued by its Supervisory Authority, on its business.

6.4 Following the completion of the first NRA in 2015/2016, the Proceeds of Crime Act, 2018 established an Identified Risk Framework Steering Committee which is responsible for conducting all future NRAs in The Bahamas. More information about this Committee and The Bahamas' National Identified Risk Framework can be found in Section II of this Code.

II. THE LEGISLATIVE AND REGULATORY FRAMEWORK FOR AML IN THE BAHAMAS

7 THE LEGISLATIVE FRAMEWORK

7.1 The substantive laws relating to AML in The Bahamas are contained in:

- the Proceeds of Crime Act, 2018
- the Financial Transactions Reporting Act, 2018
- the Financial Transactions Reporting Regulations, 2018
- the Financial Intelligence Unit Act, 2000;
- the Financial Intelligence (Transactions Reporting) Regulations, 2001;
- the Anti-Terrorism Act, 2018; and
- the Anti-Terrorism Regulations, 2019.

7.2 A summary overview of the laws can be found in ***Appendix A***. These laws, as well as others referred to in this Code, can be viewed in full and downloaded from http://laws.bahamas.gov.bs.

7.3 The legislation, which includes all subsequent amendments and subordinate legislative measures sets out procedures which are designed to achieve two purposes: firstly, to enable suspicious transactions to be recognized as such and reported to the authorities; and secondly, to ensure that if a customer comes under investigation in the future, a financial institution can effectively contribute to the audit trail.

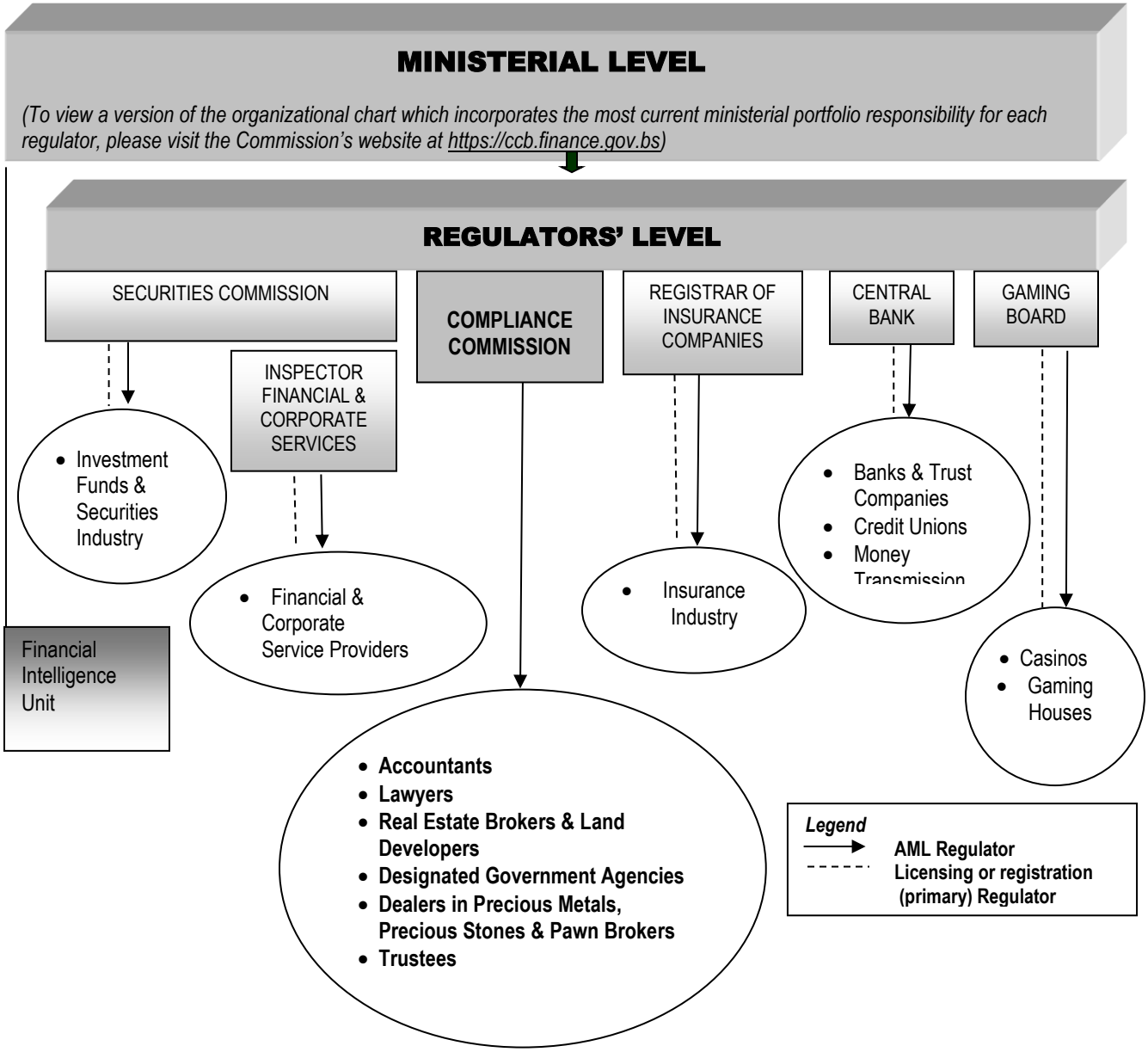
8. THE REGULATORY FRAMEWORK

8.1 An organizational chart of the AML regulatory framework, specifically identifying Dealers in Precious Metals and Precious Stones, is found below at ***Fig. 1***. The Central Bank regulates the banks and trust company's industry; the Securities Commission regulates the securities and investment funds industry; the Insurance Commission regulates the insurance industry; the Inspector of Financial and Corporate Services regulates financial and corporate service providers and the Gaming Board regulates casinos. The authority for the Commission to supervise the financial institutions within its remit, including designated

Dealers in Precious Metals and Precious Stones, is found in section 33 (1) of the FTRA.

8.2 The Financial Intelligence Unit (FIU) is the agency charged with, amongst other things, receiving and analyzing suspicious transactions reports from financial institutions (See paragraphs. 27.1 to 27.1.4) for more details about the FIU).

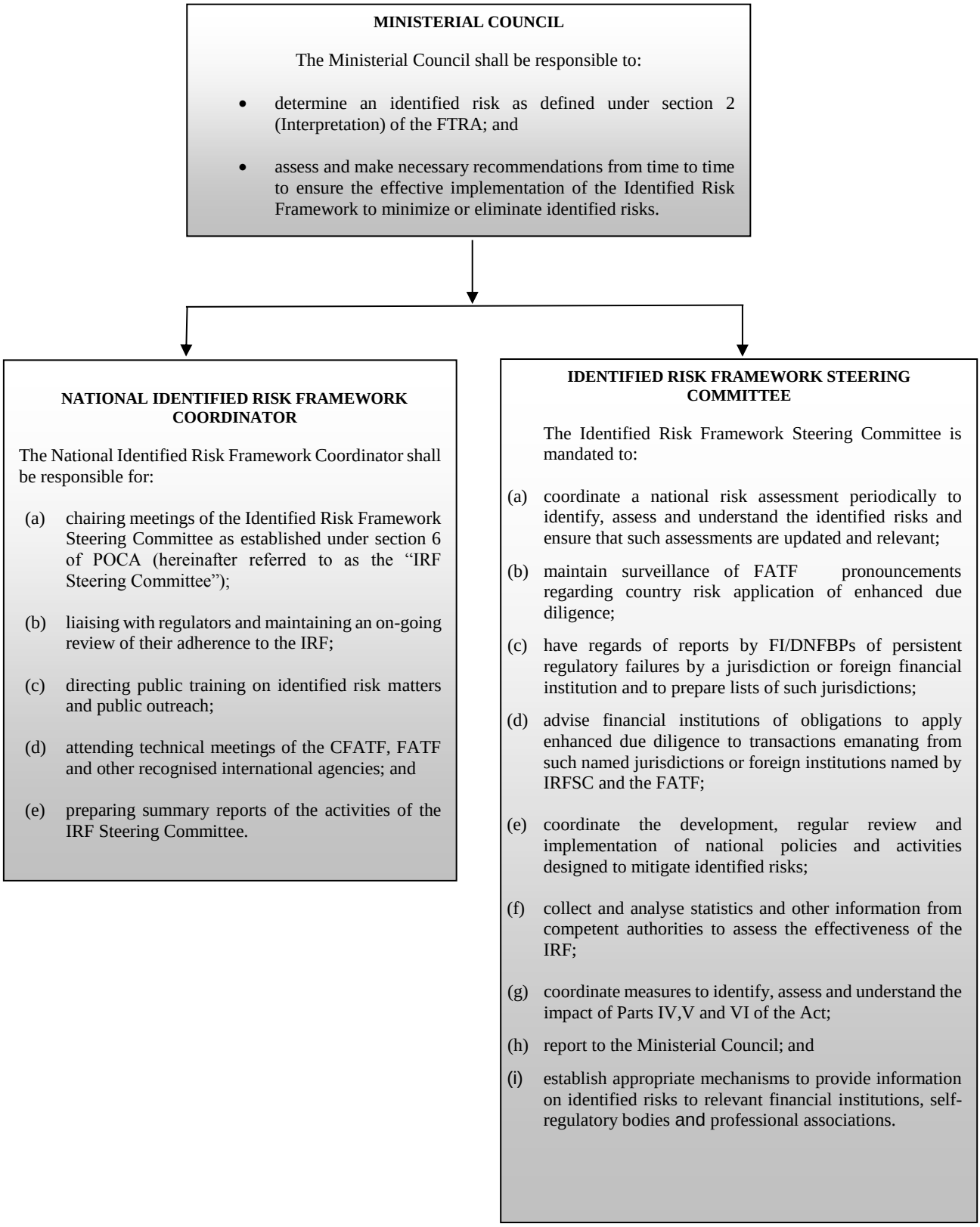
Fig. 1: Regulatory Framework for AML in The Bahamas



9. THE BAHAMAS NATIONAL IDENTIFIED RISK FRAMEWORK

9.1 The Bahamas National Identified Risk Framework (NIRF) consists of a Ministerial Council, a National Identified Risk Framework Coordinator and an Identified Risk Framework Steering Committee. Together they are charged with the responsibility of coordinating actions to assess risks, and apply resources, aimed at ensuring the risks identified are mitigated effectively (See sections 4, 5 & 6 of the Proceeds of Crime Act, 2018).

Fig.2: Below illustrates the Framework of the Ministerial Council



III. THE DEALER AS A FINANCIAL INSTITUTION

10. WHEN IS A DEALER A FINANCIAL INSTITUTION?

10.1 Dealers in Precious Metals and Precious Stones in The Bahamas are subject to the money laundering laws on two levels. On the first level, all Dealers in Precious Metals and Precious Stones are subject to the provisions of the Proceeds of Crime Act (POCA) 2018. Section 9 of POCA indicates it is an offence for persons to conceal the proceeds of crime, Section 10 states it is an offence to make arrangements concerning the proceeds of crime and section 11 provides it is an offence to acquire, use or possess the proceeds of crime

10.1.1 On the second level, all Dealers in Precious Metals and Precious Stones who offer prescribed financial services under section 4 (c) of the FTRA, in addition to being subject to the POCA, also subject to the AML/CFT regime contained in the FTRA, the FIUA, all Regulations and Guidelines made pursuant to these Acts and this Code. When offering prescribed financial services pursuant to the FTRA, the dealer is deemed to be a financial institution under the FTRA. Section 25 of the FTRA requires financial institutions to report suspicious transactions. Section 49 of the FTRA sets out the penalty for breaching s.25 of the FTRA.

10.2 When providing prescribed financial services under section 4 (c) of the FTRA.

10.2.1 A dealer is a financial institution for AML purposes in any situation when he engages in, or carries out transactions for a client concerning:

(i) Buying for the purpose of trade, sale, exchange, or otherwise dealing in any previously owned precious metals or precious stones, whether altering the same after acquisition or not; or

(ii) Lending of cash on the security of previously owned precious metals or precious stones of which the person takes possession, but not ownership, in expectation of profit, gain or reward.

10.2.2 Precious metals are defined as any article made of or containing gold, silver or platinum and such other precious metal as may be prescribed and precious stones, includes diamonds, rubies, sapphires and emeralds as per section 2 of the FTRA. Therefore, a

person whose business or any part of whose business consist of providing services in the circumstances specified in section 4(c)(i) and (ii) of the FTRA, they are designated as a financial institution and are required to be registered with the Commission.

10.2.3 Dealers in precious metals and stones (DPMS) must fulfill specific obligations under the Financial Transactions Reporting Act (FTRA 2018) and associated Laws to help combat money laundering, and terrorist financing in The Bahamas.

10.2.4 Dealers in Precious Metals and Precious Stones/ Pawn Shops must meet the obligations of the FTRA including registering with the CC, implementing an AML compliance program, and are subject to risk- based examinations as defined in Section 17 (see below).

10.2.5 Dealers in Precious Metals and Precious Stones/ Pawn Shops are subject to Customer Due Diligence (CDD) obligations, as specified in Section VII, whenever the company engages in transactions for a client as in a single transaction, equal to or above or linked transactions in the amount of B$15,000 (B$15,000 threshold transaction amount for CDD).

10.2.6 Dealers in Precious Metals and Precious Stones/Pawn Shops must conduct simplified due diligence on transactions below $15,000. The simplified due diligence requirement is to identify the customers (I.e. name of customer & contact information e.g. phone number & address). There is no requirement to verify the customer's identity. However, the business relationship should be continually monitored for trigger events which may create a requirement for further due diligence in future.

10.2.7 Dealers must perform CDD where it suspects money laundering or terrorism financing, and where it has reason to doubt the veracity or adequacy of information obtained from earlier CDD.

10.2.8 Dealers must also perform any prescribed measures relating to anti-terrorism sanctions, ministerial directives or to give effect to recommendations of the Financial Action Task Force.

A dealers' main obligations under the AML/CFT laws are summarized below:

i. Register with the CC;

ii. Submit Reports to the FIU;

iii. No "Tipping-off";

iv. Keep Records;

v. Ascertain customer identity;

vi. Ascertain whether the customer is acting for a Third Party;

vii. Appoint a Compliance Officer and Money Laundering Reporting Officer;

viii. Develop and implement an effective AML Compliance Programme

11 VULNERABILITIES OF DEALERS IN PRECIOUS METALS AND STONES

11.1 The key risks and vulnerabilities identified by The Bahamas ML/TF National Risk Assessment[4] within the Dealers in Precious Metals and Precious Stones, for which dealers should observe and seek to mitigate the various operational risks of their businesses are noted below:

- This sector which is highly cash intensive can attract criminals to launder money due to the high value items sold which can provide a way for criminals to place large amounts of illicit funds into the financial system. Criminals can also have an avenue to disguise the origin of funds.
- Liquidity of products in precious metals and stones, particularly gold and diamond, offer the advantage of having a high intrinsic value in a relatively compact form. They can be "cashed" easily in most areas of the world. Hence, they are vulnerable to be used in money laundering for their ease to be hidden and transported.
- Precious stones and metals are portable, highly valuable, and can be easily bought and sold. These characteristics make it easier for criminals (including terrorists) to exploit them to launder their illicit funds. Criminals are also known to use funds obtained from their illegal activity to buy precious metals and stones, and subsequently convert them back to cash. Such precious commodities could also be used directly to support criminal activities. The risk increases when the transaction is conducted in cash where it is more difficult to trace the origin of the funds.
- Precious metals and precious stones are easily transportable, highly liquid and a highly concentrated bearer form of wealth. They serve as international mediums of exchange and can be converted into cash anywhere in the world. In addition, precious metals, especially gold, silver and platinum, have a readily and actively traded market, and can be melted into various forms, thereby obliterating refinery marks and leaving them virtually untraceable.

4 Reference the Commonwealth of The Bahamas National Money Laundering & Terrorist Financing Risk Assessment Summary 2015/2016 via the Compliance website at https://ccb.finance.gov.bs.

11.2 OTHER VULNERABILITIES ASSOCIATED WITH DEALERS[5]:

- The regulatory characteristics of the gold market makes it attractive for organized crime groups to own cash-for-gold businesses in order to place and integrate illicit proceeds. Given the limited level of industry oversight and licensing requirements, cash-for-gold businesses have the potential to provide criminal groups with a continuous supply of untraceable gold commodities from various sources. Furthermore, this supply is purchased at below market cost, directly from the general public—who do not have to prove that they own the second-hand gold presented for sale. The high-volume, low value transactions conducted through these cash-intensive businesses can be easily falsified or co-mingled with the proceeds of crime, while the purchased gold can be used to make untraceable gold-based payments for illicit goods and services. Because much of the recycled material is purchased in cash, large numbers of transactions are undertaken anonymously. Individuals who have a need to launder cash, especially those involved in organized crime, are very willing to participate in the cash-for-gold business because there is a high propensity to make a profit and in most jurisdictions, there is little governance or oversight of this type of activity. People with no criminal history are also prepared to undertake this activity even if they suspect that the purpose of the activity is ML. Trade in recycled gold, both legal and illegal, requires little start-up capital and therefore operations can be very itinerant, opening and closing with little difficulty. This adds to the difficulty for regulators to monitor these activities.

11.3 As cash is the most common form of money laundering, Dealers in Precious Metals and Precious Stones should be aware that money laundering risks posed by transactions, particularly where there are no direct contact with a client, should also be an area of concern and should be closely monitored with proper procedures in place to mitigate any potential risks **(See Appendix D for a summary of related red flags).**

Please note that the above lists are not an exhaustive listing.

5 FATF Report /June 2013 Money Laundering and Terrorist Financing Vulnerabilities of Dealers in Precious Metals and Precious Stones

IV. SUPERVISORY FRAMEWORK OF THE COMMISSION

12. THE COMMISSION

12.1 The Establishment of the Commission

12.1.1 Section 31(1-3) and section 32 (1-2) of the FTRA establishes the continuation and functions (as noted below) of the Commission as a body corporate for the purpose of ensuring that financial institutions within its remit (as set out in sections 4 (c) of the FTRA, comply with the provisions of the Act. Sections 33-37 provides for the registration, powers, confidentiality requirements and other matters relative to the Commission. The Commission consists of three members appointed by the Governor-General.

12.2 Functions of the Commission

12.2.1 **The Commission has a two-fold function, namely:-**

- to maintain a general review of financial institutions for which it has supervisory responsibility, in relation to the conduct of financial transactions and to ensure compliance with the provisions of the FTRA, the FI(TR)R, POCA and guidelines issued by the FIU; and

- whenever the Commission deems such to be necessary, to conduct on-site examinations of the business of its registrant financial institution for the purpose of ensuring compliance with the provisions of the AML laws and regulations. The Commission can appoint an auditor, at the expense of the dealer, who will conduct such examination and report thereon to the Commission.

12.3 Powers of the Commission

12.3.1 **The Commission has powers to:**

- do all things necessary for the performance of its functions including entering into contracts;

- require, at all reasonable times, a financial institution to produce transaction records, verification records and any other records prescribed by Regulations that must be kept under the FTRA 2018;
- require financial institutions to provide such information or explanation, as it may reasonably require, for the purpose of enabling the Commission to perform its functions under the FTRA 2018;
- periodically issue Codes of Practice, particularly to provide guidance as to the duties, requirements and standards to be complied with and the procedures (whether as to verification, record-keeping, reporting of suspicious transactions or otherwise) and best practices to be observed by its registrant financial institutions in meeting their obligations under the FTRA 2018 and other AML laws; and
- pursuant to section 57 of the FTRA, 2018 notwithstanding any penalties under the FTRA, 2018, the Commission as a Supervisory Authority (as defined in Section 2 of the FTRA, 2018) may impose administrative penalties on financial institutions and individuals of financial institutions for failure to comply with provisions of the FTRA, 2018 and Proceeds of Crime Act 2018 (POCA). The Commission has implemented an enforcement program that sets out the process that the Commission will follow when a financial institution or individual of a financial institution or individual of a financial institution fails to comply with the FTRA, 2018 or POCA, 2018. The Commission may become aware of non-compliance based on examinations, evaluations, complaints or market intelligence. Registrants must familiarize themselves with the penalties and obligations under the FTRA, 2018 and POCA, 2018.

12.3.2 The Commission's Schedule of Administrative Monetary Penalties can be found at https://ccb.finance.gov.bs/regulatory-legal-framework/enforcement-sanctions-penalties/. See also the Commission's Schedule of Administrative Monetary Penalties at Appendix C below.

12.4 Supervision of the Commission

12.4.1 The Commission supervises its registrants, which includes Dealers in Precious Metals and Precious Stones, through a combination of registration, risk assessments, on-site and off-site examinations, follow up processes of all remedial actions, education, training and awareness programmes. The Commission however, is not obligated to provide training as

it is the dealers responsibility to meet this obligation. In addition, periodic directions intended to supplement the Codes are issued when necessary.

12.4.2 The Commission also has an established annual programme of engagements with the representative bodies of the financial institutions that it regulates. Separate consultative meetings are held each year with the owners and senior management to discuss plans for the ensuing year.

12.4.3 As part of an industry awareness inititative, The Commission also particpates in joint Industry briefings with other regulators on an annual basis or whenever necessary.

13 REGISTRATION OF DEALERS IN PRECIOUS METALS AND PRECIOUS STONES WITH THE COMMISSION

13.1 It is mandated by law, in accordance with section 33(1) of the FTRA for Dealers in Precious Metals and Precious Stones carrying out business pursuant to section 4(c) of the FTRA to register with the Commission. The registration process is simple and free of charge. Mandatory Registration is available on-line via the Commission's website at https://ccb.finance.gov.bs.

13.2 Dealers in Precious Metals and Precious Stones registered with the Commission are required to confirm their status via the Commission's website by December 31st of each year.

Notwithstanding the above, the Commission is at liberty to adopt supplementary measures that it deems necessary to achieve or enhance effective supervision.

13.4 **Dealers in Precious Metals and Precious Stones that fail to comply with the provisions of section 33(2) of the FTRA commits an offence and is liable to a penalty of five thousand dollars ($5,000) for each day that the FI remains unregistered. Further, where a FI fails to notify the Commission as required under section 33(3), the FI commits an offence and is liable to a penalty of five thousand dollars ($5,000) for each failure to notify the Commission.**

13.5 **N.B. The Commission does not license or regulate the business activities of the financial institutions for which it has AML supervisory responsibility. Licensing of these activities, if required by law, is regulated by the statutory authority charged with this responsibility.**

14. COMMISSION AWARENESS AND TRAINING PROGRAMMES FOR DEALERS IN PRECIOUS METALS AND PRECIOUS STONES

14.1 Though not obligated to do so, The Commission organises annual training programmes for Dealers in Precious Metals and Precious Stones. In addition, officers of the Commission are available to offer specific training programmes for individual companies upon request. The annual training provided by the Commission does not preclude the dealer from participating in other forms of training and development in the AML space, independent of what the Commission provides. In fact, it is encouraged since it is the responsibility of the dealer.

14.2 Dealers in Precious Metals and Precious Stones may engage in self-directed learning (for example, by subscribing to free subscriptions to publications and newsletters from think tanks and professional bodies or by participating in webinars) as well as attending other independently sponsored and organized forms of training and development initiatives.

14.3 As a tool of supervision, the Commission also convenes a meeting at the beginning of each year with owners and executives of the sector. The purpose of these meetings is to collaborate and to discuss any AML concerns of the profession, as well as the Commission and to convey the Commission's strategic plans for the year. These meetings are extremely beneficial for both parties, in that, the Commission can appreciate the concerns in the industry and the profession appreciates that the Commission welcomes dialogue. The Commission also uses the opportunity to update the profession on any current trends, as well as legislative changes, including those being contemplated, etc.

15 BENEFICIAL OWNERSHIP

15.1 The transparency of beneficial ownership of legal persons and legal arrangements is a requirement by statute law and in accordance with FATF standards to deter and prevent

the misuse of corporate vehicles.[6] Dealers in Precious Metals and Precious Stones are therefore required to put in place adequate measures to:

a) prevent legal persons and legal arrangements from being used for criminal purposes;

b) make legal persons and arrangements sufficiently transparent; and

c) ensure that accurate, up-to-date basic information and beneficial ownership information are available and can be accessed by the Commission in a timely fashion.

15.2 Beneficial owner refers to the natural person(s) who ultimately[7] owns or controls a client and/or the natural person on whose behalf a transaction is being conducted. It also includes a person who exercises ultimate effective control over a legal person or legal arrangement.

15.3 From the company's perspective, the term beneficial ownership, when used to refer to beneficial ownership of a transaction in AML context is conventionally understood as equating to ultimate control over funds in such account, whether through ownership or other means. A key task is to identify and verify your customers' beneficial ownership arrangements. It is crucial to know who the beneficial owner(s) is so that you can make appropriate decisions about the level of money laundering and terrorist financing risk associated with your customer.

16 FIT & PROPER TESTS

16.1 The Commission, via its endorsement of the FATF Standards, in particular recommendation 28.4 (b), requires that dealers under its remit ensure full compliance to fit and proper best practices of its key persons namely, beneficial owners and the individuals involved in the management and control of the company, as well as those who exercise significant power or discharge significant responsibilities in relation to the day-to-day operations.

16.1.1 The fit and proper assessment is both an initial process undertaken during the registration and a continuous and cumulative process, where factors such as honesty, integrity and reputation; competence and capability; and financial soundness, as well as previous

6 Refer to the FATF Recommendations 24 & 25, coupled with their Interpretive Notes.

7 Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. Definition taken from the Glossary to the FATF Recommendations.

disciplinary records are assessed. These factors, which are universally accepted, constitute a framework of minimum standards for sound supervisory practices. However, regulators are free to adopt supplementary measures that they deem necessary to achieve and/or enhance effective supervision in their jurisdiction. For example, they may assess the ongoing conduct of business, and the history of compliance with all applicable laws, regulations and codes.

16.1.2 The Commission, pursuant to section 37 of the FTRA, has the authority to assess and take all necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function within the company that provides financial services in accordance with sections 4(c) of the FTRA .

16.2 The Commission, during its mandatory registration process of all registrants, pursuant to section 33(1) of the FTRA, will consider universally accepted factors when assessing the fitness and propriety of beneficial owners and individuals involved in the management and control of the company. These key factors are outlined in some detail below.

16.2.1 **Honesty, Integrity and Reputation** – an examination of the person's character; moral soundness; and ethical compass. In determining the honesty, integrity and reputation of key persons holding interest in the company or key managerial positions, the Commission will take into account, among other things, whether the person is absence of criminal convictions in any country which render one unfit to be a dealer; an undischarged bankrupt; disqualification as a dealer in any other country or has been convicted, on indictment, of dishonesty, fraud, narcotics and human trafficking, money laundering, terrorist and proliferation financing; other identified risks offences; theft or financial crime within the past ten (10) years. Older convictions or indictments will be reviewed on a case-by-case basis.

16.2.2 The Commission will not accept for registration, a company where persons (i.e., beneficial owners, senior management or individual with significant power or authority) are under the age of twenty-one; legally declared to be of an unsound mind; or who is certified to be suffering from a mental disorder within the meaning of the Mental Health Act; outdated police record or convicted of any of the offenses outlined above. The Commission will examine each applicant on a case-by-case basis taking into account the seriousness of, and circumstances surrounding the offence, the explanation offered by the convicted

person, the relevance of the offence to the proposed role, the passage of time since the offence was committed and evidence of the individual's rehabilitation.

16.2.3 **Competence and Reliability** – demonstration through their experience and training that they are suitable to perform, operate and manage the company's affairs and possess the educational background, work experience or expertise in the nature of the business being conducted and/or continued professional development in relation to the job functions.

16.2.4 **Financial Soundness** – an examination of their fiscal responsibility and financial integrity. In determining the financial soundness of the key person (natural or corporate) the Commission will examine, among other things, whether there are any indicators that the key person will not be able to meet its debts as they become due; subject to any court judgement and/or have financial obligations that have not been satisfied within a reasonable period.

16.2.5 **Previous disciplinary record** - general compliance history and whether the Commission or any other regulatory authority has imposed a disciplinary sanction or administrative fine on the dealer.

16.3 All individuals with the responsibility for the management and control of the company and key persons within the company must prove to, and assure the Commission that they comply with fit and proper requirements. For Non-Dealers in Precious Metals and Precious Stones, this can be accomplished through the Know Your Employee (KYE) process. Dealers in Precious Metals and Precious Stones are hereby made aware that the Commission will take all measures necessary to ensure that fitness, propriety or other qualification tests are adhered to on a continuous basis.

16.4 **Failure to adhere to any of the above criteria may lead to the non-registration or de-registration of the company. Further, a person who commits an offence of money laundering or any identified risk activity knowingly or un-knowingly, will be liable on summary conviction, to imprisonment pursuant to section 15 of the Proceeds of Crime Act, 2018.** (See **Appendix B** for penalties)

POLICY ON ADMINISTRATIVE PENALTIES FOR REGISTRANTS OF THE COMPLIANCE COMMISSION OF THE BAHAMAS UNDER THE FINANCIAL TRANSACTIONS REPORTING ACT 2018

1. Pursuant to section 57 of the FTRA, notwithstanding any penalties under the FTRA, the Commission as a Supervisory Authority[8] may impose administrative penalties to financial institutions and individuals of financial institutions for failure to comply with provisions of the FTRA and Proceeds of Crime Act 2018 (POCA).

2. Administrative penalties are monetary penalties imposed by the Commission via legislative authority without the commencement of legal proceedings. The imposition of administrative penalties provides an alternative reprimand which is less costly and time consuming.

3. Penalties are imposed as a mechanism to enforce compliance with regulatory legislation and dissuade financial institutions and individuals from breaching their obligations under the FTRA or POCA.

4. This policy sets out the process that the Commission will usually follow when a financial institution or individual of a financial institution fails to comply with the FTRA or POCA. The Commission may become aware of non-compliance based on examinations, evaluation, complaints or market intelligence. Registrants must familiarize themselves with the penalties and obligations under the FTRA and POCA.

17. RISK-BASED EXAMINATION PROCESS

17.1 The Commission carries out its supervisory oversight by means of a risk assessment exercise, as well as an on-site and off-site examination programmes. Companys are required to complete a Risk Assessment Questionnaire issued by the Commission for an initial assessment of the inherent risks to the Company. The purpose of the risk assessment questionnaire is to gather information on the salient features of the company's overall structure, clients (including geographical location and beneficial owners), products, tranactions, delivery channels, and oversight and governance. The outcome of the risk assessment along with the latest on-site examination evaluation, will determine the frequency and intensity of the Commission's examination program of the company. The risk assessment will be followed by an on-site or off-site examination of the company.

[8] Section 2 of the FTRA defines Supervisory Authority as "the agency designated by law for ensuring compliance with the requirements of this Act and any other Anti-Money Laundering laws of The Bahamas, and includes the Central Bank of The Bahamas, the Securities Commission of the Bahamas, the Insurance Commission of The Bahamas, the Inspector of Financial and Corporate Services, the Gaming Board and the Compliance Commission.

17.1.1 On-site examination will not be conducted in the absence of the firm's documented risk-based policies and procedures manual, unless otherwise instructed by the Commission. In this regard, the firm will be given a specific timeline to document its risk-based policies and procedures manual.

17.1.2 Risks, once assessed, are not static – risks may increase or decrease. Risk assessments must be updated when there is a material event or change in the risk profile of the entity, for example introduction of new products and services, as awareness of new vulnerabilities and typologies become known, important changes in existing products and services and when new information on ML/TF typologies and national risks is available. The risk assessment must also be tested as part of the internal compliance effectiveness review. The risk assessment is evaluated during on-site and off-site examinations.

17.1.3 The Commission administers four (4) types of examinations, as outlined below:

- routine (on-site only);
- follow-up (on-site or off-site examination);
- random (on-site only); and
- special (on-site only).

17.1.4 The most important of these four examinations is the routine examination as it provides an in-depth assessment of the company's risk profile, policies and procedures, and tests the adequacy, effectiveness and control measures implemented to mitigate risks by a company to satisfy its AML obligations.

17.1.5 The examination focuses on procedures and systems to examine the company's obligation to comply with AML laws and guidelines and to implement an AML Compliance Program. The Bahamian AML laws and applicable guidelines require DNFBPs to implement an AML Compliance Program as outlined below:

- Conduct and document a risk assessment of the company's inherent risks to determine the level of exposure to the risks of money laundering, terrorist financing, proliferation financing;
- Establish written risk-based policies and procedures that comply with the provisions of AML laws and guidelines;
- Identify and verify customers and their source of funds;

- Appoint a CO and a MLRO;
- Keep transaction, identification and vertification records;
- Conduct on-going monitoring of customer transactions;
- Report suspicious transactions to the FIU;
- Ensure the management and appropriate staff receive AML training annually;
- Conduct internal AML compliance reviews of its operations at least once per year; and
- Submit to AML examination by the Commission and its appointed agents.

17.2 On-Site Examinations

17.2.1 Section 32(1)(b) of the FTRA authorises the Commission to conduct on-site examinations (OSEs) of the prescribed financial services performed by dealers, when deemed necessary.

17.2.2 **N.B.: The OSE is not an audit of the business activities. It is simply a process to determine the dealers' level of risks, the measures in place to mitigate the risks and the company's compliance with the AML requirements.**

17.2.3 With the exception of the routine examination, which must be conducted by a licensed public accountant, duly appointed by the Commission, all other types of on-site examinations are conducted by the Commission's Inspection Unit.

17.3 Off-Site Examinations

17.3.1 The off-site examination of the dealer will only be carried out by the Commission's Inspection Unit during a follow-up of a routine examination or during a risk assessment of the company. The follow-up precedures can be found in para. 17.6 and the risk assessment in para. 19.

17.4 Types of examinations:

17.4.1 Routine Examination

17.4.1-1 The routine examination is conducted on-site and must be performed by a licensed public accountant or accounting company approved by the Commission. The approved list of Accountants is issued annually and posted on the Commission's website.

17.4.2 **N.B. The routine examination takes the form of an "agreed upon procedure" designed to test the adequacy of AML systems that have been implemented by a dealer for the purpose of meeting its obligations under the AML laws and regulations. The "agreed upon procedure" was developed in conjunction with BICA.**

17.4.3 The Commission determines, on a risk-sensitive basis, when a supervised financial institution should be required to undergo an on-site examination, having due regard for the adequacy of its policies and procedures for AML purposes and risk assessment.

17.4.4 The Commission's examination year for the routine examination runs from **1st January to 31st December of each year or specified by the Commission**. However, the risk rating assigned to the company by the Commission will determine the examination cycle of the dealers that provide prescribed financial services. As previously stated, the routine examination must be an on-site examination. The on-site examination report, must be completed and submitted to the Commission on or before the 30th June of each year following the period covered by the examination or as specified by the Commission.

17.4.5 The licensed public accountant, engaged in conducting a routine on-site examination, must first undergo the relevant training by the Commision prior to obtaining a Letter of Appointment[9], which gives him or her the authorization to commence an examination.

9 A Letter of Appointment is a document issued to licensed accountants by the Commission authorizing them to conduct on-site examinations as its agents. This document indemnifies the accountant from any action which may arise in the course of or as a result of the examination.

17.4.6 A dealer may select the licensed public accountant of its choice, however, the examining accountant must be independent of the company and the company should satisfy itself that the examiner has a current and valid Letter of Appointment.

17.4.7 A routine examination assesses the dealer's compliance with the AML laws i.e. the FTRA, FTRR, the FI(TR)R, this Code and the FIU Guidelines. The examination ensures evidence of requisite documentation and reviews the policies, procedures and practices in place for the under-noted operational areas of the dealer's financial intermediary activities:

(1) the verification/identification of clients;

(2) maintenance of clients verification and transaction records;

(3) reporting of suspicious transactions to the FIU;

(4) appointment of a CO and MLRO;

(5) the internal procedures for money laundering, detection and prevention as required by the FI(TR)R inclusive of personnel training; and

17.4.8 In the case of a routine on-site examination, once completed, the examining accountant should have an exit meeting with the company to discuss the examination findings. Within 10 days of completing the examination form the examining accountant must submit the completed examination form to the Commission to be evaluated. Those dealers that receive an adverse rating on the routine on-site examination will be scheduled for a follow-up examination.

17.5 Frequency of the routine on-site examination

17.5.1 The Commission's frequency and intensity of the on-site examination of the dealer is on a risk sensitive basis, taking into account:

- the risk rating assigned (i.e., low, medium or high) to the company by the Commission;
- the risk rating score of the last on-site examination conducted;

- the Commission's understanding of the ML/TF risks profile of the dealer, its characteristics and in particular its diversity;
- the identified ML/TF risks, the policies, procedures and internal controls associated with the dealer, as identified by the Commission's assessment of the dealer's risk profile; and
- the ML/TF risks present in The Bahamas;

NB: Companys will also be subject to follow up off-site examination during the interim period of the risk-based examination cycle.

17.5.2 The Commission will advise the company regarding the next date for a routine on-site examination taking into account the following considerations:

- the Commission's risk assessment of the company's prescribed financial services;
- an evaluation of the company's risk-based policies and procedures for combating money laundering and terrorist financing to determine their adequacy; and
- an evaluation by the Commission of the latest examination completed in relation to the company to determine the company's level of compliance with its statutory obligations under the AML laws and the Commission's Codes of Practice.

17.6 Follow-up Examinations

17.6.1 Follow-up examinations are conducted solely for the purpose of addressing the deficiencies of the AML compliance program of dealers that have been identified through a risk assessment and the routine on-site examination. The examination can be conducted on-site or off-site depending on the severity of the case. Such examinations are specific in scope and will focus on the identified weaknesses. Follow-up examinations are conducted by Examiners of the Commission's Inspection Unit.

17.6.2 Procedures for on-site Follow-up visits

17.6.2(a) Where an adverse rating is given, a Notice is issued advising the company of a follow-up examination to take place within fourteen (14) working days. Further, the Commission will

advise the company of the specific timeline to rectify all deficiencies discussed during the follow-up visit.

17.6.2(b) Steps for Follow-up on-site Examinations:

Step 1. The Commission contacts the dealer to arrange a meeting with Senior Management and/or the CO/MLRO Officer(s) within fourteen working (14) days. The purpose of the meeting is to discuss the results of the routine examination.

Step 2. During the meeting, the inadequacies of the AML compliance program are clearly identified, and a strategy is devised for addressing them.

Step 3. The Commission will in turn issue a final letter outlining the deficiencies and set a deadline for the company to satisfactorily address all issues. Failure to adhere to the set deadline, may result in the Commission invoking administrative penalties.

17.6.2(c) Where sufficient progress is evident, no further follow-up visit is required regarding those issues and a report to this effect is made and the company is advised that all deficiencies have been satisfactorily addressed.

17.6.3 Procedures for off-site Follow-up

17.6.3(a) If the follow-up is to be conducted off-site, this means that there were deficiencies identified that can be resolved without a follow up on-site examination. The Commission will request additional information and make the necessary assessment. Pending no further action, the company will be advised accordingly.

17.6.3(b) However, if a dealer does not adhere to the strategy outlined for resolving the deficiencies within their AML compliance program, the following steps below are taken:

Step 1. A warning letter is forwarded to the dealer highlighting the details of previous discussions and/or communications and reminding the company of the agreed-upon strategy for addressing the deficiencies. A maximum period of three (3) months will be given for the dealer to rectify all deficiencies.

Step 2. The Examiner will follow up in the interim to determine the company's progress in adequately addressing the deficiencies. However, the

company has an obligation to inform the Commission that the deficiencies have been addressed and the recommendations implemented.

Step 3 Where the AML compliance program's examination is found to be adequate, a final report is written to this effect. If there is insufficient progress, a report is written on the non-compliance of the law and The Compliance Commission will determine whether or not legal action is to be pursued.

17.7 Random Examination

17.7.1 In addition to the routine examination, dealers are also subject to random on-site examinations by the Inspection Unit of the Commission. The primary purpose of the random examination is to test the routine examination process. The random examination, whenever selected, will override the risk based approach examination cycle.

17.7.2 The assessment process to be followed for a random examination is the same as that for the routine examination process (see section 17.4 to 17.5).

17.7.3 In the case of a random examination, a Notice will be sent to the dealer at least two (2) weeks prior to the examination. This Notice will be forwarded to the MLRO/CO or the Senior Management of the dealer.

17.8 Special Examination

17.8.1 The Commission will conduct an on-site examination of a dealer in "special" circumstances, to determine if there has been any infraction of the AML laws and the extent of any such violations. Such an examination will usually take place where a dealer has violated any provisions of the AML laws, or where information comes to the attention of the Commission that a statutorily dealer is providing prescribed financial services despite having advised the Commission to the contrary. Depending on the nature of the circumstances, which give rise to invoking this approach, the procedure may be either a full examination as in the case of a routine examination, or an investigation directed towards a specific issue.

C. INTERNAL AML PROCEDURES

This part provides some guidance on implementing the internal AML procedures to give effect to the obligations in:

- Part II (sections 6-9, 13-14) of the FTRA and Part lll (regulations 4-13) of the FTRR that deal respectively with customer due diligence, verification requirements, Record-keeping (section 15-18) of the FTRA, Suspicious Transactions and Reporting (section 25-30) of the FTRA; and

- Regulation 3-6 of the FI(TR)R which requires the implementation of internal reporting procedures for identification, record keeping, suspicious transaction reporting and staff awareness, education and training[10].

The Commission has implemented a risk-based supervisory framework for addressing AML vulnerabilities posed to the entire company. The process of implementing such a framework involves putting in place procedures for identifying the money laundering, terrorist financing and proliferation financing risks facing the company, given its clientele, products, transactions, geographical regions and delivery channels. Companies should have regard to all available information, including published money laundering typologies[11] and terrorist lists, to assist with identifying potential risks. For Dealers in Precious Metals and Precious Stones to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the company. The success of internal policies and procedures will depend largely on the internal control systems. Two (2) key factors that will assist in achieving this objective are:

1. Culture of Compliance

Compliance must be embedded within the very fabric of an organization, if the goal of the organization is to adhere to the legislative laws of the country. The culture of compliance must be a part of the everyday workflow and sets the foundation and expectation for

[10] These procedures are mandated by Recommendations 10-11, 18, 20, 22-23, of the FATF's 40 Recommendations

[11] See FATF Money Laundering Typologies, http://www1.oecd.org/fatf/FATDocs_en.htm#Trends

individual behavior across the organization. Without a commitment to compliance, even the best policies and procedures will be useless. This should encompass:

- developing, delivering, and maintaining a training program for all Dealers in Precious Metals and Precious Stones as well as Non-Dealers in Precious Metals and Precious Stones with responsibility for any aspect of the company's AML compliance program;
- monitoring for any government regulatory changes; and
- undertaking a regularly scheduled review of applicable compliance policies and procedures within legal practices, which will help foster a culture of compliance in the company.

2. Senior Management Responsibility and Support

Senior management is ultimately responsible for ensuring that the dealer maintains an effective AML internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and engagement in AML is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance by setting the tone at the top, and ensuring that staff adheres to the policies, procedures and processes designed to limit and control risks.

V. INTERNAL COMPLIANCE EFFECTIVENESS REVIEW

18. INTERNAL COMPLIANCE REVIEWS

18.1 Dealer firms are required to perform and document an internal compliance effectiveness review (every two years at a minimum) the results of which should be accessible for review both by examining independent accountants and the Commission's Examiners.

18.2 The purpose of the effectiveness review is to assess the effectiveness of the compliance program. Accordingly, the firm must conduct a review of the policies and procedures, risk assessment, compliance training program and assess if they cover the current dealer requirements and guidelines. The effectiveness review must cover and test all obligations applicable to your sector. This can be a useful tool in apprising the Commission of any changes which may have occurred between examinations and demonstrate that deficiencies identified in the effectiveness review has been updated. Such changes may include number of facilities or transactions, risk assessment, size and complexity of the business, training program and verification of compliance with policies, procedures, and controls to mitigate identified risks. Larger dealer firms may wish to assign this role to their Internal Audit or Compliance Department. Smaller dealer firms may accomplish the same objective by **assigning the review to the compliance officer.**

18.3 Information Technology (IT) Infrastructure

18.3.1 Dealers are required to have policies in place and take such measures as may be needed to identify and assess the ML/TF risks that may arise in relation to:-

(a) the development of new products and new business practices, including new delivery mechanisms, and

(b) the use of new or developing technologies for both new and pre-existing products.

18.3.2 Dealers must undertake the risk assessments prior to the launch or use of such practices and technologies; and take appropriate measures to manage and mitigate the risks. Periodic reviews and updates of all technology must also be undertaken to ensure that Management Information Systems (MIS) are adequate and up-to-date to avoid penetration of ML/TF within the system.

18.3.3 The MIS is required to provide the company with timely information on a regular basis to enable the company to detect irregularity and/or any suspicious activity. The MIS shall be adequate, in that, it is commensurate with the nature, scale, and complexity of the dealer's activities and ML/TF risk profile.

18.3.4 It is worth noting that cyber- criminals are constantly working to find innovative and effective means to steal information, data and ultimately money by any means possible. Therefore, awareness of cyber-criminal threats and techniques are the best defence. Dealers in Precious Metals and Precious Stones should initiate an awareness program to ensure that their employees are trained and well informed to recognize when cyber criminals are conducting fraudulent transactions, downloading malware or compromising sensitive data. Some mitigating measures include:

(i) upgrade of IT systems periodically (as mentioned earlier) and put in place mechanism to avoid computer systems (email, email server, internet) from being compromised, intercepted or altered by cyber-criminals;

(ii) establish a sound and robust technology risk management framework;

(iii) strengthen system security, reliability, availability and recoverability; and

(iv) emphasize the benefit of using appropriate technologies and control mechanisms that protect customer data and transactions.

VI. RISK–BASED FRAMEWORK

19. Obligations under the Law to Develop a Risk-Based Framework

19.1 In recognition of The Bahamas National Risk Assessment (NRA), the direction of the country in its efforts to combating AML, the FATF standards of Recommendation and in keeping with international best practices, the Commission has adopted and implemented a risk-based AML/CFT supervisory regime. The primary goal is to ensure that dealers under the supervision of the Commission have adequate controls and resources in place to manage and mitigate the inherent risks identified.

19.1.1 Every financial institution pursuant to section 5 of the FTRA is required to:

- take appropriate measures to identify, assess and understand the identified or inherent risks in relation to its customer/clients and the countries or jurisdictions of their origin; the countries or jurisdictions of its operations; its products, transactions and delivery channels;
- develop and implement a comprehensive risk management system approved by the financial institution's senior management and commensurate with the scope of its activities, incorporating continuous identification, measurement, monitoring and controlling of identified risks;
- take appropriate measures to manage and mitigate the inherent risks identified;
- take account of any risk assessment carried out at a national level and any regulatory guidance issued by its Supervisory Authority; and
- upon request, provide the Supervisory Authority with a copy of its risk assessment.

19.1.2 Every financial institution shall carry out a risk assessment:

- prior to the launch of new business practices;
- prior to the use of new or developing technologies;

- when there is a major event or development in the management and operation of the group, to identify and assess the identified risks that may arise in relation to such products, business practices or technology for both new and pre-existing products and such assessment shall consider:

- the customer/client's geographic area, product, transaction and means of delivery risk factors, which shall be proportionate to the nature and size of the financial institution's business; and

- the outcome of any risk assessment carried out at a national level, and any regulatory guidance issued.

19.1.3 Every financial institution shall document in writing the outcome of a risk assessment and shall keep the same up to date and make it available to relevant competent authorities and regulatory bodies upon request.

19.1.4 Every dealer, regardless of its size and complexity is expected to develop and implement an adequate risk assessment and management system for AML. A risk assessment enables the company to focus its AML efforts and to adopt appropriate measures to optimally allocate the available resources. This process is necessary for managing the risks of ML/TF to which the company may be vulnerable. It involves the identification, analysis, management and mitigation of such risks, inclusive of the on-going monitoring of the risks.

19.1.5 Terrorism financing describes the activities that provide financial support to terrorists or terrorist organizations. The objective is to suppress terrorism by depleting the resources of the financers to the terrorist or terrorist cells. Unlike ML where the funding source is from illicit activities, TF can be derived from both legitimate (example, by individuals and organizations through donations and investment in legitimate businesses) and illegitimate sources. The global effort to curb TF, drove the terrorist to illegal sources through organized crime such as exploitation, trafficking, kidnapping etc. – which differs from the placement, layering and integration stages used in ML. However, both ML and TF threats seeks to exploit the same set of vulnerable features and characteristics of products offered by companies to launder proceeds of crime or fund terrorism. Therefore, the risk assessment related to money laundering is also applicable to terrorism financing.

Fig. 3 - OVERVIEW OF FIVE (5) STAGES OF A ML/TF RISK ASSESSMENT ROCESS[12]:

19.2 STAGE 1 - RISK IDENTIFICATION

19.2.1 In adherence to the obligations highlighted in 19.1.1 to 19.1.5 above, it is imperative that Dealers in Precious Metals and Precious Stones take the appropriate steps to identify, assess and understand the ML /TF inherent risks posed to the company via its clients, products; transactions, delivery channels and countries or geographical areas. Depending on the nature of the company's business the inherent risks categories may be expanded. The objective is to ensure that reasonable measures are taken to satisfy the company that all new and existing client relationships, products, activities and processes are properly

12 Refer to Appendix F for more reference reading on how to conduct a risk assessment.

assessed to determine the level of risk associated with all aspects of the business to avoid the company being used as a conduit for laundering or funding terrorism.

19.2.2 Proper scrutiny should be extended to the under-noted key factors:

- What is the size and nature of the business?
- Who is the beneficial owner(s)?
- What type of clients and products does the company have?
- Are funds derived from legitimate sources in every transaction?
- What kind of delivery channels are used for the products?
- What jurisdiction does the company operate from?

19.2.3 It is important to categorize the key risks and vulnerabilities based on the degree of money laundering and terrorist financing risks they pose to the company. The type of inherent risks and vulnerabilities should be documented and placed in the company's policies and procedures manual. Further the type, volume and value of the transactions should also be documented along with the control measures. Dealers in Precious Metals and Precious Stones should ensure that they are satisfied with the following details for the various categories of inherent risk indicators outlined below to be able to make a determination regarding the AML risks each pose. This is not an exhaustive list and should only be used as a guide:

Risk Categories	Risk Indicators
Business Operation	• Is the operating structure complex? • Is it integrated with other sectors, plus the scope and accessibility of the operation? • Does the company have a comprehensive risk management system approved by senior management and commensurate with the scope of its activities, incorporating continuous identification, measurement, monitoring and controlling of identified risks? • Does the company have effective policies, procedures and systems in place to mitigate inherent risks? • Does the company take measures to manage and mitigate the inherent risks?

	• Does the company take account of any risk assessment carried out at a national level and any regulatory guidance issued by the Commission?
The Client	• Is the client a Politically Exposed Person (PEP)? • Is the client a cash intensive business (i.e., money service business, casinos or money transfer agents etc.)? • Is it difficult to determine the beneficial owner or hard to determine the legal persons? • Is there public (verifiable and open source) information that is adverse - that associates the client with any known money laundering, terrorist financing and proliferation financing activities? • Is the client's occupation or business activities commonly linked to money laundering or terrorist financing activities? • Does the client use intermediaries that are not subject to adequate AML/CFT laws and measures? • Does the client change settlement or execution instructions without appropriate explanation?
Products	• Do the products provided to the client offer the anonymity and movement of funds commonly linked to money laundering and terrorist financing activities? • What is the nature of the products and the extent of their vulnerability? • Are the products offered deemed high risk by the Commission or other credible sources like the IMF or WB?
Transactions	• Are there large volumes of transactions with high risk clients and businesses? • Are there frequent movement of funds to or from high risk countries? • Does the company engage in high volume of cash transactions?

Delivery Channels	• Are the delivery channels complex? • Are the delivery channels face-to-face, via a third party, electronic devices, postal mail, telephone, fax or email?
Geographical Reach	• Does the client's jurisdiction apply globally acceptable AML standards or is the jurisdiction identified as being commonly linked to money laundering or terrorist financing activities by the Bahamas or other credible sources like the IMF, FATF, World Bank? • What is the exposure to high risk jurisdictions and other locations of concern? • Is the jurisdiction subject to sanctions, embargoes or similar measures issued by the United Nations? • Is dictatorship promoted whereby the rule of law is at the mercy of the dictator? • Is the client jurisdiction identified by credible sources as having significant levels of corruption or other criminal activity?

19.3 STAGE 2 - RISK ANALYSIS

19.3.1 Once the company has identified the areas of the business operations that are susceptible to ML/TF, it is imperative to conduct an analysis in order to assess the likelihood of the occurrence of risk events and impact of ML/TF risks. An effective process of ML/TF risk analysis serves as a basis for establishing an adequate system of risk management and control, and consequently, for reaching the ultimate goal of minimising possible adverse effects arising from that risk.

19.3.2 The likelihood of occurrence is a combination of threat and vulnerability, or in other words, risk events occur when a threat exploits vulnerability. For example:

Fig. 4 Risk Analysis (Likehood & Impact)

19.3.3 The level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their impact. Please refer to section 11 above which highlights some of the vulnerabilities of the Dealers in Precious Metals and Precious Stones. It should be noted that this is not an exhaustive list. Every segment of the business operations where ML/TF threats and vulnerabilities to those threats may emerge must be analysed continuously to determine the exposure to ML/TF and to ensure that same is properly managed.

19.4 STAGE 3 - RISK MATRIX

19.4.1 As it is required by law for every FI and DNFBPs to conduct a risk assessment as outlined above in sections 19.1.1 to 19.1.4, the company should establish whether all identified categories of risks pose a low, medium or high risk to the business operations. The company must review different factors such as the establishment and maintenance of a client relationship, number and scope of transactions, geographical location and nature of the business relationship etc. At the beginning of any client relationship, a risk rating designation should be determined, based on the information contained in the client profile and relationship documentation. Hence, companies should develop a risk matrix to:

- ascertain which inherent risk factors (all identified categories of risks) pose a low, medium or high ML/TF risks;
- establish whether the delivery channels pose an additional higher ML/TF risk factor; and
- establish whether the country risk is an overall higher ML/TF risk factor.

The matrix should also include all other risk factors identified.

19.4.2 The timing to review the risk rating should be predicated on the overall/composite risk rating (for example, high risk to be reassessed every twelve (12) months, medium every eighteen (18) months and low risk every twenty-four (24) months).

19.4.3 The criteria for the risk designation should be reviewed by the Compliance Officer annually, as part of the company's annual risk assessment.

19.4.4 LEVEL OF ML/TF RISK RATING

The level of ML/TF risk will generally be affected by both internal and external factors. For example, internal risk factors may increase due to inadequate compliance resources, weak risk controls and insufficient senior management involvement. External level risks may rise due to factors such as the action of third parties and/or political and public developments.

Fig. 5 – THE RATING BELOW SIGNIFIES THE LEVEL OF SUSCEPTIBILITY TO ML/TF RISK.

The Level of Susceptibility to ML/TF Risk	Definition / Likelihood
HIGH (Almost Certain)	Probably occurs several times per year. Assessment on the risk factors indicates that the company is highly vulnerable and there is a high chance of ML/TF occurring in this area of business operations.
MEDIUM (Possible)	Probably occurs once per year. Assessment on the risk factor indicates that the company is moderately/fairly vulnerable and there is a possibility of ML/TF occurring in this area of business operations.
LOW (Unlikely)	Unlikely to occur but not impossible. Assessment on the risk factor indicates that the company is less vulnerable and there is a low chance of ML/TF occurring in this area of business operations.

19.4.6. The Commission requires dealers, at a minimum, to place clients, products, transactions, delivery channels and client geographical location into one of three risk categories i.e., Low Risk, Medium Risk or High Risk[13]

19.5 STAGE 4 - RISK MANAGEMENT/CONTROL & MITIGATION

19.5.1 Based on the analysis, the company should set the overall AML/CFT strategy and ensure that it concurs with the risk appetite and risk culture. Dealers shall develop adequate

13 It should be noted that the number of risk categories, i.e. three (3), required by the Commission is a minimum number. Some financial institutions may have more categories, but the rationale for the number of categories and the criteria for each should be clearly documented and available for review during the course of an examination.

policies and procedures to control and mitigate the ML/TF risks that have been identified.

19.5.2 The risk control and mitigation shall be tailored according to the identified ML/TF risk level and seek to:

- Ensure that management clearly promotes the AML strategy and sets the tone at the top;
- Develop an AML policy, procedures and mitigating measures;
- Determine which measures will be taken for which risk categories;
- Ensure that management sets transaction limit for higher risk customer/transaction;
- Ensure sufficient training in AML policies and procedures for staff; and
- Provide appropriate tools and adequate resources to implement the AML systems.

19.5.3 An adequate system of ML/TF risk management should include:

- A risk assessment of ML/TF risks of the business;
- Policies and procedures to control ML/TF risks;
- An organizational structure to execute these risk management controls; and
- A process to systematically check and assess the adequacy of the control systems.

19.5.4 Adequate and effective risk mitigation strategies should be designed, developed and implemented to lessen or reduce, if not totally eliminate, the adverse impact of the known or perceived risks inherent in a particular undertaking before any damage or disaster takes place. Senior management's ability and willingness to take necessary corrective action is also a critical determining factor to this process of mitigating the adverse risks. Mitigation plans should be documented.

19.5.5 Companies must also ensure that their procedures include mechanisms for appropriate **risk mitigation** which involves identifying and applying client due diligence/KYC policies and procedures to effectively mitigate the money laundering risk of particular clients and products identified during the risk assessment process.

19.5.6 The company should document the risks assessment, consider all relevant risk factors to determine the level of risk and the appropriate type of mitigation plan to be applied, update risks assessments and to have in place mechanisms to provide information to relevant competent authorities. A senior officer should be responsible for documenting all risks

assessments of the dealer and the assessments should be kept in such a way that it is stored on microfiche, computer disk or in other electronic form.

19.5.7 This process includes being able to:

(a) Document the outcome of the company's risks assessments;
(b) Consider all the relevant risk factors before determining what is the level of overall risks and the appropriate level and type of mitigation to be applied;
(c) Keep these assessments up to date; and
(d) Have appropriate mechanisms to provide risk assessment information to competent authorities and self-regulatory bodies upon request.

19.6 STAGE 5 - RISK MONITORING AND REVIEW

19.6.1 Management should adequately and effectively manage ML/TF risks, to verify the level of implementation and effective functioning of the ML/FT risk controls, and to determine whether the risk management measures correspond to the company's risk analysis. The company should set up compliance monitoring and audit program, which should encompass regular testing to ensure that procedures and measures are working correctly and the production of compliance and audit reports. Monitoring should be on-going as the risks may change significantly at any time and to the extent that the mitigation strategies become ineffective and require revision. Monitoring should be a standard part of the management review program.

19.6.2 Senior management of the company should ensure the allocation of adequate resources, taking into account the risks posed to the company. It should establish an appropriate and continuing process for monitoring the risks, in particular, those activities assessed to be of a higher risk of ML/TF.

VII. CLIENT IDENTIFICATION/VERIFICATION (KYC) [14] PROCEDURES

20. VERIFICATION DETAILS AND DOCUMENTARY EVIDENCE PROCEDURES

20.1.1 Dealers have a statutory obligation to undertake customer due diligence measures when establishing a business relationship with a customer/client. The true identity of each client and beneficial owner must be determined. A summary of the identification and verification triggers required by the law include (Please refer FTRA sections 6-9, 11-14):

- where a customer/client seeks to conduct a transaction involving $15,000 or more either for himself or on someone else's behalf.

20.2 Verification of identity of individuals

20.2.1 Where a dealer is required to verify the identity of any individual pursuant to section 7 of the FTRA the following information is required:-

- the full, correct and legal name of the individual;
- contact information[15] and;
- date and place of birth.

20.2.2 In addition to the requirements above, the following information and documentation may be required (based on the company's risk-rating procedures) to verify the identity of an individual:-

- evidence of the source of funds and source of wealth;
- a specimen signature;
- telephone and fax number, if any;
- occupation, name of employer, and where self-employed, the nature of

[14] " KYC" is the shortened form for "know your customer" or "know your client". In the AML realm, this, knowing your customer, is achieved through the process of conducting a due diligence exercise to gather, verify and assess pertinent information on the client.

15 Points of contact may include - mobile phone number, business mobile phone, personal landline number, personal mailing address, business mailing address, residential mailing address and any other means of contact that the Commission may specify.

the self-employment; or

- a copy of the relevant identification pages of the passport; a driver's license; a voter's card; national identity card; or such other identification document bearing a photographic likeness of the individual as is reasonably capable of establishing the identity of the individual.

20.3 Verification of corporate entity

20.3.1 Where a dealer is required to verify the existence of a corporate entity, the dealer must require the corporate entity to submit the under-noted documents:-

a) a certified copy of the Certificate of Incorporation;

b) a certified copy of the Memorandum of Association and Articles of Association[16] of the entity;

c) a certified copy of the resolution of the Board of Directors of the corporate entity authorizing the opening of the account and conferring authority on the natural person who will conduct the transaction;

d) documentary evidence as is required under regulation 6 of the FTRR for the verification of the natural person who will conduct the transaction;

e) documentary evidence to satisfy the requirements for the identification and verification of the identity of all beneficial owners of the corporate entity. The obligation to verify the identity of beneficial owners shall only extend to those with at least 10% or more controlling interest in the corporate entity. Further, to the extent that there is doubt under the above obligation as to whether the person with the controlling interest is the beneficial owner or where no natural person exerts control via ownership interest, the identity of the natural person, if any, exercising control of the legal person or arrangement via other means; or where no natural person is identified above, the identity of the relevant natural person who holds the position of senior managing official shall be obtained;

16 In the case of a Bahamian incorporated company, if the law company has, as part of the files, the documents of incorporation (e.g. certificate, Memorandum and Articles of Association) bearing an original seal of the Registrar General this would be sufficient to meet this obligation.

f) a certificate of good standing; the location of the registered office and if different, the location of the principal place of business;

g) a description of the nature of the business, including the date of commencement of the business,

h) a description of the products provided by the business and the location/address of principal business; and

i) such other official documentary and other information as is reasonably capable of establishing information on the client's ownership and control structural of the corporate entity.

20.3.2 In addition to the requirements above, the following information and documents may also be relied upon to support verification of a corporate entity:

- the names and addresses of all officers and directors of the corporate entity;
- the purpose of the transaction; and
- the potential parameters of the transaction.

20.4 ASCERTAIN CUSTOMER IDENTITY – KNOW YOUR CUSTOMER

20.4.1 If you cannot satisfactorily apply your due diligence measures in relation to a Customer, e.g., you are unable to identify and verify a Customer's identity or obtain sufficient information about the nature and purpose of a transaction, you must **NOT** carry out a transaction for that Customer or enter into a business relationship with the Customer and you must terminate any business relationship already established. You should also consider submitting a STR/SAR to the FIU.

a) All Customers

You must **identify** who is the prospective customer and **verify** the person's identity by reference to independent and reliable source materials. Such material should include documentary identification issued by the Government departments or agencies. You must also ask the source of funds for the transaction. Customer's identification, also called CDD or Know Your Customer–KYC, must be obtained for customers who are individuals as well as companies. You must obtain satisfactory evidence of the Customer's identity before establishing a business relationship or completing a transaction for occasional customers.

b) High Risk Customers/Transactions

There are customers and types of transactions and products which may pose higher risk to your business and you are required to take additional measures in those cases. The AML/CFT laws have identified certain high risks customers and require you to conduct Enhanced Due Diligence ("EDD") on these customers. You may also determine that certain customers, transactions and products pose a higher risk to your business and apply EDD. You must take specific measures to identify and verify the identity of the following individuals or entities:

i. Any individual or entity who conducts business transactions with persons and financial institutions in or from other countries which do not or which insufficiently comply with the recommendations of the Financial Action Task Force ("the FATF");
ii. Any individual or entity who conducts a complex or unusual transaction, (whether completed or not), unusual patterns of transactions and insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
iii. Domestic and Foreign Politically Exposed Persons (PEPs) who are PEPs (Foreign PEPs are always considered high risk);
iv. Any individual or entity for whom you have to send a suspicious transaction report to the FIU (reasonable measures and exceptions apply e.g., to avoid tipping-off);
v. Any customer or transaction, product type that you have identified as posing a higher risk to your business; e.g. pawn-broking transactions, transactions over $15,000.00.

20.5 Politically Exposed Persons (PEPs)

20.5.1 Caution must be taken when dealing with PEPs; a special category of High-Risk clients[17]. At the out-set of the client/business relationship, the company should:

- Identify all PEPs within the client data base;
- Identify the Country that each PEP is associated;
- Determine the type of PEP (i.e., foreign, domestic or person entrusted with a prominent function by an international organization);
- Identify the type of business, industry, personal financial situation of each PEP;
- Identify each PEPs affiliation, employment, association, etc;
- Develop a profile of each PEPs transactions;
- Determine each PEPs expected vs actual transactions; and
- Identify and investigate transactions that are outside the norm, or which are high risk.

20.5.2 Dealers are cautioned that PEPs may expose their businesses to significant risks. These risks, whether reputational, legal etc. can be extremely detrimental and costly. Such incidences usually occur when these persons abuse their public office. Hence, systems should be in place to ensure ongoing monitoring of PEPs. Due to the continual evolution of the sanctions lists and PEPs databases (additions as well as deletions), these lists should be consulted as a part of the company's on-going monitoring of its clients.

21. SIMPLIFIED DUE DILIGENCE PROCESS

21.1 What is Simplified Due Diligence?

21.1.1 Simplified measures are appropriate in situations where low risk is established. This depends on the type of customer, country or geographic area or products, services, transactions or delivery channels.

21.1.2 Simplified or reduced customer due diligence is the lowest form of due diligence and does not go beyond the identification of the client. Simplified CDD is reserved for those instances where the customer, product/services combination falls into the lowest risk category where there is little opportunity or risk of ML/TF. This would not include an instance where there is a beneficial owner involved (where there is someone acting for

[17] Refer to Appendix F for FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22).

another, there is an element of risk involved and at the very least Standard CDD should be employed). Continued monitoring is required to determine when trigger events occur that may require further due diligence at a future date.

21.1.3 Simplified or reduced customer due diligence is also subject to, in all cases, the overriding statutory obligation[18] to carry out verification in any situation where the law firm suspects that a transaction involves the proceeds of criminal conduct or is destined for financing terrorist activities. Simplified or reduced due diligence means that the obligation to obtain the full complement of documentary evidence normally required is relaxed. The low risks due diligence procedures, should at a minimum, be consistent with the low risks identified by the National Risk Assessment (NRA).

Examples of customer types where Simplified Due Diligence may be applied:

(i) professions subject to requirements to combat ML and TF consistent with FATF recommendations;

(ii) financial institutions/DNFBPs supervised by the CC;

(iii) public administrations or enterprises;

(iv) public companies listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership;

(v) countries identified by credible sources (such as mutual evaluations or detailed assessment reports) as having effective AML/CFT systems as having a low level of corruption or other criminal activity

Examples of Countries which applied Simplified Due Diligence:

(i) **Guatemala – Small account threshold based on an average income analysis**

In 2011, Guatemala conducted an income analysis based on the monthly minimum wage in the country, which was approx. 273, 44 USD, and the average remittances received on a monthly basis (according to the International Organization of Migration) which was 283, 74 USD (total monthly income of 584, 4 USD). Guatemala worked on the assumption that a family receives remittances and a salary on a monthly basis, or two minimum wages per month for their subsistence. On this basis, households with an average monthly income of less than 625 USD can benefit from simplified CDD measures.

[18] Section 8, FTRA

(ii) **Peru – Simplified CDD measures based on a specific authorisation of the supervisor**

In 2015, the financial supervisor of Peru (SBS) issued a revised general AML/CFT regulation that enables financial institutions to apply simplified CDD measures, based on an authorization granted by the SBS for a specific product or service. When the SBS authorization is granted, financial institutions only have to collect the full name, type and number of ID document of the customer, and the verification is done though the National ID or International ID (for foreigners). In the standard regime, customers would also be requested to provide information on their nationality and residence, phone number and/or e-mail address, occupation and name of employer[19].

21.2 When must Simplified Due Diligence be carried out?

21.2.1 Where the risks identified are low, the law firm shall conduct simplified due diligence measures unless there is a suspicion of activities related to any identified risks in which case enhanced customer due diligence measures shall be undertaken.

21.2.2 The procedures require a law firm to establish to its satisfaction that it is dealing with a legitimate person (natural, corporate or legal) and verify the identity of those persons who have authority to conduct business through any facility provided. Whenever possible, the prospective client should be interviewed personally.

21.2.3 Ultimately, simplified due diligence procedures should ensure that the firm is satisfied with the identity and existence of the client; that the proper authorisations exist for the prescribed financial services being sought by the customer/client, including that the person seeking to conduct the affairs of the entity, in a relevant case, is duly authorised to do so.

21.3 Additional guidance on due diligence for regulated financial institution clients to which simplified due diligence may be applied:

21.3.1 For regulated financial institutions (both local and foreign), it is recommended that the confirmation of their existence and regulated status be checked by the following means:

- checking with the relevant regulator or supervisory body;
- checking with another office, subsidiary or branch in the same country;

[19] Source: FATF Guidance – Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence, November, 2017.

- checking with a regulated bank of the institution if it is an overseas institution; and
- obtaining from the relevant institution evidence of its licence and its authorization to conduct business with the firm.

21.3.2 In addition, the firm is required to satisfy itself that the regulated financial institution is subject to AML supervision that is equivalent to or exceeds standards under Bahamian law.

21.3.3 **N.B. Where simplified due diligence is applied to satisfy record-keeping obligations, the file should contain adequate documentation including, in appropriate cases, a copy of the relevant certificate or license or such similar document that supports the application of simplified due diligence, as well as other relevant copies of substantiating evidence.**

21.4. **Special circumstances where simplified due diligence may be applied in the case of a previous or existing client:**

21.4.1 There are two circumstances in which a firm may apply simplified or reduced due diligence procedures for a client who would otherwise be subject to full due diligence. This is where the firm may already have the necessary information on file. The two circumstances are:

(1) where the firm has reasonable grounds to believe that in relation to a particular client, the verification information/details/ documentation which it has obtained on an earlier occasion is still reasonably capable of establishing the identity of that client; and

(2) where the client is an existing one, who closes a facility and then establishes another with the firm, in which case the existing records may be transferred to the new facility.

21.4.2 **N.B. However, the opportunity should be taken to confirm the relevant customer verification information. This is particularly important where there has been no recent contact or communication with the client or when a previously dormant facility is being reactivated**.

21.4.3 **Standard Customer Due Diligence** occurs in those general situations where there is the potential risk, but it is unlikely that the risks will be materialized. In addition to the identification and verification process, the firm needs to gather additional information to understand the nature of the business relationship; check references; based on the purpose of the account, gather relevant information; inquire behind information, if there is

a suspicion that it is inaccurate etc. Continued monitoring is required to determine when trigger events occur that may require further due diligence at a future date.

22. ENHANCED DUE DILIGENCE PROCESS

22. What is Enhanced Due Diligence?

22.1.1 Enhanced due diligence (EDD) is an in-depth and extensive investigation of a client's particular characteristics, risk factors and other available information and documentation. EDD procedures must be considered for clients designated as high risk, politically exposed persons (PEPs), cash intensive business and trusts, charities and complex organizations. EDD should be conducted on clients deemed to pose high risks for money laundering, terrorist financing and the financing of proliferation. EDD records/files or alerted transactions are subject to a higher, more frequent level of scrutiny.

22.1.2 New or existing clients that pose higher money laundering or terrorist financing risks tend to increase the overall risk profile to the financial institution. To this end, it is imperative that the financial institution mitigate and manage these risks. As such, the company must have well-defined escalation and EDD processes and procedures in place.

22.1.3 EDD measures to apply to high risk customers include but is not limited to:

- Verification of identity using independent sources e.g., additional form of Government issued identification;
- Obtaining details of the source of the customer's funds and the purpose of the transaction;
- Obtaining approval from the senior officer to conduct the transaction;
- Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;
- Imposing a cash threshold limit for transactions after which a senior officer's approval is needed to conduct the transaction;
- Verifying the source of funds for the transaction e.g., if Customer states the money is from his bank account, ask for proof.
- Ongoing monitoring (e.g., monthly, quarterly or on a transaction basis) of the Customer's account through the relationship; or
- Obtaining details about the source of items in pawn-broking transactions.

22.2 When must EDD be carried out?

22.2.1 EDD is required where the customer and product/service combination are considered a much greater/high risk. The EDD, as a higher level of due diligence, is required to mitigate the increased risk (i.e. increased opportunity for ML/TF through the service/product the firm is providing the client). The EDD procedure is not one size fit all, instead, it depends on the nature and severity of the risks. As such, the additional due diligence can take many forms including additional information to verify the client's identity; source of income; adverse media check etc. The additional checks are proportionate and relative to the risks identified. If it is an existing client and adverse information makes it way to the firm, sometimes it may even take investigative services to ascertain its credibility and inform the firm's decision on the next steps/appropriate action. EDD is a risk mitigating/risk management tool. There are a number of situations that can give rise to increased risks (for example, not meeting clients face to face; dealing with a PEP; offering Trust services etc.).

22.2.2 Dealers should apply enhanced due diligence measures to business relationships and transactions with natural and legal persons and financial institutions from countries which FATF stipulates as high-risk countries. The type of enhanced due diligence applied should be effective and proportionate to the risks. Information regarding advice and concerns about weaknesses in the AML systems of other countries may be obtained from the FATF website.[20]

23. Is the Customer acting for a Third Party?

23.1 You must take reasonable measures to determine whether the Customer is acting on behalf of a third party especially where you have to conduct EDD. Such cases will include where the Customer is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, you must obtain information on the identity of the third party and their relationship with the Customer.

In deciding who the beneficial owner is in relation to a Customer who is not a private individual, (e.g., a company) you should identify those who has ultimate control over the business and the company's assets such as the shareholders.

Particular care should be taken to ensure that any person purporting to act on behalf of the company is fully authorized to do so.

20 www.fatf-gafi.org/publ.

24. OUTSOURCING OF MATERIAL FUNCTIONS

24.1 The Commission is aware that the size, nature, complexity and resources of various dealers may warrant the need to outsource certain material functions of the company. While AML compliance functions may be performed by third parties, the ultimate responsibility for complying with AML, CDD or EDD rest with the company.

24.2 Dealers in Precious Metals and Precious Stones must ensure that the outsourcing agreement is in writing and signed off by all considered parties. The outsourcing agreement with a third party should be reviewed and updated as necessary to ensure that it continues to address accurately the outsourced function and the role of the third party to whom the outsourced function has been designated.

24.3 Specific task such as the Compliance function may be outsourced, but they must remain subject to appropriate oversight by the Head of Compliance and/or the Compliance Committee. Dealers in Precious Metals and Precious Stones should ensure that any arrangements of an outsourced function do not impede the effective on-site examination by the Commission or its representative. Regardless of the extent to which specific tasks of the compliance function are outsourced, senior management remains responsible for full compliance with all AML laws, guidelines and regulations. The outsourced functions should also remain within the jurisdiction.

VIII. INFORMATION SHARING

25 Group Level Information Sharing

25.1 From a regulatory perspective, while there are international requirements and obligations for mutual legal assistance and international co-operation vis-à-vis the exchange of information in keeping with Recommendations 37 - 40, the Commission executes its obligations while being cognizant of its powers, and commitment in accordance with the laws of The Bahamas.

25.2 From a dealer's perspective, branches should be required to implement company-wide

programmes against ML/TF, which should be applicable, and appropriate to, all branches. These should include the measures taken against ML/TF risks already established in these Codes, in addition to the under-noted measures:

(i) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(ii) the provision, at company-wide compliance, audit, and/or AML functions, of customer, account, and transaction information from branches when necessary for AML purposes; and

(iii) adequate safeguards on the confidentiality and use of information exchanged.

25.3 Dealers are required to ensure that their foreign branches apply adequate AML measures consistent with home country requirements where the minimum AML requirements of the host country are less strict than those of the home country, to the extent that the host country laws and regulations permit. If the host country does not permit the proper implementation of AML measures consistent with the home country requirements, companies should be required to apply appropriate additional measures to manage the ML/TF risks and inform their home supervisors.

IX. COMBATING THE FINANCING OF TERRORISM & PROLIFERATION

26. Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

26.1 FATF Interpretive Note to Recommendation 6.6 (c) stipulates that countries should have mechanisms for communicating designations to financial institutions and DNFBPs – immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms. To this end, the Commission, following the procedures established in law, reference section 2.3 of this Code, will notify its registrants immediately upon any such actions being taken from a national perspective. Further, FATF Interpretive Note to Recommendation 6.6 (d) states that financial institutions, including DNFBPs, are required to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure effective utilization of the information by the competent authorities. Dealers are advised to take note of FATF Recommendations 27 and 35.

26.2 Targeted Financial Sanctions Related to Proliferation

26.2.1 FATF Interpretive Note to Recommendation 7.1 requires countries to implement targeted financial sanctions to comply with the UNSC resolutions that requires countries to freeze, without delay, the funds or other assets of, as well as to ensure that no funds and other assets are made available to, and for the benefit of, any person or entity designated by the UNSC under Chapter VII. This is in accordance with the Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of mass destruction.

26.2.2 The Bahamas, in order to discharge its responsibilities in keeping with FATF Interpretive Note to Recommendation 7.1, depends on financial institutions that come in contact with clients or funds (including attempted transactions) suspected or linked to proliferation financing, to report to the competent authorities, without delay, actions taken or funds frozen in compliance with the prohibition requirements of the relevant UN Security Council resolutions. This will facilitate and ensure timely and effective utilization of the information by the competent authorities Reference section 3 of this Code).

X. RECORD KEEPING PROCEDURES

27. Statutory requirements to maintain records

27.1 Dealers shall maintain all books and records[21] concerning customer identification and transactions for use as evidence in any investigation into AML. This is an essential component of the audit trail procedures. Often, the only significant role a financial institution can play in an investigation is through the provision of relevant records, particularly where the money launderer or person financing terrorism or proliferation has used a complex web of transactions, specifically for the purpose of confusing the audit trail. The objective of the statutory requirements detailed in the following paragraphs is to ensure that the dealer can, as part of its audit trail, provide the authorities with such records and supporting information on a timely basis when required to be disclosed by law.

27.1.2 Where an obligation exists to keep records, copies of the relevant documentation are sufficient, unless the law specifically requires otherwise. It is important that the dealer satisfies itself that copies are reproductions of the original documentation. The files should also indicate, in relevant circumstances, where the original can be located.

27.1.3 The records prepared and maintained by any dealer on its customer relationships and transactions should be such that:

- requirements of legislation are fully met;
- competent third parties will be able to assess the company's observance of AML policies and procedures;
- any transactions effected via the company can be reconstructed; and
- the company can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities for disclosure of relevant information.

[21] See sections 15-18 of the FTRA with regards to Record Keeping.

27.2 Retention period to maintain verification records

27.2.1 Records relating to the verification of the identity of customer/client, including account files, business correspondence, and copies of all documents evidencing the identity of customer/client and beneficial owners, and the results of any analysis undertaken in accordance with the provisions of the FTRA, all of which shall be maintained for a period of five (5) years after the person ceases to be a client. In keeping with best practices, the date when a person ceases to be a customer/client is the date of:

i) the carrying out of a one-off transaction or the last in the series of transactions; or
ii) the ending of the business relationship, i.e. the closing of an account; or
iii) the commencement of proceedings to recover debts payable on insolvency.

27.2.2 Where formalities to end a business relationship have not been undertaken, but a period of five (5) years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction.

27.3 Transaction records

27.3.1 Records of transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holder, shall be maintained for a period of not less than five (5) years from the date of the transaction.

27.3.2 Records of any findings pursuant to section 15 of the FTRA and related transaction information shall be maintained for at least five years from the date of the transaction.

27.3.3 Records relating to on-going investigations, must be retained until it is confirmed by the FIU or local law enforcement agency that the case has been closed.

27.3.4 The investigating authorities also need to be able to establish a financial profile of any suspect transaction. For example, in addition to information on the beneficial owner of the transaction and any intermediaries involved, the volume of funds may be sought also as part of an investigation into money laundering or terrorist financing. Further, in the case of

selected transactions, information may be required on the origin of the funds (if known); the form in which the funds were offered or withdrawn, i.e. cash, cheques, etc., the identity of the person undertaking the transaction, the destination of the funds, and the form of instruction and authority.

27.3.5 The transaction records which must be kept must include the following information:

- the nature of the transaction;
- the amount of the transaction, and the currency in which it was denominated;
- the date on which the transaction was conducted;
- the parties to the transaction; and
- all other files and business correspondence and records connected to the transaction.

27.4 Format of records

27.4.1 Retention of verification and transaction records may be by way of original documents, or copied, stored on microfiche, computer disk or in other electronic form in keeping with the evolution of technology. Records required to be kept by the dealers pursuant to section 15 of the FTRA, shall be in written form in the English language, or in a form readily accessible and convertible in written form in the English language.

27.5 When records are not required to be kept

27.5.1 Special considerations for record retention on the liquidation of a financial institution.

27.5.2 Where a financial institution enters liquidation, the liquidator of the financial institution shall maintain for five (5) years from the date of the dissolution, such records that would otherwise have been required to be kept by the financial institution but for the liquidation.

27.6 Mandatory destruction of records

27.6.1 Books and records and any copies thereof, pursuant to section 15(2) of the FTRA shall be maintained for not less than five (5) years after the business relationship has ended. Notwithstanding this requirement, such records pursuant to section 17 of the FTRA shall

be destroyed as soon as practicable after the expiration of the retention period, unless required to be maintained beyond this period by any other written law, for the business purposes of the dealer, or for the detection, investigation or prosecution of any offence.

27.7 Record keeping offences

27.7.1 Dealers in contravention of section 15 of the FTRA, without reasonable excuse, to retain or properly keep records, commits an offence under section 18 of the FTRA. As such, dealers will be liable on summary conviction to a fine not exceeding twenty (20) thousand dollars in the case of an individual and one hundred (100) thousand dollars in the case of a body corporate.

XI. PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

28 THE FINANCIAL INTELLIGENCE UNIT (FIU)

28.1 The national agency for receiving suspicious transaction reports (STRs) is the Financial Intelligence Unit.

28.1.2 The FIU has power to compel production of information (except information subject to legal professional privilege), which it considers relevant to fulfill its functions.

28.1.3 It is an offence to fail or refuse to provide the information requested by the FIU. Such offence is punishable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 2 years or to both such fine and imprisonment.

28.1.4 The FIU is empowered by the FIUA to issue Guidelines, from time to time to assist financial institutions with observance and implementation of STR procedures. Copies of these Guidelines, which supplement and add to these Codes, are available from the FIU's office and electronically from the FIU's website.

28.2 Mandatory requirement to appoint a Money Laundering Reporting Officer

28.2.1 All dealers engaged in prescribed financial services are required by law[22] to appoint a Money Laundering Reporting Officer (MLRO) as a point of contact with the FIU, to handle reports of money laundering suspicions by their staff. DPMS are instructed to pay close attention to the criteria outlined in these Codes when appointing the individual to hold the position of MLRO of the company.

28.3 The MLRO must be registered with the FIU, copy the Commission on the application to the FIU to register the MLRO. Dealers should ensure that any changes in this post are immediately communicated to the FIU and the Commission.

[22] Reg. 5 of the FI(TR)R

28.3.1 The Role of the MLRO

The person appointed as the MLRO has significant responsibility to the company and should be sufficiently senior to exercise the necessary authority, competent and familiar with statue laws governing the company. The size and nature of the company should be a determining factor in selecting the individual to hold the position. Larger companies may choose to appoint, as appropriate to the circumstances, a senior member of their compliance department. In small companies, it may be appropriate to designate the sole practitioner or one of the partners. When several subsidiaries operate closely together within a group, designating a single MLRO at group level is an option.

28.3.2 The MLRO should exercise independence when determining whether the information or other matters contained in the transaction report he/she has received, give rise to a knowledge or suspicion that someone is engaged in money laundering, terrorist and/or proliferation financing.

28.3.3 In making this judgment, the MLRO should consider all other relevant information available within the dealer concerning the person or business to whom the initial report relates. This may include a review of other transaction patterns and volumes through the account(s) in the same name, the length of the business relationship, and referral to identification records held. If, after completing this review, he decides that the initial report gives rise to a knowledge or suspicion of money laundering, then he must disclose this information to the FIU. It is therefore imperative that the MLRO be granted timely access to customer verification and related due diligence information, transaction records and other relevant information.

28.3.4 The “determination” by the MLRO implies a process with at least some formality attached to it, however minimal that formality might be. It does not necessarily imply that he must give his reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for his own protection, for internal procedures to require that only written reports are submitted to him and that he should record his determination in writing, and the underlying reasons therefore.

28.3.5 The MLRO will be expected to act honestly and reasonably and to make his determinations in good faith.

28.4 Mandatory requirement to appoint a Compliance Officer

28.4.1 However, the firm may choose to combine the roles of the CO with the MLRO depending upon the size and nature of prescribed financial services that it is involved in.

28.4.2 You must appoint a senior employee at managerial level as Compliance Officer (CO). The individual you appoint will be responsible for the implementation of your compliance regime.

28.4.3 If you are a small business, employing five (5) persons or less, the CO must be the person in the most senior position. If you are the owner or operator of the business and do not employ anyone, you can appoint yourself as CO to implement a compliance regime.

28.4.4 In the case of a large business (employing over five [5] persons), the CO should be from senior management and have direct access to senior management and the board of directors.
Further, as a good governance practice, the appointed CO in a large business should not be directly involved in the receipt, transfer or payment of funds.

28.4.5 Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. The CO must:

a) have full responsibility for overseeing, developing, updating and enforcing the AML/CFT Programme;
b) have sufficient authority to oversee, develop, update and enforce AML/CFT policies and procedures throughout the company; and
c) be competent and knowledgeable regarding money laundering issues and risks and the anti-money laundering legal framework.

28.4.6 Depending on your type of business, your CO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator of the business. The identity of the CO must be treated with the strictest confidence by you and your staff.

28.4.7 The CO's responsibilities include:

i. Submitting STRs/SARs and TFRs to the FIU and keeping relevant records;
ii. Acting as Liaison officer between your business and the FIU;

iii. Implementing your AML Compliance Programme;
iv. Directing and enforcing your AML Compliance Programme;
v. Ensuring the training of employees on the AML/CFT; and
vi. Ensuring independent audits of your AML Compliance Programme.

28.4.8 For consistency and on-going attention to the compliance regime, your appointed CO may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the CO retains full responsibility for the implementation of the compliance regime.

28.4.9 Best practice: You should appoint an alternate CO to perform the CO's functions in the event the CO is absent for any reason. You will need to obtain the FIU's approval for the person to act as alternate CO.

28.5 Recognition of Suspicious Transactions

28.5.1 A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual. Efforts to recognize suspicious circumstances should commence with the request to execute the initial transaction.

28.5.2 Under the FTRA section 25 where any person conducts or seeks to conduct any transaction by, through or with a financial institution (whether or not the transaction or proposed transaction involves cash), and the financial institution knows, suspects or has reasonable grounds to suspect that the transaction or the proposed transaction involves proceeds of criminal conduct as defined in the POCA, or any offence under the POCA, the financial institution MLRO shall, as soon as practical after forming that suspicion, report that transaction or proposed transaction to the FIU.

28.5.3 Whistleblowing is an important mechanism in the prevention and detection of improper conduct, fraud and corruption. The company should implement an appropriate policy, which shall raise awareness of the whistleblowing process and raise concerns about improper conduct within in the company. The policy shall outline the mechanisms for the protection of employees who make such disclosure and the strategies implemented to address such matters as reporting, responsibility and confidentiality.

28.7 Internal Reporting of Suspicious Transactions

28.7.1 The FI(TR)R requires dealers to establish clear responsibilities and accountabilities to ensure that policies, procedures, and controls which deter criminals from using their facilities for money laundering, are implemented and maintained.

28.7.2 All dealers offering prescribed financial services operating within or from The Bahamas are required to:

i. introduce procedures for the prompt investigation of suspicions and subsequent reporting of same to the FIU;

ii. provide the MLRO with the necessary access to systems and records to fulfill this requirement; and

iii. establish close co-operation and liaison with the FIU and the Commission.

28.7.3 There is a statutory obligation on all staff to report suspicions of money laundering to the MLRO in accordance with internal procedures. However, in line with accepted practice some dealers may choose to require that such unusual or suspicious transactions be drawn simultaneously to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion.

28.7.4 All dealers have a clear obligation to ensure:

- that each relevant employee knows to which person he should report suspicions; and,
- that there is a clear reporting chain under which those suspicions will be passed without delay to the MLRO.

28.7.5 Once an employee has reported his suspicion to the MLRO, he has fully satisfied his statutory obligation.

28.8 Procedure for reporting suspicious transactions to the FIU

28.8.1 The Procedure for reporting suspicious transactions to the FIU is set out at ***Appendix E***.

28.8.2 Sufficient information should be disclosed which indicates the nature of and reason for the suspicion. Where the dealer has additional relevant evidence that could be made available, the nature of this evidence should also be clearly indicated.

28.8.3 The receipt of a disclosure will be acknowledged by the FIU. Normally, completion of a transaction will not be interrupted. However, in exceptional circumstances, such as the imminent arrest of a client and consequential restraint of assets, the dealer may be required by the FIU to discontinue the transaction or cease activity related to the client's transaction.

28.8.4 Following receipt of a disclosure and initial research by the FIU, if appropriate, the information disclosed is allocated to financial investigation officers in the FIU for further investigation. This is likely to include seeking supplementary information from the dealer making the disclosure, and from other sources. Discrete enquiries are then made to confirm the basis for suspicion. The client is not approached in the initial stages of investigating a disclosure and will not be approached unless criminal conduct is identified.

28.8.5 Access to the disclosure is restricted to financial analysts and other officers within the FIU. It is also recognised that as a result of a disclosure, a dealer may leave itself open to risks as a constructive trustee if moneys are paid away other than to the true owner. The dealer must therefore make a commercial decision as to whether funds which are the subject of any suspicious report (made either internally or to the FIU) should be paid away under instruction from the customer/client.

28.8.6 Dealers are reminded that reporting to the Commission, the Central Bank, the Commissioner of Police and any duly authorized employee of the dealer will be accorded similar protection against breach of confidentiality. It is therefore recommended that, to reduce the risk of constructive trusteeship when fraudulent activity is suspected, and to obtain the fastest possible FIU response, disclosure should be notified by telephone and the disclosure form forwarded to the FIU. Where timing is believed to be critical, a dealer should prepare a backup package of evidence for rapid release on the granting of a Court Order, search warrant, or a freezing order pursuant to the Section 4(2)(c) of the FIUA.

28.8.7 Following the submission of a disclosure report, a dealer is not precluded from subsequently terminating its relationship with the client provided it does so for commercial or risk containment reasons and does not alert the client to the fact of the disclosure which would constitute the offence of tipping off under the FTRA. However, it is recommended that, before terminating a relationship in these circumstances, the reporting institution

should liaise directly with the investigation officer in the FIU to ensure that the termination does not tip off the customer or prejudice the investigation in any way.

28.8.8 **The adequacy of the dealer's AML program to identify and properly report suspicious activity should be periodically reviewed**

28.9 TIPPING OFF

28.9.1 Preliminary enquiries of a client in order to verify his identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger a tipping off offence before an STR has been submitted in respect of that client **unless** the enquirer knows that an investigation is underway or the enquires are likely to prejudice and investigation.

28.9.2 In cases where the dealer forms a suspicion of ML/TF, and it is reasonably believed that performing a CDD process will tip-off the client, the company should proceed to file an STR with the FIU. Hence, it should be noted that failure to satisfactorily complete the CDD process, the commencement of the business relationship or performance of the transaction should cease.

28.9.3 Pursuant to section 14 of the Proceeds of Crime Act, 2018, a person commits an offence if he knowns or suspects that an STR has already been filed with the FIU, the police or other authorized agency and it becomes necessary to make further enquires, such individual tips off the client(s) that their names have been brought to the attention of the authorities and or an investigation is being carried out.

28.9.4 Pursuant to section 16 & 18 of POCA, dealers and their partners, offices and employees are protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU.

XII. STAFF RECRUITMENT, EDUCATION AND TRAINING PROCEDURES

29. KNOW YOUR EMPLOYEE (KYE) PROCEDURES

29.1 The financial services industry in The Bahamas, as in any other jurisdiction, is challenged with managing a diverse range of risks such as reputational, legal, operational etc. Consequently, in addition to financial institutions implementing proper procedures to mitigate risk from external forces, attention should also be placed on potential risks posed to financial institutions from internal forces such as from their employees. Appropriate procedures, including those for screening, should be implemented and documented for the hiring of employees. In this regard, the Commission offers some guidance to its registrant financial institutions which may be useful in managing the related risks.

29.2 The screening process for hiring new employees should seek to ensure that employees do not perform any function that causes harm in relation to the execution of their function for the company. To this end, the company's screening process, for the employees, must allow the company to be comfortable with the employee's:

- personal character (honesty, integrity and reputation)
- competence (able to effectively execute the functions of the position)
- qualifications (the required experience, knowledge and training)
-

The screening process should include, but is not limited to:

- background and employment historical checks;
- police record;
- reference checks, including character and financial references (or equivalent); and
- Qualification verification (as applicable, e.g. degrees, certifications).

29.3 For all employees, continued monitoring is encouraged to ensure they remain fit for employment. Employers should consider monitoring employees who are suspected of being linked to:

- unusual transaction activities;
- unusual increases in business activities; and
- persons known to be involved in illegal activities or associated with individuals of known questionable character.

29.4 The most effective KYE programme should be complemented by a sound on-going training programme which includes staff awareness.

30. STAFF AWARENESS PROGRAMMES

30.1 Dealers must take appropriate measures to familiarize their employees with:

i. policies and procedures designed to detect and prevent money laundering including those for identification, record keeping and internal reporting, and any legal requirements in respect thereof; and

ii training programmes which incorporates the recognition and handling of suspicious transactions.

30.2 Staff must be aware of their own personal AML statutory obligations including the fact that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions without fear of reprisal.

30.3 It is important that all dealers covered by this Code introduce adequate measures to ensure that staff members are fully aware of their responsibilities. To strengthen the company's position, the Commission strongly recommends that employees are requested to sign a confirmation document to indicate that they have read the Codes of Practice and any other requisite manual that the employee is expected to be familiar with etc.

31. STAFF EDUCATION AND TRAINING PROGRAMMES

31.1 Timing and content of training for various sectors of staff will need to be adapted by individual companies suitable for their own needs. It will also be necessary to make arrangements for refresher training at regular intervals, i.e. at least annually to ensure that staff members remain current with their responsibilities.

31.2 The Commission hosts a number of AML training seminars each year for its registrants. The following training guideline is recommended:

31.2.1 New employees

31.2.1-1 A basic training course on money laundering and terrorist financing, including relevant typologies and the subsequent need for reporting any suspicious transactions to the MLRO should be provided to all new employees within the first month of their employment. This is particularly critical for persons who will be dealing with clients or their transactions, irrespective of the level of seniority. They should be made aware that there is a legal requirement to report suspicion and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the company for the reporting of suspicious transactions.

31.2.2 Frontline Staff that deal directly with the public for the purpose of receiving and making payments, deposits etc., such as cashiers/ accounts officers

31.2.2-1 Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and the procedures to be adopted when a transaction is deemed to be suspicious.

31.2.2-2 All frontline staff should be made aware of their financial institution's policy for dealing with non-clients, including those that wish to conduct a transaction in relation to a client customer/client, particularly where large cash transactions, travelers' cheques or postal money orders are involved. They should be reminded of the need for extra vigilance in these instances.

31.2.2-3 In addition to the above, further training should be provided regarding the need to verify a customer's identity and client verification procedures. All employees should be familiarized with the company's suspicious transaction reporting procedures.

31.2.3 Administration/operations supervisors and managers

31.2.3-1 A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff in the foregoing categories. This will include the offences and penalties arising from the POCA and the FTRA for non-reporting and for assisting money launderers; procedures relating to the service of production and restraint orders; internal reporting procedures; the requirements for verification of identity; the retention of records and disclosure of suspicious transaction reports under the FIUA (See website for a summary of these offences).

31.2.4 Money Laundering Reporting Officers (MLRO) / Compliance Officers (CO)

31.2.4-1 In-depth training concerning all aspects of the legislation and internal policies will be required for the MLRO and the CO. In addition, these officers will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious transactions and on the feedback arrangements as well as on new trends and patterns of criminal activity. The Commission further recommends that companies should encourage holders of these positions to pursue and maintain domestic and/or international certification.

APPENDIX A

SUMMARY OF AML/CFT LAWS OF THE BAHAMAS

The Proceeds of Crime Act, 2018

The Proceeds of Crime Act ("POCA") criminalizes money laundering related to the proceeds of drug trafficking and other serious crimes. This Act also provides for the confiscation of the proceeds of drug trafficking or any relevant offence as described in the Schedule to the Act; the enforcement of confiscation orders and investigations into drug trafficking, ancillary offences related to drug trafficking and all other relevant offences.

The law requires persons to inform the FIU, the Police and other relevant agencies of any suspicious transactions that come to light during the course of their employment, trade or business activities. The Act provides immunity to such persons from legal action by clients aggrieved by the breach of confidentiality. It should be noted that the reporting of suspicious transactions is mandatory and a person who fails to report a suspicious transaction is liable to prosecution.

The Financial Transactions Reporting Act, 2018

The Financial Transactions Reporting Act ("FTRA") imposes mandatory obligations on designated financial institutions to: verify the identity of existing and prospective customers and clients; maintain verification and transaction records for prescribed periods; and to report suspicious transactions, which involve the proceeds of criminal conduct as defined by the Proceed of Crime Act to the Financial Intelligence Unit. This Act also establishes the Compliance Commission, an independent statutory authority which has responsibility for ensuring that designated financial institutions that are not otherwise regulated, comply with the provisions of the Act. These are outlined in Section 32(2) of the Act. The Act also provides for the Minister to designate a self-regulatory organization (SRO) for a profession, as the AML supervisor, on the recommendation of the Commission.

The Financial Transactions Reporting Regulations, 2018

The Financial Transactions Reporting Regulations, 2018 inter alia, sets out the evidence that financial institutions must obtain in satisfaction of any obligation to verify the identity of a client or customer.

The Financial Intelligence Unit Act, 2000

The Financial Intelligence Unit Act, Ch. 367 establishes the FIU of The Bahamas which has power, inter alia, to receive, analyze and disseminate information which relates to or may relate to the proceeds of offences under the Proceed of Crime Act.

The Financial Intelligence (Transactions Reporting) Regulations, 2001

The Financial Intelligence (Transactions Reporting) Regulations, Ch. 367 requires financial institutions to establish and maintain identification, record-keeping, and internal reporting procedures, including the appointment of a MLRO and Compliance Officer. These Regulations also require financial institutions to provide appropriate training for relevant employees to make them aware of the statutory provisions relating to money laundering and impose sanctions for failure to comply with Guidelines and Codes issued by the Regulators or the FIU.

The Anti-Terrorism Act, 2018

The Anti-Terrorism Act ("ATA"), criminalizes terrorist activities and the financing of terrorism and punishes offenders in or outside The Bahamas. It also prohibits the collecting of funds for terrorist/criminal purposes. Further, it makes persons responsible for the management or control of a legal entity that are involved with terrorist actions liable. The Act imposes a duty to report any suspicion to the Commissioner of Police regarding funds to be used to facilitate terrorism. The freezing of funds, forfeiture orders, sharing of forfeited funds and extradition that are related to terrorist movements are prescribed under the Act.

The Anti-Terrorism Regulations, 2019

The Anti-Terrorism Regulations ("ATR"), provides for the Attorney General to publish the United Nations Security Council Notice Orders (made pursuant to section 45 of the ATA, 2018). The Order is published to inform members of the IRF Steering Committee, all supervisory Authorities, all focal points and financial institutions of the listed terrorist entities or individuals and to comply with the ATA.

APPENDIX B

The Compliance Commission of The Bahamas on Administrative Penalties for Registrants of The Compliance Commission of The Bahamas under the FTRA 2018 – issued February 6th, 2019

Offence	Section	Classification of Offence	Amount of Penalty for Financial Institution	Amount of Penalty for Individual
Failure to conduct, document, update or provide a risk assessment upon request to the Supervisory Authority.	5	Very Serious	Up to $200,000.	Up to $50,000.
Failure to identify a customer/client or obtain any other requirements of the customer/client and beneficial owners for customer due diligence.	6 - 10	Very Serious	Up to $200,000.	Up to $50,000.
Establishing or maintaining an anonymous account or an account in a fictious name.	6(4)	Very Serious	Up to $200,000.	Up to $50,000.
Failure to fulfil the requirements of sections 5 – 9 and 14 and either opens an account or establishes a business relationship; carries out a transaction; or fails to terminate a business relationship.	11	Very Serious	Up to $200,000.	Up to $50,000.
Failure to apply enhanced customer due diligence obligations with respect to customer/clients, beneficial owner.	13	Very Serious	Up to $200,000.	Up to $50,000.
Failure to establish a risk management system to determine whether a	14	Very Serious	Up to $200,000.	Up to $50,000.

customer/client or beneficial owner is a politically exposed person.				
Failure to maintain records with respect to customer/clients or failure to provide such records in a timely basis when required by law.	15	Very Serious	Up to $200,000.	Up to $50,000.
Failure to maintain records in the manner as required.	16	Minor	Up to $50,000.	Up to $20,000.
Failure to destroy records after the expiry of 5 years from the date of the last transaction without reasonable cause.	17	Serious	Up to $125,000.	Up to $35,000.
Failure to develop and implement procedures to prevent activities related to identified risks.	19	Very Serious	Up to $200,000.	Up to $50,000.
Failure to designate a compliance officer.	20	Very Serious	Up to $200,000.	Up to $50,000.
Failure to implement internal controls with respect to a group of entities.	21	Very Serious	Up to $200,000.	Up to $50,000.
Failure to ensure compliance by a foreign subsidiary or branch with respect to obligations and/or the application of appropriate additional measures.	23	Very Serious	Up to $200,000.	Up to $50,000.
Failure to adhere to the prohibition with respect to establishing, operating or dealing with a shell bank domestically or internationally.	24	Very Serious	Up to $200,000.	Up to $50,000.

Failure to report suspicious transaction(s).	25 - 26	Very Serious	Up to $200,000.	Up to $50,000.
Failure to register with the Compliance Commission.	33(1)	Very Serious	Up to $200,000.	Up to $50,000.
Failure to notify the Compliance Commission of changes in registered office or principal place of business.	33(3)(a)	Serious	Up to $125,000.	Up to $35,000.
Failure to notify the Compliance Commission of changes in beneficial ownership, director, partner, compliance officer or money laundering reporting officer.	33(3)(b)	Serious	Up to $125,000.	Up to $35,000.
Failure to produce any record, information or explanation as required by the Compliance Commission.	34	Very Serious	Up to $200,000.	Up to $50,000.
Failure to comply with the Codes of Practice.	37	Very Serious	Up to $200,000.	Up to $50,000.

DEALERS IN PRECIOUS METALS AND PRECIOUS STONES - TYPOLOGIES

Source: APG Typologies Report 2018 - Japan

Money launderers purchased precious metals by cash derived from theft. They have conducted anonymous transactions and gave false information on customer identification (pretending to be another person or providing falsified identification documents when concluding sales contracts).

Source: APG Typologies Report 2010 - CHINESE TAIPEI

Purchase of gold bullion from proceeds of fraud

Mr. C withdrew cash from his account at Bank A in the sum of $43 million and $4.9 million in two days. An investigation found that Mr. C used a forged land ownership certificate to sell a piece of land to Developer A and received three cheques of Bank A in the sum of $5.5 million, $60 million and $80 million respectively. Mr. C deposited those cheques in an account at Bank A opened on the same day. Besides making cash withdrawals, Mr. C wired $100 million into his account at Bank B and used the money to buy 110 kg in gold bullion.

Source: APG Typologies Report 2018 – United States

Former Jeweler Faces Federal Money Laundering Charges for Pawning Diamonds Falsely Reported Stolen in 2004

U.S. Attorney's Office October 03, 2014 Northern District of Alabama (205) 244-2001

BIRMINGHAM—Federal prosecutors today charged a Vestavia Hills man with money laundering for pawning a 3-carat diamond in 2013 that was among a cache of jewels he collected $2.6 million in insurance money on in 2004 after reporting them stolen in a Mountain Brook Jewelry store robbery.

U.S. Attorney Joyce White Vance, FBI Special Agent in Charge Richard D. Schwein Jr., U.S. Secret Service Special Agent in Charge Craig Caldwell, Vestavia Hills Police Chief Dan Rary and Mountain Brook Police Chief Ted Cook announced the charges against JOSEPH HAROLD GANDY.

The U.S. Attorney's Office charged Gandy, 64, with one count of money laundering for pawning property worth more than $10,000 that he obtained through a criminal act, wire fraud, which he committed when he submitted an insurance claim on diamonds that had not been stolen. Prosecutors also charged Gandy with

one count of being a convicted felon in possession of firearms for the 99 weapons seized at his Vestavia Hills home in November 2013. Gandy is prohibited from possessing weapons because of a 1989 federal mail fraud conviction.

The FBI recovered jewelry during the search of Gandy's home and, as part of a plea agreement with the government, he also turned over a portion of the approximate $1.5 million worth of diamonds and jewelry he falsely reported stolen in 2004. Among those jewels is a rare Blue Diamond worth at least $620,000.

"This defendant revealed decade-old criminal acts, and committed a new crime when he brought forth valuable, but fraudulently obtained diamonds to pawn," Vance said. "Thanks to the committed and cooperative efforts of the Mountain Brook and Vestavia Hills police departments, the FBI and the Secret Service, Mr. Gandy avoided, but did not escape justice."

"This case illustrates the great cooperation among law enforcement at all levels," Schwein said. "I want to extend my personal appreciation to the Vestavia Hills and Mountain Brook police departments, the U.S. Secret Service, and my agents for their outstanding work. It was their diligent investigative efforts that brought this case to where it is today," he said.

"I commend the cooperative between the FBI and our investigators," Rary said. "Interagency cooperation is essential in today's environment, especially in complex investigations such as these."

Prosecutors filed the charges and the plea agreement with Gandy in U.S. District Court.

According to the plea agreement, Gandy's crime unfolded as follows:

Gandy was an owner and the operator of Denman-Crosby Jewelry Store in Mountain Brook in 2004. In December of that year, he reported that two unidentified men robbed the store at gunpoint. At the time, Denman-Crosby was promoting a loose diamond sale for Christmas. It had many diamonds and other jewelry in on consignment from jewelers in New York and elsewhere. The store carried a $2.6 million insurance policy. Gandy had increased the coverage amount with XL Specialty Insurance Company a few weeks before the robbery.

In January and March of 2005, Gandy used interstate wire transmissions to submit insurance claims from the robbery. He included a detailed inventory of jewelry worth about $2.8 million that he reported stolen. XL Specialty paid the policy's limit of $2.6 million.

In July 2013, Gandy began sending a friend to jewelry stores in Jefferson County to pawn diamonds he had reported stolen in 2004. The first effort ended when the jeweler requested documentation on a 1.59-carat diamond, mounted in a platinum setting, and attempted to examine the stone closely. The concern was that

the diamond might bear a laser inscription useful in tracing its history. Subsequently, Gandy examined 10 to 12 diamonds under a microscope and selected stones that bore no inscription.

On July 26, 2013, Gandy sent his friend to a Birmingham jewelry store to pawn a 3.01-carat emerald cut diamond he said was worth about $43,000. Gandy said he wanted at least $15,000 for the stone. The store accepted the diamond in exchange for a $12,000 loan. The diamond was one Gandy reported stolen in the Denman-Crosby robbery. He gave his friend $2,000 for making the transaction.

Between August and November of 2013, Gandy's friend pawned two more diamonds: a 3.45-carat cushion-cut diamond for $8,000; and a 2.16-carat round diamond for $2,000. Both stones were on the stolen inventory list Gandy provided the insurance company in 2005. Gandy gave his friend $1,880 after receiving the $8,000 for the 3.45-carat diamond.

Gandy's plea agreement is a "binding plea agreement" in which the government and Gandy stipulate that a 45-month prison sentence is appropriate. If the court rejects the plea agreement, either party may declare it null and void.

As part of the agreement, the government would recommend Gandy be required to pay $20,000 in restitution to the jewelers where he pawned the diamonds, and that he forfeit to the U.S. government all the jewels seized and recovered in the case. Vestavia Hills Police seized the 99 weapons at Gandy's house and has state charges pending against him. The city police are handling forfeiture of the firearms.

The government acknowledges in the plea agreement that it has no evidence or information to suggest Gandy is violent or has been engaged in previous violent behavior. The agreement notes that Gandy, through his lawyer, related that, except for older firearms he bought before his 1989 conviction or that were passed down from his father and grandfather, the firearms at his house belonged to his son who died in 2004.

The FBI, Secret Service, Vestavia Hills and Mountain Brook police departments investigated the case. Assistant U.S. Attorney George A. Martin Jr. is prosecuting the case.

Source: APG Typologies Report 2013 - THAILAND

Thai baht currency exchanged for foreign currencies used to buy gold

The case involved the proceeds of drug trafficking in Thai baht being exchanged for foreign currency with money changers who also conducted a currency distribution business.

Steps in the laundering process included:

1) The money derived from drug trafficking was exchanged for foreign currency before being smuggled out of Thailand. (Foreign currency can be taken out of Thailand, but must be declared at customs.)
2) The foreign currency originating from the drug trade deals was later used to buy gold.
3) When the gold was sold, the proceeds from the sale were treated as business income 'in good faith'.

Source: AUSTRAC Typologies Report 2008 – Australia

Bullion purchased with cash

An investigation into money laundering and structuring offences was initiated by a STR received by AUSTRAC and subsequently forwarded to a law enforcement agency. The primary suspect of the investigation was engaged in the purchase of approximately AUD180, 000 worth of silver, using cash in amounts under AUD10, 000. The individual had also employed five other people to purchase silver in structured amounts on his behalf.

APPENDIX D

Anti-Money Laundering/Countering Financing of Terrorism Suspicious Indicators (Red Flags) for Dealers

Customer and customer behavior:

- Checking identity is proving difficult
- The customer is reluctant to provide details of their identity
- There are no genuine reasons for paying large sums of money in cash.
- Cash payment is only mentioned by the customer at the conclusion of the transaction.
- Instruction on the form of payment changes suddenly just before the transaction goes through.
- The goods purchased and/or the payment arrangements are not consistent with normal practice for the type of customer concerned.
- A cash transaction is unusually large
- The customer will not disclose the source of the cash.
- The explanation by the business and/or the amounts involved is not credible.
- The customer is buying from an unusual location in comparison to their locations.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The method of delivery is unusual, for example, a request for immediate delivery, delivery to an address other than the customers address or the loading of high volume / bulky goods immediately into the customers own transport.
- Transactions having no apparent purpose or which makes no obvious financial sense, or which seems to involve unnecessary complexity.
- Unnecessary routing of funds through third parties.
- Enquires about the business's refund policy.
- Seeks a refund for spurious reasons.
- Seeks the repayment in the form of a cheque.
- Customer indiscriminately purchases merchandise without regard for value, size, or color.
- Purchases or sales that is unusual for client or supplier.
- Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's cheques, or payment from third parties.
- Attempts by client or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.

- Customer is reluctant to provide adequate identification information when making a purchase.
- Transactions that appear to be structured to avoid reporting requirements.
- A customer orders item, pays for them in cash, cancels the order and then receives a large refund.
- A customer asking about the possibility of returning goods and obtaining a cheque (especially if the customer requests that cheque be written to a third party).
- Purchase appears to be beyond the means of the client based on his stated or known occupation or income.
- Customer may attempt to use a third party cheque or a third party credit card.
- Transaction lacks business sense.
- Purchases or sales that are not in conformity with standard industry practice.

APPENDIX E

PROCEDURE FOR REPORTING SUSPICIOUS TRANSACTIONS TO THE FIU:

The Financial Transactions Reporting Act, 2018 (FTRA), outlines the procedures for reporting suspicious transactions and grants protection to those persons who report suspicious transactions.

Section 25 of the FTRA mandates a financial institution to report a transaction which the financial institution knows, suspects, or has reasonable grounds to suspect, that the transaction or proposed transaction involves money laundering, terrorist financing, proliferation financing, or any associated predicate offence, to the FIU.

On 1 June 2019, the FIU migrated from the manual filing of Suspicious Transaction Reports (STRs) to an electronic filing platform. This platform allows registered Money Laundering Reporting Officers (MLROs) or Designated Reporting Officers (DROs) to complete, file, and submit all STRs along with relevant supporting documentation to the FIU safely and securely from their offices.

Before logging into the platform, all financial institutions and their MLRO or DRO must register with the FIU by accessing the following website:-

https://fiuconnect.fiubahamas.bs/casekonnect/index.php?module=users/login

Documentation, namely, an approval letter from the financial institution, an approval letter from the regulator, a curriculum vitae, and a copy of government issued identification must also support the MLRO or DRO registration. Upon approval from the FIU, an email with a user profile and a temporary password will be received and the submission of STRs can commence.

Although the prescribed form for reporting a suspicious transaction to the FIU is via the platform, in accordance with section 25 subparagraphs (2) and (3) of the FTRA, STRs may be forwarded to the FIU by way of facsimile transactions, electronic mail, other similar means of communication, and in the case of urgent extenuating circumstances, orally.

Sufficient information should be disclosed, which indicates the nature of and reason for the suspicion. Where a Registrant has additional relevant evidence that could be made available, the nature of this evidence must be indicated.

APPENDIX F

REFERENCES:

1. The Wolfsberg Group Articles on Risk Assessment for Money Laundering
   https://www.wolfsberg-principles.com/publications/wolfsberg-standards

2. FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Precious Stones
   http://www.fatf-gafi.org/

3. FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22)
   http://www.fatf-gafi.org/

4. FATF listing of High-Risk Countries of Money Laundering or Terrorist Financing & Other Monitored jurisdictions
   http://www.fatf-gafi.org/

5. FATF Report /June 2013 Money Laundering and Terrorist Financing Vulnerabilities of Dealers in Precious Metals and Precious Stones
   http://www.fatf-gafi.org/