THE COMPLIANCE COMMISSION OF THE BAHAMAS

CODES OF PRACTICE

FOR

LAWYERS

- 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 – October, 2018
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 the Legal Profession and updates the original Codes published in 2002 and its subsequent revisions. Its purpose is to provide lawyers and law firms 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 circumstance in which a lawyer/law firm may be deemed a financial institution and therefore subject to AML supervision by the Commission, is when a lawyer/law firm:-

- provides services in the circumstances specified in section 4(e) of the FTRA. Reference is also made to section 32(2) of the FTRA.

The Commission also includes in its supervisory scope for these purposes, all lawyers that provide services on behalf of the firm. Therefore, the terms "law firm" or "firm" are used interchangeably with the

term “lawyer” or “lawyers” throughout this document to mean a sole practitioner or a partnership practicing by either of these means.

Unless the context requires otherwise, the masculine terminology used throughout the document includes the feminine gender and the singular terminology includes the plural.

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 – October, 2018

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.
"BBA"	means The Bahamas Bar Association.
"Beneficial owner"	means: (a) the natural person(s) who ultimately owns or controls a facility holder; (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 lawyer/firm to assess the extent to which the client exposes the lawyer/firm 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.
"**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.
"Eligible Introducer"	means: - (1) any other Bahamian financial institution under section 3 & 4 of the FTRA; or (2) any foreign financial institution from a reputable jurisdiction who themselves are supervised or monitored for AML that is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank, the Securities Commission, the Insurance Commission, the Inspector of Financial and Corporate Services and the Gaming Board; or (3) any other foreign financial institution from a jurisdiction outside of The Bahamas as having an equivalent or higher AML regulatory framework to that which exists under Bahamian law and which is also regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank, the Securities Commission, the Insurance Commission, the Inspector of Financial and Corporate Services or the Gaming Board.
"FATF"	means the Financial Action Task Force.

"Facility"	means:- (a) an account or arrangement that is provided by a financial institution to a facility holder and by, through or with which a facility holder may conduct two or more transactions whether or not they are so used; and (b) without limiting the generality of the foregoing, includes a life insurance policy; an annuity; and the provision, by a financial institution, of a facility for the safe custody, including a safety deposit box.
"Facility holder"	means:- (a) the person in whose name the facility is established and without limiting the generality of the forgoing, includes: (i) any person to whom the facility is assigned; (ii) where the person in paragraph (a) is a mere nominee, the ultimate natural person who is the beneficial owner, settlor or beneficiary; (iii) any person who is authorized to conduct transactions through the facility; (iv) in relation to a facility that is a life insurance policy or annuity, any person who, for the time being, is the legal or beneficial owner of that policy or annuity; and (b) for the purposes of the FTRA, a person becomes a facility holder in relation to a facility when that person is first able to use the facility to conduct transactions.
"**FCSP**"	means a financial and corporate service provider licensed under the Financial and Corporate Service Providers Act.
"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 firm (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 lawyers 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.
"Lawyer", "law firm", or "firm"	refers to a lawyer in his capacity as a financial institution pursuant to section 4(e) of the FTRA i.e., when providing prescribed financial services, unless the context otherwise requires.
"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.
"Occasional transaction"	means a one-off transaction or linked transactions that are carried out by a person otherwise than through a facility in respect of which that person is a facility holder. An example of this may be where someone purports to pay a sum over $15,000 to the firm for the benefit of a facility holder of that firm.
"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 3 and 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 lawyer under section 4(e), those services are where he/she engages in, or carry out transactions for a client concerning matters stipulated in section 4(e) 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 Trustees 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.
"Transaction"	means:- (a) a purchase, sale, loan, pledge, gift, transfer, delivery or other

	disposition, or the arrangement thereof, and includes but is not limited to - any deposit, withdrawal, exchange or transfer of funds in cash, whether in currency or by cheque, payment order settlement or set off between clearing institutions or branch offices or other instrument or by electronic or other non-physical means… (for full definition refer to section 2 of the FTRA).
"Transfer"	means buying or otherwise acquiring or agreeing to do so, seeking, selling or otherwise disposing or agreeing with another to do so or making such arrangements.
"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 counsel and attorney, 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 lawyers; the transparency of beneficial ownership of legal persons and legal arrangements; 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); information sharing; 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. Lawyers/Firms should refer to section 44 of the ATA for specific details regarding the reporting obligation in accordance with the law.

1 See Appendix B, part 3(b).

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 Lawyer/Firm 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 Lawyer/Firm must ensure facility holder(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 establishment of a facility or conduct 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 (d) and (e), as well as 23 (a) and (c) lawyers 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 (e) 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.

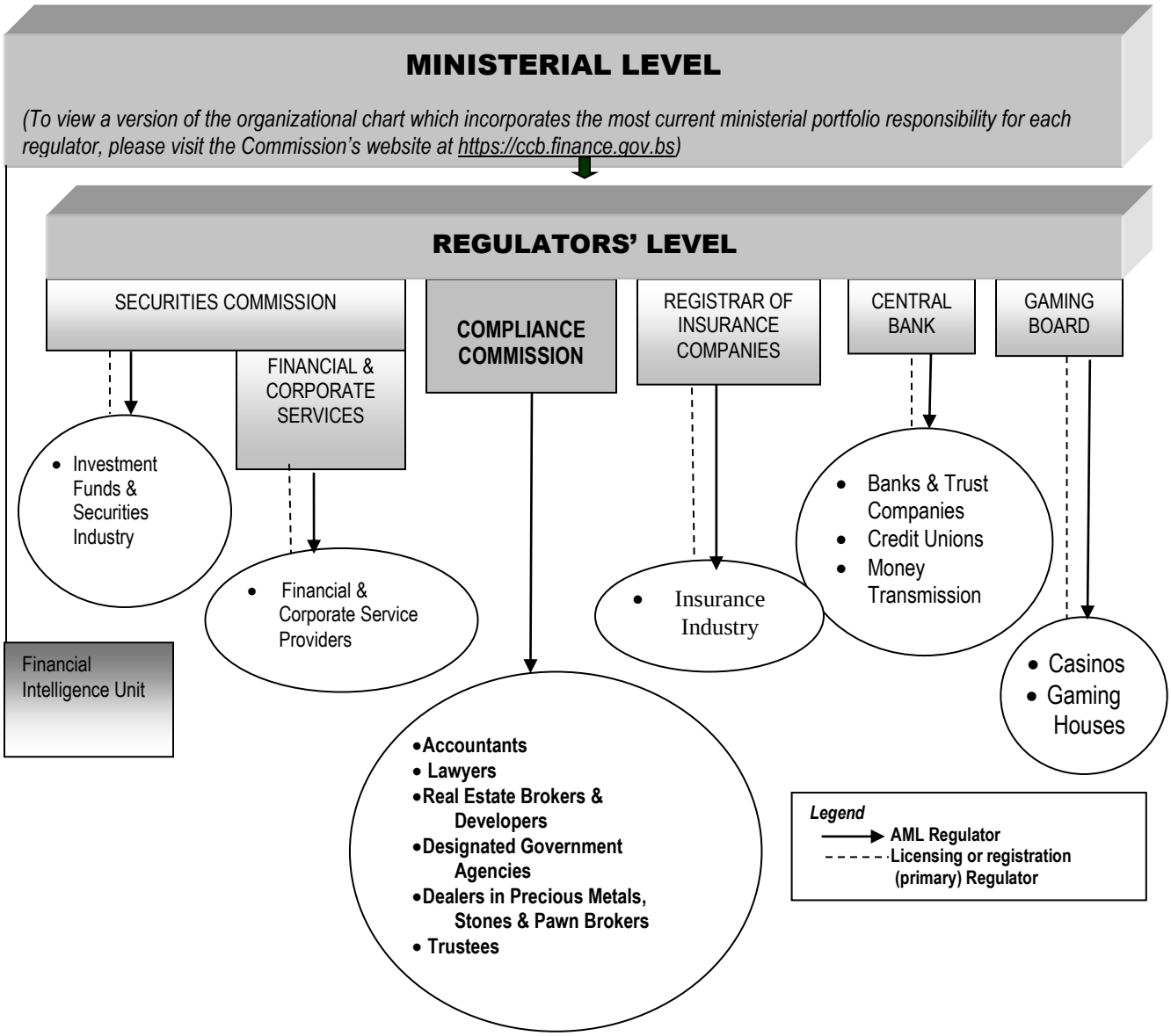
8. THE REGULATORY FRAMEWORK

8.1 An organizational chart of the AML regulatory framework, specifically identifying lawyers, 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 lawyers, 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 29.1 to 29.1.4) for more details about the FIU).

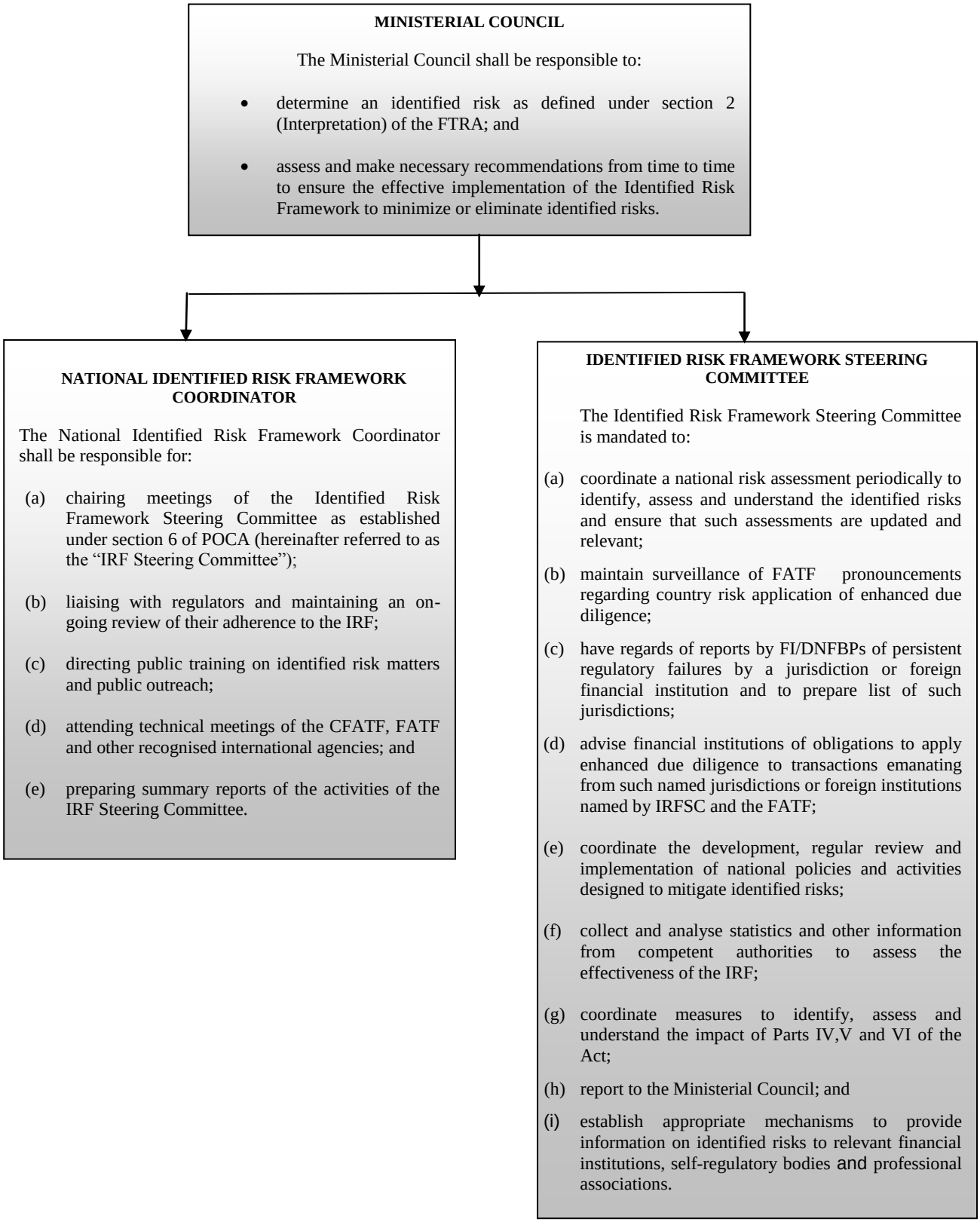
Fig. 1: Regulatory Framework for AML in The Bahamas



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 LAWYER AS A FINANCIAL INSTITUTION

10. WHEN IS A LAWYER A FINANCIAL INSTITUTION?

10.1 Lawyers in The Bahamas are subject to the money laundering laws on two levels. On the first level, all lawyers are subject to the provisions of the Proceeds of Crime Act (POCA) particularly Section 12. The law requires persons to inform the Financial Intelligence Unit (FIU), the Police and other relevant agencies of any suspicious transactions that come to light during the course of their activities. The reporting of suspicious transactions is mandatory and a person who fails to report a suspicious transaction is liable to prosecution. Section 18 of the Act provides for protected disclosure of information in the course of a person's trade, profession, business or employment.

10.1.1 On the second level, all lawyers who offer prescribed financial services whether pursuant to section 4 (e) of the FTRA, or under a financial and corporate service provider licence are, 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 lawyer is deemed to be a financial institution under the FTRA.

10.1.2 There are two circumstances in which a lawyer is deemed to be a financial institution as outlined in **Figure 3** below. For the purposes of this Code section 4(e) (under the supervision of the Commission), unless otherwise specified, it is only the first two categories of prescribed financial services outlined below that are being dealt with in this document.

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

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

(i) the buying or selling of real estate;
(ii) a deposit or investment of cash;
(iii) the management of client funds or securities;
(iv) the management of bank, savings or securities accounts;
(v) the organization of contributions for the creation, operation or management of a legal person;

(vi) the creation, incorporation, operation or management of a legal person or legal arrangement, and buying and selling of a business entity;

(vii) the provision of a registered office or acting as a registered agent; and

(viii) the acting as or arranging for another person to act as, a nominee shareholder for another person.

10.2.2 Lawyers are encouraged to separate their financial activities from those of the general law firm and to maintain separate and distinct records pertaining to the financial activities including separate financial records, (see **Fig. 3** below). This separation may occur physically through the maintenance of different filing cabinets or systems. It can also be achieved, in the case of information stored electronically, by creating separate electronic files for the financial services. By separating the activities, this will avoid providing access during the on-site examination to files and information with which the Commission is not concerned.

10.3 When providing prescribed financial services as a licensed financial and corporate service provider

10.3.1 Licensed financial and corporate service providers are financial institutions for AML purposes pursuant to the FTRA and subject to supervision by the Inspector of FCSPs where such services involve the licensees facilitating the movement of funds into, through, around and out of, the financial system on behalf of clients.

10.3.2 The business activity that is carried out under a financial and corporate service providers' licence should also be distinct and separate from the general legal practice as well as the prescribed financial services of the firm under the FTRA - See ***Fig. 3*** below.

Fig. 3: Graphic Illustration of a Law Firm's Obligations under the AML Laws.

<table>
<tr><td rowspan="2">General Legal Practice

That is all legal professional services that are <u>not</u> deemed to be prescribed financial services nor subject to a financial and corporate service providers licence.

This aspect of the firm's work is subject to AML obligations under the POCA and ATA.</td><td colspan="2">Prescribed Financial Services under any one or more of the following:</td></tr>
<tr><td>Section 4 (e) of the FTRA makes a law firm a financial institution in respect of those activities, and thereby subject to the FTRA, FTRR, FI(TR)R, and this Code in addition to being subject to POCA and ATA. The prescribed financial services under section 4 (e) are any case in which a lawyer engages in or carries out transactions for a client in respect of sub-clauses of the aforementioned section.</td><td>Licensed financial and corporate service provider activities (as defined in section 2 of the FCSPA) are subject to the requirements of the POCA, ATA and the FCSPA. They are also subject to FTRA, FTRR & FI(TR)R as a financial institution under the FTRA in those cases where their activities involve facilitating movement of funds on behalf of clients pursuant to the FCSP licence. <u>N.B. It is often the case that the licence is held, not by the firm directly, but by a subsidiary company of the firm.</u></td></tr>
<tr><td colspan="3">(POCA applicable to entire law firm including prescribed financial services under section 4 (e) of FTRA and financial and corporate services activities pursuant to a licence from the Inspector of FCSPs.)</td></tr>
</table>

11 VULNERABILITIES OF THE LEGAL PROFESSION

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

- The use of client accounts to disguise the beneficial ownership of funds or to conduct false transactions that are cancelled and require the return of funds to the client;
- Purchase and sale of real property – these high value transactions are often used in the layering and integration stages of money laundering to disguise the source of funds and legitimize large amounts of criminal proceeds;
- Creation and management of companies and trusts – create complex vehicles that may disguise the beneficial owner and disguise criminal proceeds;
- Managing client affairs and making introductions to financial institutions – give the appearance of legitimacy or respectability to the affairs of the client; and
- Terrorist financing risk is high due to legal professions core business offering.

11.2 OTHER VULNERABILITIES ASSOCIATED WITH THE LEGAL PROFESSION[5]:

- Filing of fictitious lawsuits to obtain judgment to legitimize the funds; and
- Execution of financial operations on behalf of customers, like cash deposits or withdrawals, foreign currency exchange operations, sale and purchase of shares, sending and receiving international money transfers.

11.3 As cash is the most common form of money laundering, lawyers should be aware that money laundering risks posed by products and services, 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.

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

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.

5 FATF Report /June 2013 Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.

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 section 4 (e) 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 institutions 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 law firm, 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 lawyers, 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 law firms 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 during the first quarter of each year with the BBA, amongst other bodies, to review the activities of the previous year and 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 LAWYERS WITH THE COMMISSION

13.1 It is mandated by law, in accordance with section 33(1) of the FTRA for lawyers and law firms carrying out business pursuant to section 4 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 Lawyers registered with the Commission are required to confirm their status via the Commission's website by December 31st of each year.

13.3 Lawyers registered with the Commission must be a member of the BBA in good standing and are required to be of irreproachable conduct. The Commission is of the view that the BBA is constantly monitoring its members with respect to their adherence to law and order and maintaining ethical standards. Notwithstanding the above, the Commission is at liberty to adopt supplementary measures that it deems necessary to achieve or enhance effective supervision.

13.4 **Lawyers and Law firms 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. In the case of lawyers, the BBA is charged with this responsibility.**

14. COMMISSION AWARENESS AND TRAINING PROGRAMMES FOR LAWYERS

14.1 Though not obligated to do so, The Commission organises annual training programmes for lawyers. In addition, officers of the Commission are available to offer specific training

programmes for individual firms upon request. The annual training provided by the Commission does not preclude the lawyer/law firm 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 lawyer/firm.

14.2 Lawyers 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 the leaders of the BBA. 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] Lawyers and law firms 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.

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.

15.3 From the firm's perspective, the term beneficial ownership, when used to refer to beneficial ownership of an account 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) are 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 law firms under its remit to 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 firm, 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 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 firm that provides financial services in accordance with section 4(e) 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 firm. 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 firm 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 lawyer; an undischarged bankrupt; disbarment, disqualification as a lawyer 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 firm 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 firm'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 lawyer or law firm.

16.3 All individuals with the responsibility for the management and control of the firm and key persons within the firm, including non-lawyers who are not subject to the assessment by BBA, must prove to, and assure the Commission that they comply with fit and proper requirements. For non-lawyers, this can be accomplished through the Know Your Employee (KYE) process. Lawyers and law firms 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 firm. 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.**

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. Firms are required to complete a Risk Assessment Questionnaire issued by the Commission for an initial assessment of the inherent risks to the Firm. The purpose of the risk assessment questionnaire is to gather information on the salient features of the firm's overall structure, clients (including geographical location and beneficial owners), products and services, 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 firm. The risk assessment will be followed by an on-site or off-site examination of the firm.

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 firm's risk profile, policies and procedures, and tests the adequacy, effectiveness and control measures implemented to mitigate risks by a firm to satisfy its AML obligations.

17.1.5 The examination focuses on procedures and systems to examine the firm's obligation to comply with AML laws and guidelines. The Bahamian AML laws and applicable guidelines require DNFBPs to, at a minimum:

- Conduct and document a risk assessment of the firm'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 compliance effectiveness reviews, minimum every two years; 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 law firms, 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 law firms' level of risks, the measures in place to mitigate the risks and the firm'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 law firm 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 firm. 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 firm 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 law firm 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 as specified by the Commission**. However, the risk rating assigned to the firm by the Commission will determine the examination cycle of the law firms 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[8], which gives him or her the authorization to commence an examination.

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

17.4.7 A routine examination assesses the law firm'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 law firm's prescribed financial services:

(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 firm to discuss the examination findings and any recommendations. Within 10 days of completing the examination form the examining accountant must submit the completed examination form to the Commission to be evaluated. Those law firms 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 Law firm is on a risk sensitive basis, taking into account:

- the risk rating assigned (i.e., low, medium or high) to the firm 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 Law firm, its characteristics and in particular its diversity;
- the identified ML/TF risks, the policies, procedures and internal controls associated with the law firm, as identified by the Commission's assessment of the law firm's risk profile; and

- the ML/TF risks present in The Bahamas;

NB: Firms 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 firm regarding the next date for a routine on-site examination taking into account the following considerations:

- the Commission's risk assessment of the firm's prescribed financial services;
- an evaluation of the firm'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 firm to determine the firm'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 law firms 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 firm of a follow-up examination to take place within fourteen (14) working days. Further, the Commission will advise the firm 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 law firm 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 firm 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 firm 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 firm will be advised accordingly.

17.6.3(b) However, if a law firm 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 law firm highlighting the details of previous discussions and/or communications and reminding the firm of the agreed-upon strategy for addressing the deficiencies. A maximum period of three (3) months will be given for the law firm to rectify all deficiencies.

Step 2. The Examiner will follow up in the interim to determine the firm's progress in adequately addressing the deficiencies. However, the firm 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, law firms 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 law firm at least two (2) weeks prior to the examination. This Notice will be forwarded to the MLRO/CO or the Senior Management of the law firm.

17.8 Special Examination

17.8.1 The Commission will conduct an on-site examination of a law firm 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 law firm has violated any provisions of the AML laws, or where information comes to the attention of the Commission that a statutorily law firm 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.

17.9 Examinations for firms that offer prescribed financial services, i.e. services under section 4(e) of the FTRA:

17.9.1 **Fig. 3** on page 18 illustrates how a law firm may be engaged in providing several categories of prescribed financial services. This occurs when the firm, in addition to offering services pursuant to section 4(e) of the FTRA.

17.9.2 Examinations for firms in accordance with section 4(e) of the FTRA.

17.9.2-1 Where a law firm, as a financial institition under section 4(e) of the FTRA.

17.9.2-2 The examination process in both cases follows the same procedures as for the single examination (see section 17).

17.9.3 Examinations for firms in accordance with section 4(e) that also provide prescribed financial services under a financial & corporate service providers (FCSP) licence.

17.9.3-1 Where a law firm, as a financial institution for certain of its activities under section 4(e) of the FTRA, also holds a FCSP licence, (whether in its own name or through a company

established specifically for that purpose), the business that is performed pursuant to the licence is also subject to an examination under section 11(4) of the FCSPA. This latter examination, is separate and apart from the examination required by section 32(1)(b) of the FTRA. In such a case the firm is required to have completed two separate examinations – one for the section 4(e) services under the supervision of the Compliance Commission and the other for the financial and corporate service activities under the supervision of the Inspector of FCSPs, Codes for which are available on the Securities Commission's website).

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[9].

The Commission has implemented a risk-based supervisory framework for addressing AML vulnerabilities posed to the entire firm. 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 firm, given its clientele, products, services, transactions, geographical regions and delivery channels. Firms should have regard to all available information, including published money laundering typologies[10] and terrorist lists, to assist with identifying potential risks. For lawyers and law firms to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the firm. 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 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 lawyers

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

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

as well as non-lawyers with responsibility for any aspect of the firm'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 firm.

2. Senior Management Responsibility and Support

Senior management is ultimately responsible for ensuring that the law firm 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 Law 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 legal 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 law firms may wish to assign this role to their Internal Audit or Compliance Department. Smaller law firms may accomplish the same objective by **assigning the review to the compliance officer.**

18.3 Information Technology (IT) Infrastructure

18.3.1 Law firms 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 Law firms must undertake the risk assessments prior to the launch or use of such products, 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 firm with timely information on a regular basis to enable the firm 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 law firm'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. Lawyers and law firms 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 law firms 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 facility holders and the countries or jurisdictions of their origin; the countries or jurisdictions of its operations; and its products, services, 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 a new product or business practice;
- 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:

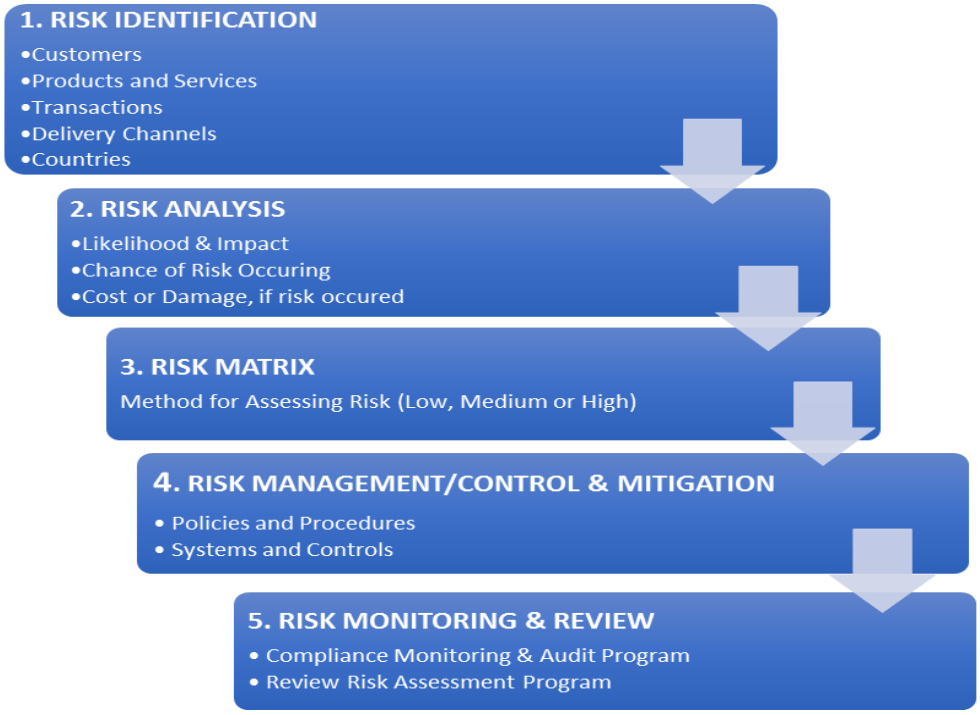
- the facility holder's geographic area, product, service, transaction and means of delivery risk factors, which shall be proportionate to the nature and size of the financial institution's business; and
- the outcome of any risk assessment carried out at a national level, and any regulatory guidance 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 law firm, 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 firm 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 firm 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 and services offered by firms to launder proceeds of crime or fund terrorism. Therefore, the risk assessment related to money laundering is also applicable to terrorism financing.

Fig. 4 - OVERVIEW OF FIVE (5) STAGES OF A ML/TF RISK ASSESSMENT ROCESS[11]:



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 lawyers/law firms take the appropriate steps to identify, assess and understand the ML /TF inherent risks posed to the firm via its clients, products and services; transactions, delivery channels and countries or geographical areas. Depending on the nature of the firm's business the inherent risks categories may be expanded. The objective is to ensure that reasonable measures are taken to satisfy the firm that all new and existing client relationships, products, activities and processes are properly assessed to determine the level of risk associated with all aspects of the business to avoid the firm 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, products and services does the firm have?

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

- Are funds derived from legitimate sources in every transaction?
- What kind of delivery channels are used for the products and services?
- What jurisdiction does the firm 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 firm. The type of inherent risks and vulnerabilities should be documented and placed in the firm's policies and procedures manual. Further the type, volume and value of the transactions should also be documented along with the control measures. Lawyers and Law firms 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 (i.e., Trust and corporate services) plus the scope and accessibility of the operation? • Does the firm 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 firm have effective policies, procedures and systems in place to mitigate inherent risks? • Does the firm take measures to manage and mitigate the inherent risks? • Does the firm 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 and Services	• Do the products and services required by or provided by 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 services and the extent of their vulnerability? • Are the products and services offered deemed high risk by the Commission or other credible sources like the IMF or WB (i.e., trust services, holding of funds for clients, management of client's funds etc.)?
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 firm engage in high volume of financial transactions?
Delivery Channels	• Are the delivery channels complex (i.e., many intermediaries)? • 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 firm 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. 5 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 legal profession. 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 firm should establish whether all identified categories of risks pose a low, medium or high risk to the business operations. The firm 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, firms 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 firm'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. 6 – 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 firm 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 firm 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 firm 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 law firms, at a minimum, to place clients, products/services, transactions, delivery channels and client geographical location into one of three risk categories i.e., Low Risk, Medium Risk or High Risk[12].

19.5 STAGE 4 - RISK MANAGEMENT/CONTROL & MITIGATION

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

12 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.

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 Firms 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, products or services identified during the risk assessment process.

19.5.6 The firm 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 law firm 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 firm'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 REVEW

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 firm's risk analysis. The firm 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 firm should ensure the allocation of adequate resources, taking into account the risks posed to the firm. The firm 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) [13] PROCEDURES

20. VERIFICATION DETAILS AND DOCUMENTARY EVIDENCE PROCEDURES

20.1 When must identification and verification take place?

20.1.1 Law firms have a statutory obligation to undertake customer due diligence measures when opening an account for or otherwise establishing a business relationship with a facility holder. 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:

- when a new facility is being opened (whether permanent or occasional);
- when a facility holder is being added to an existing facility;
- where doubt exist about the veracity or adequacy of previously obtained customer identification information of a facility holder;
- where a non-facility holder seeks to conduct a transaction involving $15,000 or more either for himself or on someone else's behalf;
- where the facility holder seeks to conduct a transaction or an occasional transaction of $15,000 or more on behalf of a third party, using his facility, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
- where there is a suspicion of activities relating to any identified risks involving the facility holder or the facility holder's account;
- where there is a material change in the way the facility is being operated;
- where there is caused to suspect that the identity of the facility holder or beneficial owner or the person conducting a transaction is in doubt;
- Where a facility holder is a corporate entity, the obligation to verify the identity of beneficial owners will only be required for those beneficial owners having a controlling interest in the corporate entity;

[13] "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.

- where there has been no recent contact with the facility holder or no transaction involving the facility within a period of 5 years, and the facility has not been closed out, the real estate firm is required, by law, to verify the identity of the facility holder; and
- where a person, who is neither a facility holder nor in an established business relationship with the financial institution wishes to carry out a transaction (to be referred to as structuring of an occasional transaction - See Figure 7 below for an explanation of structuring).

Please refer to sections 6-9 and 11-13 of the FTRA for a comprehensive view of the obligations for identification and verification of a facility holder and Part III of the FTRR for details of verification requirements.

20.1.2 Although the primary duty to verify identity using the best evidence and means available rests with the law firm; in exceptional circumstances a law firm may wish to approach a third party or eligible introducer specifically for the purpose of satisfying itself on a verification of identity that it must complete. In these exceptional circumstances, please refer to guidance via section 23 of this document.

Fig. 7: Structuring

What is structuring?

Structuring transactions as a means of avoiding having to provide verification evidence is a practice known in money laundering schemes. This structuring, which is referred to as "linked" transactions or "smurfing", presents special challenges for verification *prior* to the transaction being conducted. For this reason, there is a need in some cases to aggregate linked transactions to identify those who might structure their business activities to avoid the identification procedures.

There is no legal requirement to establish additional systems specifically to identify and aggregate linked transactions. However, where a law firm detects that two or more transactions by or on behalf of someone who is not the firm's facility holder, have totalled more than $15,000, and it has reasonable grounds to suspect that this was intentionally done to avoid meeting the $15,000 threshold that would require verification, then this information must be acted upon as soon as practicable after the lawyer/law firm forms that conclusion. The law firm/lawyer is then under an obligation to verify the identity of the person seeking to conduct any other related transaction.

The attempt to transact the linked activities must be in relation to the firm's prescribed financial services, which generates the obligation to verify identity.

This requirement exists whether or not the person conducting the transaction is doing so for himself, on behalf of someone else, or in concert with others.

- *Timing of verification in structured transactions:*

Verification of identity in a structured transaction must take place as soon as reasonably practicable after concluding that structuring is taking or has taken place.
Where the person conducting the transaction under a structured arrangement is doing so through his own facility as an

intermediary on behalf of someone else, the law firm must verify the identity of that other person as soon as reasonably practicable after concluding that structuring is taking or has taken place.

- ***Indications that transactions are being structured:***

In determining whether or not transactions are or have been structured to avoid the verification procedure, the law firm shall take into consideration the following factors:

(a) the time frame within which the transactions are conducted; and
(b) whether or not the parties to the transactions are the same person, or are associated in any way.

20.1.3 Documentary evidence sufficient to establish the identity of the client must be on record, as part of the due diligence process, for every facility or occasional transaction that has been verified for low, medium and high-risk clients.

20.1.4 Part lll of the FTRR provides a list of mandatory documentation and information that must be obtained to verify identity, as well as additional information that may be relied upon to further establish, conclusively, the identity of a person that must be verified. The determination of any additional information required for high risk clients should be documented in the firm's enhanced due diligence procedures for high risk clients.

20.2 Verification of identity of individuals

20.2.1 Where a law firm 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[14];
- date and place of birth;
- the purpose of the account; and
- the nature of the business relationship to be established.

20.2.2 In addition to the requirements above, the following information and documentation may be required (based on the firm'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;

14 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.

- occupation, name of employer, and where self-employed, the nature of the self-employment; or
- a copy of the relevant identification pages of the passport; a driver's licence; 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 law firm is required to verify the existence of a corporate entity, the law firm 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[15] 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 operate the facility;

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

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.

f) a certificate of good standing;

15 In the case of a Bahamian incorporated company, if the law firm 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.

g) the location of the registered office and if different, the location of the principal place of business;

h) a description of the nature of the business, including the date of commencement of the business, a description of the products or services 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 facility and the potential parameters of the facility, including size, in the case of investment and custody facilities; balance ranges, in the case of deposit facilities; the expected transaction volume of the facility; and written confirmation that all credits to the facility are and will be beneficially owned by the facility holder except in circumstances where the facility is being operated by an intermediary for the purpose of holding funds in his professional capacity.

20.4 Verification of identity of partnership or unincorporated business

20.4.1 Where the law firm is required to verify the identity of a partnership or other unincorporated business, pursuant to section 7(1) of the FTRA, the following information must be required:

a) verification of all partners or beneficial owners in accordance with regulation 4 of the FTRR;

b) copy of partnership agreement, (if any), or other agreement establishing the unincorporated business;

c) the mandate from the partnership or beneficial owner authorizing the opening of the account and conferring authority on those who will operate the account; and

d) any documentary evidence as is required under regulation 6 of the FTRR for the verification of the natural person who will operate the facility.

20.4.2 In addition to the requirements specified in 20.4.1 above, the following information/documents may also be relied upon to complete the verification of the partnership or other unincorporated business:

a) details regarding the description and nature of the business including: date of commencement of the business; a description of the products or services provided by the business; *and* the location of principal place of business;

b) the purpose of the account and the potential parameters of the facility including, size, in the case of investment and client facilities; balance ranges, in the case of deposit and client facilities; and the expected transaction volume of the facility;

c) written confirmation that all credits to the facility are and will be beneficially owned by the facility holder except in circumstances where the facility is being operated by an intermediary for the purpose of holding funds in his professional capacity; and

d) such documentary or other evidence as is reasonably capable of establishing the identity of a partner or beneficial owner.

20.5 Verification of trust and other legal arrangement

20.5.1 Typologies have shown the trust to be a popular vehicle for money laundering. Particular care needs to be exercised when these arrangements have been set up in locations with strict secrecy or confidentiality rules regarding disclosure of beneficiaries and other such information.

20.5.2 Trustees should be asked to state from the outset the capacity in which they are operating or making the application for a facility. Sight of certified extracts covering the appointment and powers of the trustees from/or the original trust deed, and any subsidiary deed evidencing the appointment of current trustees, should also be obtained.

20.5.3 Any application to become a facility holder or undertake a transaction on behalf of another, without the applicant identifying their trust capacity, should be regarded as suspicious and should lead to further enquiries.

20.5.4 Where a law firm is required to verify identity in relation to a trust, the law firm shall, in addition to carrying out the obligations imposed by the FTRA and the FTRR, take reasonable measures to determine the identity of the:-

(i) settlor of the trust;
(ii) beneficiaries or class of beneficiaries of the trust;
(iii) protector, if any; and
(iv) the natural person exercising effective control over the trust.

20.5.5 Where a law firm is required to verify identity in relation to a legal arrangement other than a trust, the law firm shall, in addition to the obligations imposed by the FTRA and the FTRR, take reasonable measures to determine the identity of:-

(i) the legal person exercising effective control over the legal arrangement;
(ii) the beneficiary, if any; and
(iii) the natural person establishing such arrangement.

20.5.6 Where money is received by a trust, it is important to ensure that the source of the funds is properly identified, the nature of the transaction is understood, and payments are made only in accordance with the terms of the trust and are properly authorised in writing.

20.6 Exemption from verification

Pursuant to section 8 of the FTRA, documentary evidence shall not normally be required for verification of identity of: —

(a) any financial institution regulated by the Central Bank of The Bahamas, The Securities Commission of The Bahamas, The Inspector, Financial Corporate Service Providers, The Insurance Commission of The Bahamas, or the Gaming Board;

(b) a financial institution, which is:- (i) subject to anti-money laundering and countering the financing of terrorism obligations; (ii) is under supervision for compliance with the obligations referred to in subparagraph (i); and (iii) has adequate procedures for compliance with customer due diligence and record keeping requirements;

(c) any central or local government agency or statutory body; and

(d) a publicly traded company listed on The Bahamas International Stock Exchange or any other Stock Exchange specified in the Schedule and approved by the Securities Commission of The Bahamas.

20.7 Verification of beneficial owner:

20.7.1 Where a law firm is required to verify the identity of a facility holder under Part II of the FTRA, the firm shall verify the identity of the beneficial owner of such facility in accordance with the FTRR.

20.8 Verification of facilities established by telephone or internet.

20.8.1 Where an individual, corporate entity or partnership makes a request to establish a facility by telephone, internet, or written communication, the law firm must verify, in accordance with the FTRR, the identify of that individual, corporate entity or partnership for whom the facility is being established.

20.8.2 Notwithstanding paragraph 20.8.1 above, the law firm may rely on the verification of the identity of the individual, corporate entity or partnership in accordance with regulation 9 of the FTRR.

20.9 Continued verification of accounts

20.9.1 Where the identity of the facility holder has been verified, no further verification of identity is necessary unless there is a material change in the operation of the facility.

20.9.2 Where there is a material change in the operation of a facility includes but is not limited to:-

a) change in ownership of the facility; or

b) activity which gives rise to the suspicion of any identified risk.

20.9.3 Every financial institution shall carry out monitoring of all facility holders for consistency with the facility holders stated account purposes during the business relationship.

20.10 Verification of facilities/accounts for intermediaries[16] (nominees, fiduciaries, Trustees etc.).

20.10.1 Where a transaction is being conducted by a person in his capacity as an intermediary, including a nominee or a fiduciary on behalf of another or others, those others, unless exempted, must also be verified in accordance with the above specifications set out in paragraphs **20.2 to 20.4.** The details and documents relied upon to verify those other individuals should also be contained in the file of the primary verification subject in accordance with guidance contained in para. **20.2.**

[16] Regulation 10, FTRR.

20.11 Transfer of records.

Where an existing facility holder closes one facility and opens another facility the financial institution shall confirm the identity of the facility holder and obtain any additional information with respect to the facility holder and all records relating to the existing account shall be transferred to the new facility and retained in accordance with the Act and any regulation made thereunder.

20.12 Failure to Satisfactorily Complete CDD

20.12.1 Where a law firm is unable to comply with relevant CDD measures, it shall be required not to open the account, commerce business relations or perform the transaction; or shall be required to terminate the business relationship. In the event of a client's failure to comply with CDD requirements, law firms must consider making a suspicious transaction report (STR) in relation to the client.

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 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[17] 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).

[17] Section 8, FTRA

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.

(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[18].

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

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.

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

21.2.1 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;
- 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.

21.2.2 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.

21.2.3 **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.**

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

21.3.1 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.

21.3.2 **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**.

21.3.3 **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

22.1 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 firm must have well-defined escalation and EDD processes and procedures in place.

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 or 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).

22.4 Politically Exposed Persons (PEPs)

22.4.1 Caution must be taken when dealing with PEPs; a special category of High-Risk clients[19]. At the out-set of the client/business relationship, the firm 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.

22.4.2 Law firms 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

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

sanctions lists and PEPs databases (additions as well as deletions), these lists should be consulted as a part of the firm's on-going monitoring of its clients

22.5 Enhanced Due Diligence for High Risk Clients

22.5.1 In addition to the due diligence procedures for low risk clients (see section 21 above), a law firm is required to perform enhanced due diligence in those circumstances where it knows or suspects that there is a greater propensity for illicit activity. This should become evident during the course of a risk categorization exercise where certain persons, products or services are deemed high risk. Where the National Risk Assessment (NRA) identifies high risk, the law firm should include the findings in their risk assessment and implement enhance measures to mitigate the risks.

22.5.2 The following activities (in addition to obtaining the verification information, evidence and documents required by Section 20) should form part of the firm's enhanced due diligence procedures to determine the circumstances in which a client is deemed to be high risk:

(1) Determining when the client is a high risk

Establish procedures to determine when, either during the establishment of the business relationship, or during the course of the relationship, the person is deemed high risk.

(2) Institute an approvals hierarchy for establishing relationships with high risk clients and PEPs depending on the size and management structure of the firm

Approval must be obtained from Senior Management to:

a) establish the business relationship; and

b) continue the relationship with the client who subsequent to establishing the relationship, is found to be or becomes high- risk.

(3) Develop a profile of the high-risk client and ascertain the expected activity. This profile should be regularly reviewed and updated as necessary.

The process of determining a high risk profile would include how to deal with clients from jurisdictions whose AML standards are not equivalent to the requirements found in Bahamian law. In the case of PEPs this is particularly important when dealing with clients from high risk jurisdictions e.g. 'High Intensity Financial Crimes Area' in the United States and areas that are undergoing political instability or that have a history of such. Foreign PEPs are always considered high risk and require the application of EDD. The decision

to engage or maintain the business relationship with the foreign PEP should be taken at the level of senior management.

(4) Maintain on-going monitoring of transactions for high risk clients

The law firm should ensure that all transactions are closely monitored on an ongoing basis. The procedures for monitoring high-risk clients should be reasonably capable of detecting any changes in the way the facility is being operated.

22.5.3 Enhanced Due Diligence for Higher Risk Countries

Law firms 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 RELIANCE ON THIRD PARTY (OR ELIGIBLE) INTRODUCERS

23.1 Who Is A Third Party / An Eligible Introducer?

23.1.1 A third party / eligible introducer is any one of the following:

- in the case of The Bahamas any other financial institution under section 3 and 4 of the FTRA; or
- any foreign financial institution from a reputable jurisdiction who themselves are supervised or monitored for AML that is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank, the Securities Commission, the Insurance Commission, the Inspector of Financial and Corporate Services and the Gaming Board.

23.1. 2 Firms must satisfy themselves, prior to establishing the facility, that the eligible introducer meets the specified requirements set out in accordance with the guidance of this section.

23.2 Circumstances in which the firm may rely on a verification carried out by an eligible introducer to satisfy its primary obligation to verify a client:

[20] www.fatf-gafi.org/publ

23.2.1 Lawyers and law firms must retain adequate documentation[21] to demonstrate that its KYC/due diligence procedures have been fully implemented, and that the necessary verification of the clients(s) have been executed. Depending on the circumstances, the firm may need to rely on a third-party (an eligible introducer independent or part of the same group) to undertake client due diligence measures. These measures must be in accordance with section 6(3) and sections 7-9 and 14 of the FTRA, except:

(a) where the third party/eligible introducer is suspected of breach of the identified risk framework as defined; or

(b) where the relevant facility holder has committed any offence designated as an identified risk.

23.2.2 Lawyers and law firms relying on a third party (domestically or within a foreign jurisdiction) shall immediately obtain all necessary information and documentation required under section 6(3) of the FTRA from the third party, including the identity of each facility holder and beneficial owner. Lawyers and law firms are also required to take adequate steps to ensure that the third party will upon request, provide copies of all relevant documentation without delay and is subject to AML obligations and is under supervision for compliance of these obligations. Further, there must be no obstacles which would prevent the law firm from obtaining the original documentation.

23.2.3 Notwithstanding the above, the ultimate responsibility for verifying the identity of a client rests with the firm. While firms may rely on the due diligence carried out by a third party to satisfy its primary duty to verify identity, the firm shall remain responsible for compliance with the FTRA and its regulations, including all requisite reporting requirements.

23.2.4 Lawyers and Law firms should have screening mechanism in place to satisfy itself as to the third party's reputation and integrity based on publicly available information and as to such other matters regarding the third party i.e., subject to adequate AML laws and regulation in the context of its dealings with clients and is supervised for compliance with such regulation and hailing from a reputable jurisdiction.

23.2.5 Law firms 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

[21] Adequate documentation according to substantive laws of The Bahamas.

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.[22]

23.2.6 **N.B. This exception from having to obtain full verification documentation is subject to the overriding statutory obligation[23] to carry out verification in any case where the law firm suspects that a transaction involves the proceeds of criminal conduct or is destined for financing terrorist activities.**

23.3 Eligible introductions where a facility is being established

23.3.1 In the case of facilities, eligible introductions are permitted in the following circumstances:-

(i) Establishment of facilities by telephone, internet or by written communication:

Where an individual, corporate entity or partnership makes a request to establish a facility by telephone, internet or by written communication, a law firm must verify, in accordance with the FTRR, the identity of that individual, corporate entity or partnership for whom the facility is being established.

Notwithstanding the paragraph above, the law firm may rely on the verification of the identity of the individual, corporate entity or partnership in accordance with regulation 9 of the FTRR.

(ii) *Arrangements between Existing Facilities:*

In the case of arrangements between two facilities which accommodate the conduct of transactions between them (whether held by the same or different financial institutions), the duty to verify identity is met once all such steps as are reasonably necessary to confirm the existence of the other facility have been taken. For example, where a client engages the services of a law firm to receive periodic deposits on its behalf from an account it (the client) has at an eligible introducer bank, the law firm may rely on the fact that it has confirmed the existence of such a facility, to discharge its primary obligation to verify. The records to be maintained in this situation are those that are reasonably necessary to enable the identity of the other eligible introducer (in this case the bank), the identity of the facility and the identity confirmation of the person; and

[22] www.fatf-gafi.org/publ

[23] Section 25(1) of the FTRA

(iii) *Corporate Group Introductions:*

Law firms may rely on a third party that is part of the same group of law firms and the group has applied customer due diligence, record-keeping and politically exposed persons requirements and programs against MI/TF in accordance with internal controls and foreign branches and subsidiaries and that it is supervised at the group level by a competent authority (the Commission in the case of The Bahamas). Further, that any higher country risk is adequately mitigated by the groups AML/CFT policies and procedures.

23.3.2 Where a facility has been established by any of the foregoing means, there is no need to carry out an independent verification of the client. However, the law firm is obliged to obtain and have on record an original letter from the eligible introducer:

- containing information which identifies the facility holder and any beneficiaries or relevant beneficial owners, his (the facility holder) authority to act in those cases where he is not the ultimate beneficial owner and the purpose and intended nature of the business relationship;
- advising that it (the eligible introducer) has verified the client being introduced and is in possession of the necessary verification information and documentary evidence sufficient to satisfy the requirements of the substantive AML laws in The Bahamas. The letter from the eligible introducer must also provide an undertaking to supply to the firm upon request, immediately and without delay, copies of such evidence and documentation.

23.3.3 In appropriate circumstances the firm may also seek to obtain directly from the client details regarding the source of income/funds, purpose, use, potential activity and other parameters for the operation of the facility, and document these. The fact that while the on-boarding has its genesis by way of eligible introduction, the firm must still monitor the client/facility as a part of its risk management in preparation to respond to any changes that would impact the ML/TF risks.

23.4 Eligible introductions where an occasional transaction (i.e. sums at or above the $15,000 threshold) is being attempted/conducted

23.4.1 An occasional transaction, whether such transaction is single or linked, is one in which the sum involved is equal to or above $15,000 and where the person purporting to conduct the transaction, or on whose behalf the transaction is being conducted, is not a facility holder of the firm (Reference FTRR).

23.4.2 Written confirmation certifying that the eligible introducer has carried out the required verification by law, may be used to satisfy the primary obligation on a law firm to verify identity, where $15,000 or more is involved in a transaction being conducted by or on behalf of a non-facility holder.

23.4.3 Only eligible introducers can issue written confirmation, i.e. those entities outlined in section 23.1.1 above.

23.4.4 The circumstances involving $15,000 or more in which reliance may be placed on a written confirmation issued by another eligible introducer financial institution certifying that it (the eligible introducer financial institution) has carried out the required verification are set out below:

(1) Where a deposit is made into a facility that is provided for the law firm by an eligible introducer financial institution and the law firm is unable to determine if such a deposit involved $15,000 or more. An example of this is where a facility holder client makes a deposit directly into a bank account of the law firm, then the law firm can rely on written confirmation from the bank that it (the Bank) has carried out the verification of the person making the deposit;

(2) Reliance can be placed on written confirmation of an eligible introducer e.g. a bank, which conducts a transaction of $15,000 or more on behalf of another person with the law firm that it (the bank) has carried out the required verification on the party on whose behalf it is acting; and

(3) A law firm can rely on a written confirmation from an eligible introducer (e.g. a bank) that it (the bank) has carried out the required verification on a non-facility holder who has conducted a transaction of $15,000 or more with the law firm by means of a facility which that verification subject has with the bank. The records to be kept in such eventuality should indicate:

- the identity of the eligible introducer,
- the identity of that facility, and
- the identity confirmation of the person.[24]

24 Section 6 (2), FTRA.

24 MONITORING OF FACILITIES

24.1 Law firms are expected to maintain systems and controls in place to monitor, on an ongoing basis, the relevant activities in the course of the business relationship to ensure consistency with stated facility purposes and activities and be aware of any changes in the course of the relationship. The nature and sophistication of this monitoring will depend on the nature of the business. The purpose of this monitoring is for law firms to be vigilant for any significant changes or inconsistencies in the pattern of transactions, having regard to, amongst other things, its knowledge of the customer, its business and risk profile and where necessary, the source of funds. Inconsistency is measured against the stated original purpose of the facility. Areas to monitor could be:

(a) client profile
(b) Transactions (type, frequency, amount)
(c) identify and detect suspicious transaction/activity
(b) geographical origin/destination
(c) any changes in beneficial ownership
(d) facility signatories
(e) report to the appropriate regulatory and enforcement authorities

24.2 It is recognized that the most effective method of monitoring facilities is achieved through a combination of computerized and human manual solutions. A corporate risk-based and compliance culture, properly trained, vigilant staff through their day-to-day dealing with clients, will form an effective monitoring method as a matter of course.

24.3 Law firms should, to the extent possible, examine the circumstances of complex and unusual, large transcations or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose and document their findings. Transaction monitoring is an on-going review of transaction data to look for outlying patterns and/or unusual activity.

24.4 A formal analysis of all high risk clients should be conducted taking into account the transaction history, comparision of expected verses actual activity, and documents results and action taken. All records must be maintained for a minimum period of five years (Refer to sections 15 to 18 of the FTRA and section 28 of this Code).

24.5 Having regard to the size, volume of financial services business and complexity of such business, firms should ensure that documents, data or information collected under the due diligence process is kept up-to-date and relevant, through periodic reviews of existing records, particularly for high risk clients. The process by which records are kept current should be

documented as part of the record-keeping policies.

25. OUTSOURCING OF MATERIAL FUNCTIONS

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

25.2 Lawyers and law firms 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.

25.3 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. Lawyers and law firms 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

26 Group Level Information Sharing

26.1 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.

26.2 From a law firm perspective, branches should be required to implement firm-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 firm-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.

26.3 Law firms 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, firms 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

27 Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

27.1 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. Laws firms are advised to take note of FATF Recommendations 27 and 35.

27.2 Targeted Financial Sanctions Related to Proliferation

27.2.1 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.

27.2.2 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

28. Statutory requirements to maintain records

28.1 Law firms shall maintain all books and records[25] 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 law firm 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.

28.1.2 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 law firm satisfies itself that copies are reproductions of the original documentation. The files should also indicate, in relevant circumstances, where the original can be located.

28.1.3 The records prepared and maintained by any law firm 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 firm's observance of AML policies and procedures;
- any transactions effected via the firm can be reconstructed; and
- the firm can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities for disclosure of relevant information.

28.2 Retention period to maintain verification records

28.2.1 Records relating to the verification of the identity of facility holders, including account files, business correspondence, and copies of all documents evidencing the identity of facility holders and beneficial owners, and the results of any analysis undertaken in accordance with

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

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 facility holder. In keeping with best practices, the date when a person ceases to be a facility holder 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 the facility; or
iii) the commencement of proceedings to recover debts payable on insolvency.

28.2.2 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.

28.2.3 Records relating to the verification of the identity for any transaction conducted through a facility of an intermediary shall be maintained for a period of not less than five (5) years after the intermediary ceases to be a facility holder.

28.2.4 Where a firm verifies the identity of any person by confirming the existence of a facility provided by an eligible introducer financial institution, the records that must be maintained are such that they enable the FIU to identify, at any time, the identity of the eligible introducer financial institution, the identity of the relevant facility and the identity confirmation documentation of the verification subject.

28.3 Transaction records

28.3.1 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.

28.3.2 Records of any findings pursuant to section 11(1)(a) of the FTRA and related transaction information shall be maintained for at least five years from the date of the transaction.

28.3.3 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.

28.3.4 The investigating authorities also need to be able to establish a financial profile of any suspect facility. For example, in addition to information on the beneficial owner of the facility and any intermediaries involved, the volume of funds flowing through the facility 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.

28.3.5 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;
- where applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by the law firm) directly involved in the transaction; and
- all other files and business correspondence and records connected to the facility.

28.4 Format of records

28.4.1 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 law firms 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.

28.5 When records are not required to be kept

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

28.5.2 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.

28.6 Mandatory destruction of records

28.6.1 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 law firm, or for the detection, investigation or prosecution of any offence.

28.7 Record keeping offences

28.7.1 Law firms 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, law firms 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

29 THE FINANCIAL INTELLIGENCE UNIT (FIU)

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

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

29.1.3 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.

29.1.4 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.

29.2 Mandatory requirement to appoint a Money Laundering Reporting Officer

29.2.1 All law firms engaged in prescribed financial services are required by law[26] 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. Lawyers and law firms 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 firm.

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

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

29.3.1 The Role of the MLRO

The person appointed as the MLRO has significant responsibility to the firm and should be sufficiently senior to exercise the necessary authority, competent and familiar with statue laws governing the firm. The size and nature of the firm should be a determining factor in selecting the individual to hold the position. Larger firms may choose to appoint, as appropriate to the circumstances, a senior member of their compliance department. In small firms, 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.

29.3.2 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.

29.3.3 In making this judgment, the MLRO should consider all other relevant information available within the law firm 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.

29.3.4 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.

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

29.3.6 The Commission has oversight of a diverse group of business types and sizes. In practical terms, designated law firms (or relevant profession) may vary from the sole proprietorship to large businesses with huge organizational structures. Nonetheless, each MLRO should

diligently perform the requisite duties in the most professional manner. This area will be reviewed during the on-site examination of the firm.

29.3.7 Financial institutions supervised by the Commission are at liberty to appoint a person to serve as MLRO once they are satisfied that the individual meets at least the core competencies outlined below, i.e. the MLRO should:

- have a sound understanding of what constitute money laundering, terrorist and proliferation financing;
- have a clear understanding of the inherent risks and vulnerabilities of his financial institution;
- have a basic knowledge of AML laws, rules and regulations in The Bahamas and international laws which may affect the operations of the firm;
- be given sufficient authority and independence to perform his duties;
- to the extent possible, be a Senior Officer within his institution; and
- be exposed to AML training at least once annually.

29.3.8 During the routine and/or random on-site examination, the Commission will determine whether the financial institution has complied with the above requirements.

29.4 Mandatory requirement to appoint a Compliance Officer

29.4.1 Laws firms, in accordance with prescribed financial services, are required by law[27], to appoint a Compliance Officer (CO). The designated CO must be at senior management level to be responsible for the implementation of an on-going maintenance of the identified risk, internal procedures and controls of the firm. 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.

29.5 Recognition of Suspicious Transactions

29.5.1 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 for that type of facility. 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 open a facility or execute the initial transaction.

[27] See section 20 of the FTRA

29.5.2 Section 12 (2) of the POCA requires that any person who knows, suspects or reasonably ought to have known or suspected that another person is engaged in money laundering or committing an offence related to an identified risk; proceeds of drug trafficking or any related crime and fails to report such knowledge or suspicion is guilty of an offence.

29.5.3 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.

29.5.4 Whistleblowing is an important mechanism in the prevention and detection of improper conduct, fraud and corruption. The firm should implement an appropriate policy, which shall raise awareness of the whistleblowing process and raise concerns about improper conduct within in the firm. 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.

29.6 Internal Reporting of Suspicious Transactions

29.6.1 The FI(TR)R requires law firms 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.

29.6.2 All law firms 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.

29.6.3 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 law firms 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.

29.6.4 All law firms 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.

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

29.7 Procedure for reporting suspicious transactions to the FIU

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

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

29.7.3 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 law firm may be required by the FIU to discontinue the transaction or cease activity related to the client's facility.

29.7.4 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 law firm 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.

29.7.5 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 law firm may leave itself open to risks as a constructive trustee if moneys are paid away other than to the true owner. The law firm 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 facility holder.

29.7.6 Law firms are reminded that reporting to the Commission, the Central Bank, the Commissioner of Police and any duly authorized employee of the law firm 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 law firm 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.

29.7.7 Following the submission of a disclosure report, a law firm 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.

29.7.8 The adequacy of the law firm's AML program to identify and properly report suspicious activity should be periodically reviewed.

29.8 Feedback from the FIU

29.8.1 The provision of general feedback to the financial sector on the volume and quality of disclosures and on the levels of successful investigations arising from the disclosures will be provided on a regular basis by the FIU.

29.8.2 Where applicable, law firms should ensure that all contact between particular departments/branches with the FIU and law enforcement agencies is reported back to the MLRO so that an informed overview of the situation can be maintained. In addition, the FIU will continue to provide information on request to a disclosing institution to establish the current status of a specific investigation.

29.9 TIPPING OFF

29.9.1 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.

29.9.2 In cases where the lawyer/law firm forms a suspicion of ML/TF, and it is reasonably believed that performing a CDD process will tip-off the client, the firm 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.

29.9.3 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.

29.9.4 Pursuant to section 16 & 18 of POCA, law firms 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.

I. STAFF RECRUITMENT, EDUCATION AND TRAINING PROCEDURES

30 KNOW YOUR EMPLOYEE (KYE) PROCEDURES

30.1 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.

30.2 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 firm. To this end, the firm's screening process, for the employees, must allow the firm 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).

30.3 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.

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

31. STAFF AWARENESS PROGRAMMES

31.1 Law firms 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.

31.2 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.

31.3 It is important that all law firms covered by this Code introduce adequate measures to ensure that staff members are fully aware of their responsibilities. To strengthen the firm'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.

32. STAFF EDUCATION AND TRAINING PROGRAMMES

32.1 Timing and content of training for various sectors of staff will need to be adapted by individual firms 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.

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

32.2.1 New employees

32.2.1-1 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 firm for the reporting of suspicious transactions.

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

32.2.2-1 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.

32.2.2-2 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 facility holder, particularly where large transactions, travelers' cheques or postal money orders are involved. They should be reminded of the need for extra vigilance in these instances.

32.2.2-3 In addition to the above, further training should be provided regarding the need to verify a customer's identity and on the business' own facility creation and client verification procedures. All employees should be familiarized with the firm's suspicious transaction reporting procedures.

32.2.3 Administration/operations supervisors and managers

32.2.3-1 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 **Appendix C** for a summary of these offences).

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

32.2.4-1 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 firms 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

Money Laundering /Terrorist Financing Offences, Penalties and Defences Money Laundering Offences

The POCA establishes several specific money laundering offences and penalties. In performing their functions, law firms should pay particular attention to the vulnerabilities of their service inherent in these offences.

N.B. THE OFFENCES UNDER THE POCA APPLY TO ALL PERSONS AND ARE NOT LIMITED ONLY TO THOSE CIRCUMSTANCES WHERE A LAWYER IS ACTING AS A FINANCIAL INSTITUTION. THEY ARE THEREFORE APPLICABLE TO RELEVANT CIRCUMSTANCES AFFECTING THE GENERAL PRACTICE OF LAWYER UNLIKE THE FTRA WHICH IS RESTRICTED TO THOSE CIRCUMSTANCES IN WHICH A LAWYER IS ACTING AS A FINANCIAL INSTITUTION.

In addition, there are many offences which arise from failing to comply with certain requests or obligations imposed under the FTRA, the Financial Intelligence Unit Act and the Regulations made pursuant to these Acts. A matrix of these offences also appears hereunder.

(1) MONEY LAUNDERING OFFENCES, PENALTIES AND DEFENCES UNDER POCA

For the purposes of the POCA, the term “criminal conduct” means conduct relating to the commission of any offence.

The term “property” under the POCA means, all property wherever situated and includes money, all forms of property, real or personal, heritable or moveable, things in action and other intangible or incorporeal property.

Offence	Penalties	Defences
Concealing (Section 9) It is an offence to conceal, disguise, convert, or transfer the proceeds of any crime or remove the proceeds of any crime from The Bahamas. For this offence, references to concealing or disguising criminal property includes concealing or disguising the proceeds of any identified risk activity, nature, source,	On summary conviction - imprisonment for a term not exceeding 7 years or a fine not exceeding $500,000 or both. On conviction on indictment - imprisonment for a term not exceeding 20 years or a fine or both.	A person does not commit an offence: - if he makes an authorized disclosure under section 19 and (if the disclosure is made before he does the act) he has the appropriate consent; - if he intended to make such a disclosure but had a

location, disposition, movement or ownership or any rights with respect to the property. This section applies where a person acts with knowledge or with reasonable suspicion.		reasonable excuse for not doing so; or - if he does an act for the purposes of carrying out his functions relating to the enforcement of any provision of this Act.
Arrangements Concerning Proceeds of Crime (Section 10). It is an offence for any person to enter into an arrangement if a person knows, suspects, or ought to reasonably have known or suspected that he has entered or is entering into an arrangement which facilitates, by whatever means, the acquisition, retention, use, concealment or the control of proceeds of crime by or on behalf of another person if he	On summary conviction - imprisonment for a term not exceeding 7 years or a fine not exceeding $500,000 or both. On conviction on indictment - imprisonment for a term not exceeding 20 years or a fine or both.	A person does not commit an offence: - if he makes an authorized disclosure under section 19 and (if the disclosure is made before he does the act) he has the appropriate consent; - if he intended to make such a disclosure but had a reasonable excuse for not doing so; or - if he does an act for the purposes of carrying out his functions relating to the enforcement of any provision of this Act.

Offence	Penalties	Defences
Acquisition, Possession or Use (Section 11) It is an offence to acquire, use or possess the proceeds of crime if a person knows, suspects, or ought to reasonably have known or suspected it was a proceed of crime.	On summary conviction - imprisonment for a term not exceeding 7 years or a fine not exceeding $500,000 or both. On conviction on indictment - imprisonment for a term not exceeding 20 years or a fine	A person does not commit an offence: - if he makes an authorized disclosure under section 19 and (if the disclosure is made before he does the act) he has the appropriate consent; - if he intended to make such a disclosure but had a

	or both.	reasonable excuse for not doing so; or - if he does an act for the purposes of carrying out his functions relating to the enforcement of any provision of this Act.
Failure To Disclose (Section 12) For an offence to be committed, three conditions must be satisfied. First, the person must know or suspect or reasonably ought to have known or suspected that another person is engaged in money laundering or committing an offence related to an identified risk. Second, the information on which his knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion came to him in the course of business. Third, that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him. This section applies to a person, firm or sole practitioner engaged in accountancy, audit or taxation advice or legal services involving the participation in financial or real property transactions.	On summary conviction - imprisonment for a term not exceeding 12 years or a fine not exceeding $500,000 or both. On conviction on indictment - imprisonment for a term not exceeding 20 years or a fine or both.	A person does not commit an offence: - if he has a reasonable excuse for not disclosing the information or other matter; or - if he does not reasonably know or suspect that another person is engaged in money laundering or an identified risk activity.
Tipping Off (Section 14) A person commits an offence if he knows or suspects that any disclosure regarding money laundering has been made or an action has been taken by the	On summary conviction - imprisonment for a term not exceeding 12 years or a fine not exceeding $500,000 or both.	

Financial Intelligence Unit relating to money laundering and he makes a disclosure to another person which is likely to prejudice any investigation which might be conducted following the disclosures.	On conviction on indictment - imprisonment for a term not exceeding 20 years or a fine or both.	

(2) MONEY LAUNDERING RELATED OFFENCES UNDER THE FTRA & FI(TR)R

These offences relate to the various AML obligations imposed on financial institutions.

Offence	Penalties	Defences
Failing or refusing to provide records, information or explanation when required to do so by the Commission (Section 34(2)) It is an offence for any person to fail or refuse to produce any record or to supply any information or explanation as required by the Commission.	On summary conviction – a fine not exceeding $50,000 or imprisonment not exceeding 3 years or both a fine and imprisonment.	
Failure to Comply with Identification Requirements (Section 47) It is an offence for a financial institution which intentionally fails to undertake the identification of a facility holder or otherwise to fulfil the identification or other requirements of the facility holder in accordance with subsections (2) – (5) of section 6.	On summary conviction – imprisonment for up to 5 years or a fine up to $500,000 or both.	
Recordkeeping Offences (Sections 18 and 47(d)) It is an offence for a financial institution when it fails without	On summary conviction – a fine not exceeding $20,000 maximum for an individual and $100,000	A person does not commit an offence: - if he can prove that he took

reasonable excuse, to retain or to properly keep records. It is an offence when a financial institution intentionally fails to maintain books and records as required by section 16, or destroys or removes such records, or fails to make such information available in a timely manner in response to a lawful request for such books or records.	maximum in the case of a corporation. On summary conviction - imprisonment for up to 5 years or a fine up to $500,000 or both.	all reasonable steps to ensure that he complied with that provision or that in the circumstances of the particular case, he could not reasonably have been expected to ensure that he complied with the provision.
Failure to Report Suspicious Transactions (Section 49) It is an offence for a financial institution which intentionally fails to submit a report to the Financial Intelligence Unit as required by sections 25 ad 26.	On summary conviction – imprisonment up to 5 years or a fine up to $500,000 or both.	A person does not commit an offence: - if he can prove that he took all reasonable steps to ensure that he complied with that provision or that in the circumstances of the particular case, he could not reasonably have been expected to ensure that he complied with the provision.

(3) (a) TERRORIST FINANCING OFFENCES UNDER THE ATA

Offence	Penalties	Defences
Offence of Terrorism (Section 14) It is an offence for a person in or out of The Bahamas to carry out an act: (a) that constitutes an offence under any of the Treaties listed in the First Schedule; or (b) any act for the purpose of	On conviction on information where death ensues and where that act would have constituted the offence of murder or treason, may be sentenced to death or in any other case is liable to	

intimidating the public or compelling a government/international organization to do or to refrain from doing anything that is intended to cause - a. death or serious bodily harm to a civilian; b. serious risk to health or safety of the public; c. substantial property damage; d. serious interference with an essential service, facility or system; e. prejudice to national security or disruption of public safety including in the provision of emergency services, to any computer or electronic system or to the provision of services directly related to banking, communications, infrastructure, financial services, public utilities, transportation or other essential infrastructure; or f. cybercrime resulting in any offence under this Act.	imprisonment for life.	
14(2) –It is an offence for a person or terrorist entity in or out of The Bahamas (a) to commit the offence of terrorism directly or indirectly, unlawfully and willfully; (b) to participate as an accomplice in the offence of terrorism or the financing of terrorism (c) to organize or direct others to commit the offence of terrorism or the financing of	On conviction on information where death ensues and where that act would have constituted the offence of murder or treason, may be sentenced to death or in any other case is liable to imprisonment for life	

terrorism or (d) to contribute to the commission of the offence of terrorism of the financing of terrorism.		
Offence of Financing of Terrorism (Section 15) It is an offence for any person to provide or collect funds; or provide financial services or make such services available to persons, whether by means that are direct or indirect, unlawful and willful with the intention or knowledge that the funds or services are to be used in full or in part (a) in order to carry out an offence of terrorism, (b) by a terrorist or by a terrorist organization for any purpose, (c) to conduct an act that constitutes an offence in any of the Treaties listed in the Schedule (d) in order to facilitate travel by an individual to a foreign State for the purpose of carrying out a terrorist act, or participating in or providing instruction or training to carry out a terrorist act (e) by a listed entity (f) by an entity owned or controlled directly or indirectly by a listed entity (g) by a person or entity acting on behalf of or at the direction of a designated person or listed entity (h) to facilitate the travel or activities of a foreign terrorist fighter (i) to carry out any other act to intimidate the public or compel the government to do or refrain from doing an act or it is	A person, or director or person in charge of a legal entity is liable on conviction on indictment to a fine of up to twenty-five million dollars and to imprisonment for twenty-five years. Where a body corporate or its director, manager or other similar officer is convicted, the Court shall have the power to (a) revoke business licenses (b) order that the body corporate be wound up (c) forfeit the assets and properties of the body corporate to the Confiscated Assets Fund (d) prohibit the body corporate from performing any further activities.	

intended to cause death or serious bodily harm or any damage mentioned in section 14(1).		
Reporting Requirements (Section 49) It is an offence for a financial institution to know or have reasonable grounds to suspect that any funds maintained on its books are by any individual entity or legal entity who (a) commits terrorist acts or participates in or facilitates the commission of terrorists acts or the financing of terrorism; (b) is a designated entity; (c) is a listed entity and the financial institution fails to report the existence of such funds to the FIU.	Liable on summary conviction to a fine not exceeding two hundred and fifty thousand dollars ($250,000).	
Financing of Proliferation of Weapons of Mass Destruction (Section 9) It is an offence for any person who provides financial services or makes such services available to persons or attempts to do so whether by means that are direct or indirect, unlawful and willful with the intention or knowledge that the funds or services are to be used in full or in part (a) to manufacture, develop or produce or participate in the development or production of a nuclear, biological or chemical weapon for use in terrorists acts (b) to distribute, or supply a nuclear, biological or chemical weapon to carry out a terrorist act (c) to train groups of persons to develop or	A person, or director or person in charge of a legal entity is liable on conviction on indictment to a fine of up to twenty-five million dollars and to imprisonment for twenty-five years. Where a body corporate or its director, manager or other similar officer is convicted, the Court shall have the power to (a) revoke business licenses (b) order that the body corporate be wound up (c) forfeit the assets and properties of the body corporate to the Confiscated Assets Fund (d) prohibit the body corporate from performing any	A person does not commit an offence if he can show that he did not know and had no reasonable cause to believe that the object was a weapon for the purposes of those sections.

produce or participate in the development of a nuclear, biological or chemical weapon for use by a terrorist or terrorist organization (d) conducts and constitutes an offence under the Treaties listed in the Schedule (e) to carry out any other act to intimidate the public or compel the government to do or refrain from doing an act or it is intended to cause death or serious bodily harm or any damage.	further activities.	
Duty to disclose information relating to offences and terrorist acts (Section 69 (1) It is an offence for any financial institution who has any information which will assist in (a) preventing the commission by another person, of a terrorist act or (b) securing the arrest or prosecution of another person for an offence under the ATA and fails to disclose the information to the Commissioner of Police or the Director of Public Prosecutions.	Liable on conviction on indictment to a fine of ten thousand dollars ($10,000) and to imprisonment for two (2) years.	
Procedure for designated entities (Section 44) When a financial institution receives the list of designated entities referred to in section 43(2)(a) or (d) it shall (a)(i) freeze all funds held by it in the name of a designated entity, (ii) inform the Attorney general and FIU that a designated		

entity has funds with the financial institution (iii) inform the designated entity that the funds have been frozen.		

The ATA incorporates all offences contained in the Treaties listed in its First Schedule, which are reproduced in 3 (b) below. It is important to note that terrorism offences in the ATA have been incorporated into the list of predicate offences appearing in the First Schedule of POCA and thereby subject to the requirement imposed upon law firms under the FTRA and the FIUA. Section 50 of the ATA requires the reporting of offences under the Act to be made to the Commissioner of Police.

(3) (b) THE SCHEDULE TO THE ATA

LIST OF TREATIES RELATIVE TO TERRORISM

1. Convention on offences and certain other Acts committed on Board Aircraft signed at Tokyo 14th September, 1963.
2. Convention for the Suppression of Unlawful Seizure of Aircraft, done at the Hague on 16th December, 1970.
3. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23rd September, 1971.
4. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14th December, 1973.
5. International Convention against the taking of Hostages, adopted by the General Assembly of the United Nations 17th December, 1979.
6. Convention on the Physical Protection of Nuclear Material signed at Vienna on 3rd March, 1980.
7. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 24th February, 1988.
8. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10th March, 1988.
9. Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10th March, 1988.
10. Convention on the Marking of Plastic Explosives for the Purpose of Detection, signed at Montreal on 1st March, 1991.

11. International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15th December, 1997.
12. International Convention for the Suppression of the Financing of Terrorism adopted by the General Assembly of the United Nations on 9th December, 1999.
13. The Biological Weapons Convention entered into force on 26th March 1975.; and
14. The Chemical Weapons Convention (CWC) adopted by the Conference on Disarmament in Geneva on 3rd September 1992.

APPENDIX C

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 customer/client or beneficial owner is a politically	14	Very Serious	Up to $200,000.	Up to $50,000.

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.

APPENDIX D

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 E

LEGAL PROFESSION - TYPOLOGIES

Source: PROFESSIONAL MONEY LAUNDERING (2018 | FATF Report) - United States

A Complicit Lawyer and Bank Employee

A lawyer in Texas was convicted for laundering money for an Organized Crime Groups (OCG) and engaging in a variety of fraud schemes. The OCG operated in the US, Canada, Africa, Asia and Europe. A complicit bank employee was also convicted for her role in creating counterfeit checks and monitoring money flows between the numerous accounts controlled by the OCG.

All of the victims of these various fraud schemes were instructed to wire money into funnel accounts held by other co-conspirators (money mules), who then quickly transferred the money to other US accounts as well as accounts around the world before victims could discover the fraud. Several millions of dollars were laundered in this manner. The numerous bank accounts opened by the mules served as the initial “layer” in the laundering process, which allowed coconspirators to distance or conceal the source and nature of the illicit proceeds. For example, during a one-year period, a key money mule opened 38 fraudulent bank accounts.

The fraud schemes took several forms. Many victims were law firms that were solicited online, provided counterfeit cashier’s checks for deposit into the firms’ trust accounts. The law firms were then directed to wire money to third-party shell businesses controlled by the co-conspirators. The fraud conspiracy also employed hackers who compromised both individual and corporate e-mail accounts, ordering wire transfers from brokerage and business accounts to shell accounts controlled by co-conspirators. The shell companies were incorporated in Florida with fictitious names and then used to open bank accounts at banks in Florida in those names.

The licensed attorney in Texas worked for the co-conspirators by laundering victim money through an interest on lawyers’ trust account (IOLTA)[28]. He also met with individual money mules to retrieve cash from their funnel accounts. The lawyer recruited his paralegal and others to open accounts used in the laundering scheme.

28 An IOLTA is an account opened by an attorney with the intention of holding client funds for future services. It is opened at a bank with a presumed higher level of confidentiality accorded to attorney-client relationships and related transactions.

Source: PROFESSIONAL MONEY LAUNDERING (2018 | FATF Report) – Italy

Operation CICERO

This case was initiated by a special currency police unit within the Guardia di Finanza as a follow-up investigation to a judicially authorized search conducted on the boss of a major organized crime group (La Cosa Nostra or LCN) in Palermo, Italy. This investigation was aimed at identifying those individuals acting as nominees, as well as individuals who facilitated the movement of criminal proceeds on behalf of LCN. The investigation identified that a well-known lawyer was the beneficial owner of the companies used to launder funds via a Palermo-based construction company, which was linked to family members of the organized crime boss.

The lawyer performed a “money box” function for the LCN, which consisted of managing the financial resources of the crime group with the purpose of concealing the origins of the illicit proceeds and avoiding detection by authorities of any assets purchased from these proceeds. Through his professional relationships, the lawyer developed and tapped into an elite social network, which he also made available to the organized crime group.

The lawyer, who was operating as a PML, conducted a number of services, such as: (a) obtaining a mortgage to purchase an apartment with EUR 450 000 in criminal proceeds on behalf of an organized crime family member; (b) using a fictitious contract to purchase an apartment with EUR 110 000 on behalf of the organized crime group; and (c) layering and integrating legal funds with criminal assets derived from construction work carried out on land purchased with criminal proceeds.

This investigation led to confiscation proceedings against nine individuals totaling EUR 550 000 as well as seven properties owned by the lawyer.

Source: APG Typologies Report 2013 - Malaysia

Malaysia Ponzi scheme Perpetrated by Professional (Lawyer)

311. Methods used:

- Use of nominees or third parties etc.
- Use of professional services (lawyers)
- Real estate

312. Mr. A was a lawyer turned businessman where he established a property investment company which offered services to investors to buy properties at a lower price and an option to re-sell at higher price. The difference between the purchase price and selling price would be distributed to the investors as investment return. In addition, all the investors were required to pay a substantial amount in member fees to the company annually.

313. Mr. A appointed two legal firms to complete the legal documentation on the sales and purchase transactions on the properties for the investors.

314. Initially, the investment scheme was carried out in accordance with the law. However, as the number of members grew, Mr. A and his team could not obtain sufficient optional-properties to meet the demand of the increasing investors. He started to hire proxies by recycling the properties among the existing investors, proxies and the new investors. The same units of properties were sold and resold to investors via proxies and new investors at a different price. The profit would then be ploughed back to the investors to gain trust and confidence for further investment, which resulted in the value of investments multiplying tremendously.

315. Investors were initially not suspicious of the investment scheme by the investment company because the monies needed to purchase the invested 56 optional properties were deposited into a trust account opened by the two legal firms. They trusted that the lawyers would carry out due diligence work on the optional properties they had purchased.

316. However, the monies that the investors banked-in were then partially paid as return to the other investors, but the majority of it was siphoned out by Mr. A. Approximately 100 million of ringgit (USD31,721,967) was transferred out to a foreign country before Mr. A and his family absconded from the country.

317. The investigation revealed that the investment scheme had lured a total of 500 investors, who suffered losses of 250 million ringgit (equivalent to USD76 million), while the 200 properties registered under proxies' name were valued at not more than 70 million ringgit (equivalent to USD21 million). The case is currently being investigated for cheating and money laundering offences.

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 Legal Professionals
   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 Legal Professionals
   http://www.fatf-gafi.org/