THE INSURANCE COMMISSION
OF THE BAHAMAS

GUIDELINES FOR
INSURANCE COMPANIES:

ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM & PROLIFERATION FINANCING

AML/CFT/PF Guidelines

Date of Last Issue: March 31, 2016
Revised: September 30, 2018

THE INSURANCE COMMISSION OF THE BAHAMAS

Poinciana House-North Building,
31A East Bay Street
P.O. Box N-4844
Nassau, Bahamas

Tel: (242) 328–1068
Fax: (242) 397-4100
E-mail: policies@icb.gov.bs
Website: www.icb.gov.bs

EXPLANATORY FOREWORD

The Insurance Commission of The Bahamas "the Commission" has power under section 8 of the Insurance Act, Chapter 347 to ensure that insurance companies comply with the requirements of the Financial Transactions Reporting Act and other anti-money laundering (AML) and combating the financing of terrorism (CFT) and proliferation financing (PF) provisions found in the AML laws. The Commission has responsibility for the AML supervision of licensees, including the facilitation of the AML examination process. For this purpose, the Commission has issued these Guidelines for insurance companies. Copies of all AML Guidelines issued by the Commission are available electronically on its website.

Obligations imposed by these Guidelines are enforceable in accordance with the Insurance Act, Chapter 347, Insurance (General) Regulations, 2010, External Insurance Act, Chapter 348, Proceeds of Crime Act, 2018, Financial Transactions Reporting Act, 2018 (FTRA), Financial Transactions Reporting Regulations, 2018 (FTRR), Financial Intelligence (Transactions Reporting) Regulations (FITRR), 2001 and the Anti-Terrorism Act, 2018.

All references in this document to AML include obligations for CFT and PF under the Anti-Terrorism Act, 2018 unless the context requires otherwise.

Long term insurance companies are identified as financial institutions subject to AML regulation by virtue of section 3(1)(b) and (h)(iv) and (v) of the FTRA, 2018. Pursuant to section 25 – 30 of the FTRA and regulation 14, general insurance companies are required to report suspicious transactions.

These Guidelines apply to all persons or companies registered to provide insurance business in and from within The Bahamas. Notwithstanding the exemptions given to general insurance companies in relation to AML requirements, persons or companies registered to carry on general insurance business are required to comply with these guidelines particularly the guidance on customer due diligence, know your customer measures and risk management. The Commission further requires that all measures are carried out utilizing a risk based and best practice approach, after taking into consideration the size, nature, and complexity of the licensees' insurance operations.

These Guidelines are intended to provide insurance companies with practical guidance and examples of good practice on how to implement the requirements of the AML/CFT legislation. It also supports the regulatory objective of maintaining the reputation of The Bahamas as a first-rate international financial centre with zero tolerance for criminal activity.

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 will continue to issue periodic directions to supplement these Guidelines as changing circumstances dictate.

MICHELE C. E. FIELDS
SUPERINTENDENT OF INSURANCE

September 30, 2018

INDEX

A. DEFINITIONS

"AML" means anti-money laundering.

"AML laws" means the Proceeds of Crime Act, the Financial Transactions Reporting Act, the Financial Intelligence Unit Act, the Anti-Terrorism Act 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.

"beneficiary" means the person named in a life insurance policy to receive the insurance proceeds upon the death of the policyholder or upon the maturity of an endowment.

"beneficial owner" means the natural person(s) who ultimately owns or controls a customer and and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

"cash" means notes and coins in any currency and includes postal orders, cheques of any kind including travelers' cheques, bankers' drafts, bearer bonds bearer shares and virtual currency, coins, paper money, travelers' cheques, postal money orders and other similar bearer-type negotiable instruments.

"CFATF" means the Caribbean Financial Action Task Force.

"CFT" means combating the financing of terrorism.

"CPF" means countering proliferation financing.

"CO" means Compliance Officer.

"company" means a body corporate licensed under the Insurance Act, Chapter 347.

"the Commission" means the Insurance Commission of The Bahamas established under section 4 of the Insurance Act, Chapter 347.

"licensees" means the insurance companies licensed by the Commission under the Insurance Act, Chapter 347 for which the Commission has AML/CFT supervisory responsibility.

"customer" means policyholder or beneficial owner.

"customer due diligence" or "CDD" – The objective of customer due diligence which is sometimes referred to as KYC, is to ensure that reasonable steps are taken to satisfy the insurer that the customer and/or beneficial owner is who he claims to be and that his funds are derived from a legitimate source or are not intended to be used for terrorism.

"designated non-financial business and profession" has the meaning given to it in section 4 of the FTRA.

"eligible introducer" means –

(1) any other Bahamian financial institution under section 3 of the FTRA; or

(2) any foreign financial institution from a country that is:

- a licensed bank;
- a licensed trust company;
- a licensed casino;
- a person regulated by the equivalent of the Securities Commission of The Bahamas; and
- any designated non-financial business and professions regulated by the Compliance Commission.

"FATF" means the Financial Action Task Force.

"facility" is any account or arrangement that is provided by an insurance company to a client by, through or with which the client may conduct two or more transactions whether or not they are so used. A facility in the case of an insurance company is essentially any of those services that would qualify him to be a financial institution as set out in the preceding paragraph. It also specifically includes provision of facilities for safe custody, such as safety deposit boxes.

"facility holder" is the client and any person who is authorized to issue instructions in relation to how transactions should be conducted through a facility provided by the insurance company.

"financial institution" means a person or entity described in section 3 of the FTRA who or which provides financial intermediary services and on who have been imposed AML obligations pursuant to the AML laws.

"financial intermediary services" are those services defined in section 3(1)(b) and (h) of the FTRA which make a life insurance company, in relation to those services, a financial institution for AML purposes. Those services are where the company administers or manages funds on behalf of other persons or acts as trustee in respect of funds of other persons, i.e. any case in which a life insurance company facilitates the movement of funds, into, out of and around the financial system and includes being a signatory on the client's bank account irrespective of the location of the account or the location of the other signatories to the account.

"foreign financial institution" means a financial institution in a foreign jurisdiction that is subject to an equivalent regime of monitoring, supervision and regulation as is herein provided and is subject to equivalent or higher anti-money laundering and anti-terrorism financing standards of regulation as provided for by Bahamian law.

"FI(TR)R" means the Financial Intelligence (Transactions Reporting) Regulations, Ch. 367.

"FIU" means the Financial Intelligence Unit.

"FIUA" means the Financial Intelligence Unit Act, Ch. 367.

"FTRA" means the Financial Transactions Reporting Act, 2018.

"FTRR" means the Financial Transactions Reporting Regulations, 2018.

"insurance intermediary" means a broker, agent, sub-agent, adjuster, risk manager, consultant, or such other persons who give advice by way of directly offering, advertising or on a person-to-person basis in respect of an insurance product and includes the promotion of such product or the facilitation of an agreement or contract between an insurer and a customer.

"insured" means the party named on or in a policy or certificate.

"insurer" means any company carrying on insurance or reinsurance business and, except where otherwise stated, includes all the members of an association of underwriters that is registered as an insurer.

"know your client/customer" or **"KYC"** which is also referred to as customer due diligence, is designed to ensure that reasonable steps are taken to satisfy the firm that the client is who he claims to be and that his funds are derived from a legitimate source or are not intended to be used for terrorism.

"MLRO" means money laundering reporting officer.

"occasional transaction" means any one-off transaction including, but not limited to cash, that involves a payment, deposit, withdrawal, debit, repayment, encashment, exchange, or transfer of sums that is 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 in cash over $15,000 to the insurance company for the benefit of one of its facility holders.

"para." Means paragraph.

"POCA" means the Proceeds of Crime Act, 2018.

"policyholder" means the person who for the time being has the legal title to the policy and includes any person to whom a policy is for the time being assigned.

"politically exposed persons" or "PEPs" is the term used to describe natural persons who are or have been entrusted with prominent public functions, their immediate family members and persons known to be close associates of such persons. It includes:

(a) Heads of State, Heads of Government, Ministers and Deputy or Assistant Ministers;

(b) Members of Parliament;

(c) Senior government officials;

(d) Members of Supreme Courts, Constitutional Courts or other high-level judicial bodies;

(e) Members of Boards of Central Banks;

(f) Ambassadors, Charges d'affaires and high-ranking officers in the armed forces or law enforcement;

(g) Members of the Administrative, Senior Management or Supervisory Boards of government-owned enterprises;

(h) Immediate family members of any of the above such as:

- a spouse,
- a partner (including a person who is considered by his national law as equivalent to a spouse),
- siblings,
- children and their spouses, and
- parents;

(i) Persons known to be close associates of persons identified in (a) through (f) above, such as:

- any person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any close business relations, with a PEP, and

- any individual who has sole beneficial ownership of a legal entity or legal arrangement which has established for the benefit of a PEP.

"STR" means a suspicious transaction report.

"transaction" means any deposit, withdrawal, exchange or transfer of funds in cash, by cheque, payment order or other instrument, and includes electronic transfer of funds in cash.

B. BACKGROUND

This part describes the phenomenon of money laundering, terrorist financing, proliferation financing background and general introductory information on the money laundering and terrorist financing regulatory framework of The Bahamas and the global efforts against money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction.

It also covers the details of the supervisory framework of the Commission. This supervisory framework includes an on-site and off-site examination process for insurers and associations and AML/CFT/CPF education and training programme for insurance companies.

I. MONEY LAUNDERING, FINANCING OF TERRORISM, AND PROLIFERATION FINANCING

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 cash 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 in-directly, 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 imposes individual targeted sanctions (an assets freeze, travel ban, and arms embargo) upon individuals, groups, undertakings and entities designated on the ISIL (Da'esh) & Al-Qaida Sanctions List. The United Nations under UNSCR 1267 has produced a list of designate persons/countries with known or suspected terrorist connections. Licensees are required to acquaint themselves and include as a part of their AML/CFT guidelines, policies and procedures, all obligations under PART IV – Implementation of United Nations Security Council Resolutions, ss. 43-49, ATA. 2018.

2.4 Licensees are advised that this list is updated periodically. Once received by the Ministry of Foreign Affairs, it is forwarded to the Office of the Attorney General. The list of individuals or entities, and their associates, designated as terrorist entities by the Security Council of the United Nations is then circulated by the National Identified Risk Framework Coordinator. The Coordinator is also responsible for maintaining an updated list. (s.43, ATA, 2018)

3 PROLIFERATION FINANCING

3.1 Proliferation of Weapons of Mass Destruction (WMD) refers to chemical, biological, radiological, or nuclear weapons that are capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

3.2 Proliferation financing is the "act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".

3.3 All insurance companies are required to implement internal controls and procedures to prevent criminals from using them to facilitate proliferation financing. They should ensure that employees are trained and aware of the controls and procedures.

3.4 Licensees are encouraged to refer to the *FATF Guidance on Counter Proliferation Financing (www.fatf-gafi.org)* and The Bahamas' *Guidance Note of Proliferation and Proliferation Financing. (www.icb.gov.bs)*

4 Vulnerabilities in insurance

4.1 Certain points of vulnerability have been identified in the laundering process, namely:

- purchase of insurance products sold by brokers;
- entry of cash into the financial system;
- cross-border flows of cash; and
- transfers within and from the financial system

[1] See Appendix C

[2] UN 1999 International Convention for the Suppression of the Financing of Terrorism

4.2 Insurance companies as providers of certain financial intermediary services are susceptible to being used not only in the layering and integration stages, as has been the case historically, but also to disguise the origin of funds before placing them into the financial system.

4.3 The Financial Action Task Force (FATF) typologies of 2004-2005 identified the following money laundering vulnerabilities for insurance companies:

- investment type products (i.e. annuities)
- marine property and casualty contracts
- fraudulent insurance claims
- terrorist financing
- general insurance for goods likely to have been purchased with illegal funds

4.4 Insurance can be used in different ways by money launderers and terrorist financiers. The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (cash or bank transfer) and contract law. Insurers should take these factors into account when assessing this vulnerability. This means they should prepare a risk profile of the type of business in general and of each business relationship.

4.5 Examples of the type of life insurance contracts that are vulnerable as a vehicle for laundering money or terrorist financing are products, such as:

- unit-linked or with profit single premium contracts
- single premium life insurance policies that store cash value
- fixed and variable annuities
- (second hand) endowment policies

4.6 When a life insurance policy matures or is surrendered, funds become available to the policyholder.

4.7 Insurance companies should pay particular attention to the money laundering risks presented by the services which they offer to avoid being manipulated by criminals seeking to launder illicit proceed.

4.8 All insurance companies are required to implement internal controls and procedures to prevent criminals from using them as a facilitator for proliferation financing.

4.9 Insurance companies in The Bahamas are subject to the money laundering laws on two levels. On the first level, all insurance companies are subject to the provisions of the Proceeds of Crime Act, 2018. On the second level all life insurance companies that offer financial intermediary services as defined in the FTRA pursuant to section 3, are also subject to the AML regime contained in the Financial Intelligence Unit Act 2000 and all regulations and guidelines made pursuant to these Acts, in relation to those financial intermediary services. For the purposes of these services, the insurance company is deemed to be a financial institution under the FTRA.

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 main international body for tackling money laundering and terrorist financing. The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. Further information on the FATF can be found at www.fatf-gafi.org.

5.1.2 In February 2012 the FATF published its revised Forty (40) Recommendations on tackling money laundering and combating terrorism financing. Recently, the Recommendations were updated in February 2018. The 40 Recommendations set out the framework for AML and CFT initiatives and are designed for universal application. They provide a complete set of counter-measures against money laundering and terrorist financing covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

5.1.3 The FATF has also promoted the concept of regional organizations along the lines of its own structure, whose goals would be to raise awareness of money laundering, terrorist financing and proliferation financing and introduce regional evaluation programmes to monitor the implementation of the 40 Recommendations, amongst other things.

5.2 The Caribbean Financial Action Task Force (CFATF)

5.2.1 The CFATF was established 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.

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 www.cfatf@cfatf.org.

5.2.3 The Bahamas is one of the founding members of CFATF. The Bahamas' AML regime is evaluated every four years by CFATF.

5.3 International Monetary Fund (IMF) – Financial Sector Assessment Programme (FSAP)

5.3.1 The Bahamas, as a member of the IMF, also participates in the (FSAP). The FSAP, a joint IMF and World Bank effort introduced in May 1999, aims to increase the effectiveness of efforts to promote the soundness of financial systems in member countries. Supported by experts from a range of national agencies and standard-setting bodies, work under the program seeks to identify the strengths and vulnerabilities of a country's financial system; to determine how key sources of risk are being managed; to ascertain the sector's developmental and technical assistance needs; and to help prioritize policy responses. Detailed assessments of observance of relevant financial sector standards and codes (including the FATF's 40 Recommendations), which give rise to *Reports on Observance of Standards and Codes* (ROSCs) as a by-product, are a key component of the FSAP. These generally occur on a five-year cycle.

5.4 International Association of Insurance Supervisors (IAIS)

5.4.1 The Bahamas is a member of the International Association of Insurance Supervisors (IAIS), whose aim is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders. The IAIS also conducts its assessment of the supervisory authority's and its implementation of the *Insurance Core Principles*.

II. THE LEGISLATIVE AND REGULATORY STRUCTURE FOR AML/CFT IN THE BAHAMAS

6. THE LEGISLATIVE FRAMEWORK

6.1 The Bahamian substantive law relating to AML/CFT is contained in:

- the Proceeds of Crime Act, 2018
- the Financial Transactions Reporting Act, 2018
- the Financial Transactions Reporting Regulations
- the Financial Transaction Reporting (Wire Transfers) Regulations, 2018
- the Financial Intelligence Unit Act
- the Financial Intelligence (Transactions Reporting) Regulations, and
- the Anti-Terrorism Act, 2018

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

6.3 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 provide its part of the audit trail.

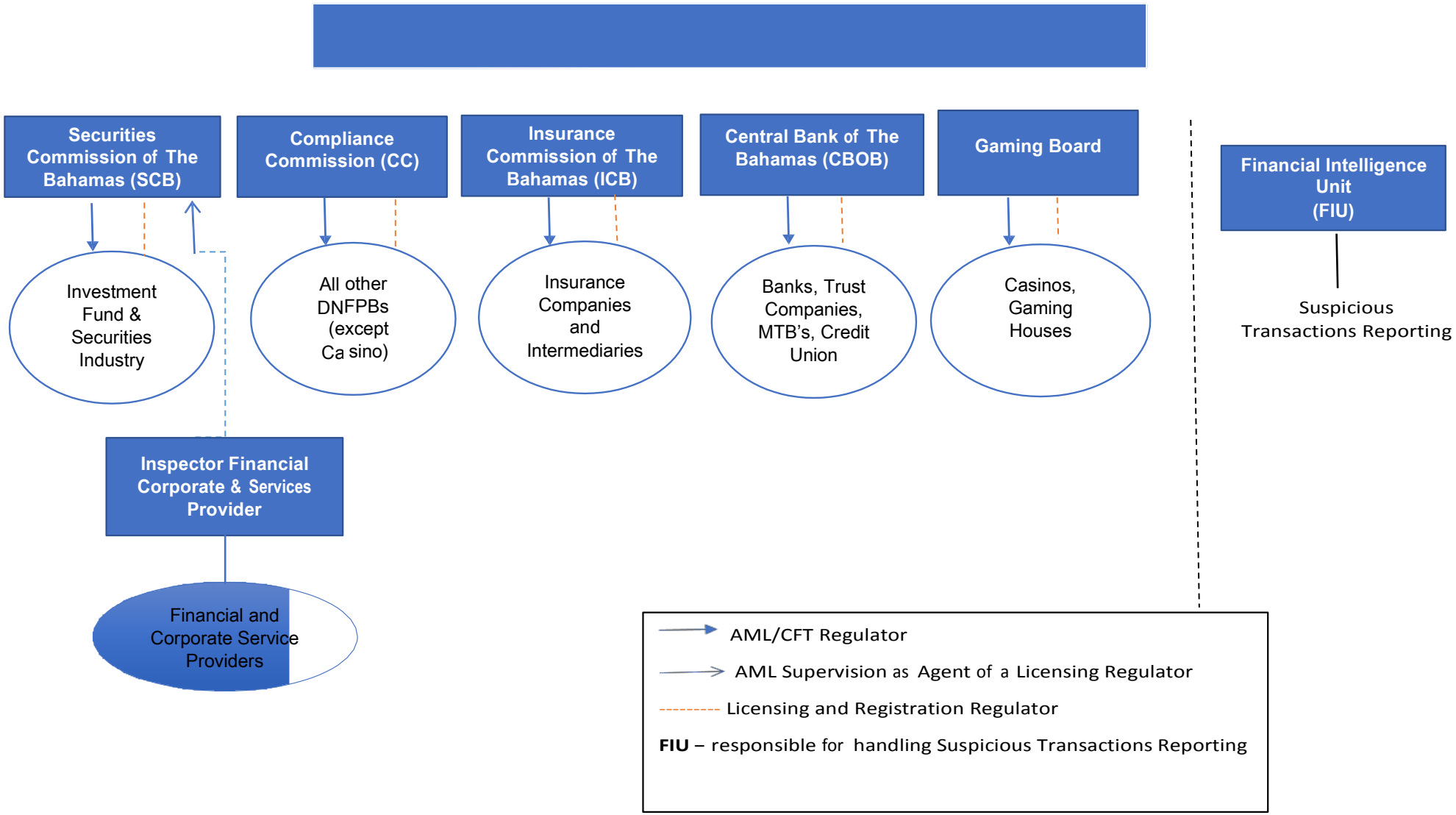
7. THE REGULATORY FRAMEWORK

7.1 The Commission supervises all licensees of the insurance industry and administers the AML on-site examination for this sector. All other sectors are regulated by the designated regulator. The authority for the Commission to supervise insurance companies is found in section 8 and 207 of the Insurance Act; and section 45 of the External Insurance Act.

7.2 The structure of the AML regulatory framework, specifically identifying licensees, is found in *Fig. 1* below. The Central Bank regulates the banking and trust companies industry, the Securities Commission regulates the securities and investment funds industry, the Inspector of Financial and Corporate Services regulates financial and corporate service providers and the Gaming Board regulates casinos and gaming houses.

7.3 The Financial Intelligence Unit or FIU is the agency charged, amongst other things, with receiving and analyzing suspicious transactions reports from financial institutions (See paras. 18.1 to 18.8 for more details about the FIU).

Figure 1. Regulatory Structure for AML in The Bahamas



III. THE INSURANCE COMPANY AS A FINANCIAL INSTITUTION

8 **When is an insurance company a financial institution?**

8.1 Where an insurance company is deemed to be a financial institution, it is required to comply with the AML/CFT/CPF obligations set out in the relevant legislation. The circumstances in which an insurance company is deemed to be a financial institution is set out below.

8.2 Life insurance companies in The Bahamas are considered financial institutions for AML/CFT/CPF purposes and are subject to the anti-money laundering and terrorist financing laws, pursuant to section 3 of the FTRA and thereby subject to supervision by the Commission where services rendered by them involve facilitating the entry or placement, movement, or removal of funds into, within or out of the financial system on behalf of clients in circumstances where the life insurance company merely acts in relation to those funds, as an agent, intermediary or conduit for the client.

8.3 In accordance with the FTRA, general insurance companies are not defined as financial institutions but are required to fulfil all obligations under sections 25-30 in relation to the reporting of suspicious transactions.

IV. SUPERVISORY FRAMEWORK OF THE COMMISSION

9. THE COMMISSION

9.1 The establishment of the Commission

9.1.1 Section 4 of the Insurance Act, Chapter 347 establishes the Commission as a body corporate for the purpose of ensuring that all companies carrying on insurance business (as set out in section 3 of the IA) comply with the provisions of the Insurance Act, Chapter 347 and the External Insurance Act, Chapter 348. The Commission consists of the Superintendent, Deputy Superintendent, three to five Commissioners appointed by the Governor-General.

9.2 How the Commission supervises life insurance companies for AML purposes

9.2.1 The Commission supervises life insurance companies, through a combination of on-site and off-site examinations, and education, training and awareness programmes. In addition, periodic notices and guidelines, intended to supplement the AML Guidelines are issued.

9.2.2 The Commission also has established a programme of engagement annually with the representative bodies of the insurance industry that it regulates. Separate consultative meetings are held regularly with the Superintendent and Analysts, amongst other bodies, to review the activities of the previous year and to discuss plans for the ensuing year.

10. THE EXAMINATION PROCESS

10.1 The Commission carries out its AML/CFT supervision of insurance companies by means of on-site and off-site inspection programmes.

10.2 Within this framework, there are four types of examination which the Commission administers:

- routine (which may be either an on-site or an off-site examination),
- follow-up,
- random (on-site only), and
- special (on-site only).

Further details on the procedures for the examination types can be found at para. 10.6 below.

10.3 On-Site Examinations

10.3.1 Under section 69 of the Insurance Act, Chapter 347, the Commission empowers to conduct on-site examinations.

10.3.2 The AML/CFT on-site examination is not an audit of the business activities. It is the process by which the Commission ensures that the AML/CFT laws are being fully complied with.

10.3.3 With the exception of the routine examination which is conducted by the external auditor, all other types of on-site examinations are conducted by the Commission's Supervision Unit.

10.4 Off-Site Examinations

10.4.1 In order to conduct an off-site examination, the licensee must first obtain from the Commission, a waiver from the routine on-site examination. A waiver request must be made in writing.

10.4.2 *Waiver from the routine on-site examination*

10.4.2-1 A waiver exempts an insurance company from the requirement to submit to a routine on-site examination during a given examination year. A waiver is granted based on all of the following criteria being met:

- the insurance company must have submitted to at least one (1) on-site examination;
- previous examination(s) should reveal that the company has complied with AML laws including relevant Policies and Procedures;
- the critical areas of the examination e.g. customer verification, suspicious transaction reporting, etc. reveal no deficiencies; and
- the company has not increased or added any class of insurance business within one year of its last examination.

10.4.2-2 Where a waiver has been granted, an insurance company will instead be required to conduct an off-site examination during such period.

10.4.2-3 For the off-site examination, the insurance company is required to have a Money Laundering Reporting Officer, or a Senior Officer approved by the Commission for this purpose, complete the examination form in-house and forward it onto the Commission's office. This completed examination form will be evaluated by the Commission's staff in the same manner as a return for an on-site examination. The Commission, in turn, will communicate any concerns arising from the assessment to the insurance company. (See para. 10.6.2-2 for the *Follow-up Examination* process).

10.4.2-4 The completed examination form must be submitted to the Commission within four (4) months of the end of the financial year.

During the period of a waiver, the financial institution is not precluded from selection for a random examination (see para. 10.6.3), or for a special examination (see para. 10.6.4), both of which are conducted by the Commission's Supervision Unit.

10.5 Types of examination

10.5.1 *Routine Examination*

10.5.1-1 The routine examination may take the form of either an on-site examination or an off-site examination. The examination form will be used to evaluate the insurance company's compliance levels.

10.5.1-2 The routine examination is designed to test the adequacy of AML/CFT/CPF systems that have been implemented by an insurance company for the purpose of meeting its obligations under the AML/CFT/CPF laws and regulations.

10.5.1-3 A life or non-life insurance company which has developed and enforces sound AML policies and procedures, poses less risk for money laundering and terrorist financing than one which has no or less stringent policies and procedures. Consequently, the higher the money laundering/terrorist financing risk, the more vigorous supervision will be applied.

10.5.1-4 The Commission's conducts the routine examination on a calendar year basis. For each annual period, all life insurance companies that provide financial intermediary services must submit those aspects of their business to a routine examination. The examination, (whether on-site or off-site), must be completed within four (4) months of the financial period.

10.5.1-5 A routine examination assesses the licensee's compliance with the AML laws i.e. the FTRA, FTRR, FI(TR)R and ATA these Guidelines and the FIU Guidelines. The examination reviews the procedures/practices in place for the five (5) operational areas of life insurance companies' activities as follows:

(1) the verification/identification of customers;
(2) maintenance of customer verification and transaction records;
(3) reporting of suspicious transactions to the FIU;
(4) assignment of a MLRO and CO; and
(5) the internal procedures for training personnel on money laundering detection and prevention as required by the FI(TR)R.

10.5.1-6 In the case of a routine on-site examination, once completed, the examining accountant should discuss the contents of the examination form with the financial institution. Upon completing the examination form the examining accountant must immediately submit the completed examination form to the Commission to be evaluated and no later than four (4) months after the financial year end. Please see *Appendix C* for an overview of the Commission's evaluation process. Those life insurance companies that receive an adverse rating on the routine on-site examination will be scheduled for a follow-up examination.

10.6.1-7 Frequency of the routine on-site examination

10.6.1-7(a) EXAMINATION PERIOD

> The Commission's examination year is based on the calendar year (1st January to 31st December).
>
> All life insurance companies are required to submit examinations returns within four (4) months of the financial year for off-site or on-site examinations.

10.6.1-7(b) The routine annual examination will be carried out on an annual basis unless the insurance company makes an application for a waiver.

Upon the written application for a waiver of an insurance company, the Commission will issue written directions to an insurance company regarding the next date for a routine on-site examination taking into account the following considerations:

- an evaluation of the insurance company's risk-based policies and procedures for combating money laundering and terrorist financing to determine their adequacy;
- whether the insurance company has met all of its examination requirements, dating back to the effective date of the FTRA, i.e. 25th May, 2018; and

an evaluation by the Commission of all previous examinations completed in relation to the insurance company to determine the insurance company's level of compliance with its statutory obligations under the AML/CFT/CPF laws and the Commission's Guidelines.

10.6.2 *Follow-up Examination*

10.6.2-1 Follow-up examinations are always on-site examinations and are solely for the purpose of addressing the deficiencies of the AML/CFT/CPF systems of life insurance companies that are revealed through the routine or off-site examination process. Such examinations are specific in scope and will focus on identified weaknesses. Follow-up examinations are conducted by the Commission's Supervision Unit.

10.6.2-2 Procedure for follow-up visits

10.6.2-2(a) Where an adverse rating is given, a Notice is issued advising of a follow-up examination. Unless otherwise stated, life insurance companies are given up to three (3) months to rectify all deficiencies discussed during the follow-up visit.

10.6.2-2(b) Below are the steps for Follow-up Examinations.

Step 1. The Commission contacts the insurance company to arrange a meeting with Management and/or the MLRO two (2) weeks prior to the meeting date. The purpose of the meeting is to discuss the results of the routine examination.

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

Step 3. A date is set within one (1) month for the Commission to revisit the

insurance company to determine the level of progress.

10.6.2-2(c) Where sufficient progress is evident, no further visit is made regarding those issues and a report to this effect is made.

10.6.2-2(d) However, if an insurance company does not adhere to the strategy outlined for resolving the inadequacies of their AML/CFT system the following steps below are taken. In addition, actions outlined in the AML/CFT Ladders of Intervention can also be taken.

Step 1. A letter is forwarded to the insurance company highlighting the details of previous meetings including minutes from any prior meeting reminding it of the agreed-upon strategy for addressing inadequacies of the entity. A period of two (2) weeks is given for the insurance company to rectify all inadequate systems.

Step 2. The examiner visits the insurance company at the end of the two (2) week period to determine whether the problems have been remedied.

Step 3. Where the systems are examined and seem adequate, a final report is written to this effect. If there is insufficient progress, a report is written and forwarded to the Commissioners who will determine whether legal action is to be pursued.

10.6.3 ***Random Examination***

10.6.3-1 In addition to the routine examination, life insurance companies are also subject to random on-site examinations by the Supervision Unit of the Commission. The primary purpose of the random examination is to test the routine examination process.

10.6.3-2 The assessment process to be followed for a random examination is the same as that for the routine examination process (see para. 10.5.1).

10.6.3-3 In the case of a random examination, a notice will be sent to the insurance company at least two weeks prior to the examination. This notice will be forwarded to the MLRO or the Senior Management of the insurance company.

10.6.4 ***Special Examination***

10.6.4-1 The Commission will conduct an on-site examination of an insurance company in "special" circumstances, based on cause, to determine whether there has been any infraction of the AML laws and the extent of the violation. Such an examination will usually take place where an insurance company has violated any provision of the AML/CFT laws, or where information comes to the attention of the Commission that a statutorily prescribed financial institution is providing financial services despite having advised the Commission to the contrary.

10.6.4-2 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.

11 EXAMINATIONS FOR INSURANCE COMPANIES UNDER SECTION 207 OF THE INSURANCE ACT, Chapter 347

11.1 The examination form is designed to examine whether insurance companies are adhering to the AML/CFT laws and obligations. The examination form addresses the assessment of risks, customer verification procedures and records and covers suspicious transactions

reporting, staff training and politically exposed persons.

11.2 On completion of an examination, the form should then be forwarded to the Commission.

12. INDUSTRY ENGAGEMENT AND TRAINING PROGRAMMES FOR INSURANCE COMPANIES

12.1 The Commission will conduct annual training programmes for insurance companies. In addition, officers of the Commission are available for specific training programmes for individual companies upon request.

12.2 As a tool of supervision, the Commission will engage with the industry on an annual basis to collaborate and to discuss any AML/CFT/CPF concerns. The Commission will determine whether companies are conducting AML/CFT/CPF training of employees annually.

C. INTERNAL AML/CFT/CPF PROCEDURES

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

For life insurance companies:

- Parts II of the FTRA and the FTRR that deal respectively with customer verification/identification (sections 6-8, 11-13), record-keeping (section 15-18) suspicious transactions and reporting (sections 25-30)

- Regulation 5 of the FI(TR)R which call for the implementation of internal procedures for identification, education and training (sections 19-21 and 46-57).

Pursuant to section 5 of the FTRA, licensees are required to develop and implement a comprehensive risk management system for addressing AML vulnerabilities posed to the entire company. They must take appropriate measures to identify, assess and understand its risks. The process involves documenting and putting procedures in place for identifying money laundering, terrorist and proliferation financing risks facing the licensee, given its clientele, products, transactions and delivery channels. Licensees must also give regard to the risks that have been identified in the country's national risk assessment. In this regard, licensees should take into consideration the risks of the country that have been identified by the Identified Risk Framework Steering Committee. Licensees should have regard to all available information, including published money laundering typologies or terrorist lists, to assist with identifying potential risks.

Insurance companies are required to:

a) Assess and identify the risks prior to the launch or use of new or developing products and business practices, including new delivery mechanisms when dealing with new or developing technologies for both new and pre-existing products; and

b) Take appropriate measures to manage and mitigate those risks.

In order for licensees to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the licensee. The success of internal policies and procedures will be dependent largely on internal control systems. Two key systems that will assist in achieving this objective are discussed below.

Culture of compliance

This should encompass:

- developing, delivering, and maintaining a training programme;
- monitoring for any government regulatory changes; and
- undertaking a regularly scheduled review of applicable compliance policies and procedures within International Financial Reporting Standards, which will help constitute a culture of compliance in the industry.

Senior management ownership and support

Strong senior management leadership and engagement in AML/CFT/CPF is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the firm's policies, procedures and processes designed to limit and control risks. Policies and procedures are effective only at the point that firm/company owners and senior management support the policies.

V. INTERNAL CONTROLS AND PROCEDURES OF AML/CFT/CPF SYSTEMS

13. INTERNAL CONTROLS FOR INSURANCE COMPANIES

13.1 Having regard to its ML/TF risks and the size of the business, insurance companies are required to implement internal control and procedures to mitigate risks of money laundering and terrorist financing.

Internal policies, procedures and controls should include:

(a) a compliance management programme (includes the appointment of a compliance officer and money laundering officer at the management level);

(b) screening procedures to ensure high standards when hiring employees;

(c) an ongoing employee training programme; and

(d) an independent audit function to test the system.

13.2 Insurance companies that are a part of a group of companies are required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group.

In addition to those listed above in 13.1, measures implemented by group wide programmes should also include:

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

(b) the provision, at group-level compliance, an audit of AML/CFT functions, customer, account, and transaction information from branches and subsidiaries when necessary, for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done)[3]. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management[4]; and

(c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping off.

13.3 INTERNAL CONTROLS AND PROCEDURES FOR FOREIGN BRANCHES AND SUBSIDIARIES

Since standards of control vary between different countries, careful attention should be paid to the place of origin of the verification documents and the background against which they are produced. Where appropriate certified translations of these documents should be obtained in English.

Where overseas branches or subsidiaries do not have appropriate CDD measures in place, they are required to apply appropriate additional measures to manage

[3] This could include an STR, its underlying information, or the fact that an STR has been submitted.

[4] The scope and extent of the information to be shared may be determined taking into consideration the sensitivity of the information, and its relevance to the company's AML/CFT risk management programme.

the ML/TF risks and inform their home supervisor/regulator.

Where the minimum AML/CFT requirements of The Bahamas are less strict than those of the home country, insurance companies are required to ensure that the overseas branch/subsidiary implements the requirements of the home country, to the extent that the laws of The Bahamas permits.

13.4 INTERNAL TESTING OF COMPLIANCE LEVELS

Licensees are required to perform periodic internal reviews, the results of which should be accessible for review both by examining independent accountants and the Commission's examiners.

In addition to the examination programmes, periodic testing and auditing of the AML/CFT policies, procedures and controls should be undertaken. This can be a useful tool in apprising the Commission of any changes which may have occurred between examinations. Such changes may include number of facilities, staff movements, and verification of compliance with policies, procedures and controls to counter money laundering, terrorist financing and proliferation financing activities in relation to all of their financial intermediary services. Larger licensees may wish to assign this role to their Internal Audit or Compliance Department. Smaller licensees may accomplish the same objective by introducing a regular review by their management personnel.

VI. CUSTOMER DUE DILIGENCE/KNOW YOUR CUSTOMER (CDD/KYC)[5] PROCEDURES

14. GUIDANCE ON IDENTIFICATION/VERIFICATION PROCEDURES

14.1 The objective of KYC, which is also referred to as customer due diligence, is to ensure that financial institutions ascertain the true identity of each customer. In this regard, insurance companies or intermediaries must ascertain the true identity of each customer, beneficial owner and beneficiary of the policy and assess with an appropriate degree of confidence the types of business and transactions the customer is likely to undertake.

Licensees are also required to incorporate into their AML risk management framework, a risk-based KYC process in conformity with the guidance set out in this Part C.

14.2 CDD for Life Insurance Companies

Life insurance companies must obtain sufficient information concerning the beneficiary at the beginning so that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights. For a beneficiary that is designated by characteristics or by class or by other means – the company must obtain sufficient information concerning the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary at the time of the payout.

Verification procedures of the identity of the beneficiary(ies) should be followed as soon as the beneficiary is identified or designated, and at the time of payout.

[5] "KYC" is the shortened form for "know your customer" or "know your client". This is the same concept used in the banking sector and may be described as "customer/client due diligence" or its diminutive form "CDD".

14.3 POLITICALLY EXPOSED PERSONS

Politically Exposed Persons (PEPs) are defined as "individuals who hold or have held a domestic prominent public function or a prominent public function in a foreign jurisdiction". If the PEP or close associate is no longer a PEP at the time of Licensees should determine according to the risk profile of the PEP and the licensee's risk assessment.

The risk-based approach requires insurance companies to assess the ML/TF/PF risk of a PEP who is no longer entrusted with a prominent public function and take effective action to mitigate this risk. The following should be taken into consideration:

1) Whether the individual could still exercise the same level of influence;
2) Seniority of the position once held as a PEP; or
3) Whether the individual's previous and current function are connected or linked in any way

Licensees are required to perform customer due diligence measures when engaging in business relationships with PEPs and with related parties, including immediate family members, close associates or related companies. Such relationships may expose Licensees to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. In addition, a PEP includes any corporation, business or other entity that has been formed by, or for the benefit of a senior official.

14.3.1 **Foreign PEPs** are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

14.3.2 **Domestic PEPs** are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

14.3.3 International organization PEPs are persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

14.3.4 Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

14.3.5 A close associate is an individual who is closely connected to a PEP, either socially or professionally. This includes any individual who is widely and publicly known to maintain a close relationship with a PEP and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of a PEP.

14.3.6 In relation to life insurance policies and other investment related insurance policies, insurance companies are required to take reasonable measures to determine whether the beneficiaries and/or, where required the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should inform senior management before the payout of policy proceeds, to conduct enhanced measures on the whole business relationship with the policyholder, and to consider a suspicious transaction report. They should also conduct enhanced monitoring on that relationship.

14.3.7 **CDD Measures for Foreign PEPs**

In addition to performing CDD measures outlined in paragraph 14, licensees are required to:

(a) Put risk management systems in place to determine whether a customer or beneficial owner is a PEP;

(b) Obtain senior management approval when establishing business relationships or when conducting business with continuing or existing customers;

(c) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) Conduct enhanced monitoring.

14.3.8 **CDD Measures for Domestics PEPs**

PEPs or persons who have been entrusted with a prominent function by an international organization. In addition to performing the CDD measures already mentioned, licensees are required to:

(a) Take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) Adopt the measures in 14.3.6 (a) – (d), where it is determined that there is a higher risk in the business relationship.

14.4 Risk Identification

14.4.1 Licensees should ensure that they are satisfied about the following details for all their clients, in order to be able to make a determination about the AML risk each poses:

- who the client is? Is there public information that associates this person with any known money laundering or terrorist financing activities?
- what is his business? Is this client's occupation or business activities commonly linked to money laundering or terrorist financing activities?
- where is he located? Does the client's jurisdiction apply globally acceptable AML standards?
- where does he transact business? Does the jurisdiction where this client transacts business apply adequate AML standards or is it commonly linked to money laundering or terrorist financing activities?
- what products and services does he require? Do the products and services provided to the client offer the anonymity and movement of funds commonly linked to money laundering and terrorist financing activities?

14.4.2 A similar assessment of the risks inherent in products and services offered should be carried out.

14.4.3 It is recommended that clients, products and services should be categorized based on the degree of money laundering and terrorist financing risk they pose to the licensee.

14.5 Categorization and mitigation of Risk

14.5.1 The Commission requires Licensees conduct a risk assessment and should place clients and products/services into one of three risk categories, i.e. Low, Medium or High Risk.

14.5.2 Licensees 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.

14.5.3 Risk Characteristics

14.5.3-1 Determining the potential money laundering and terrorist financing risks posed by a customer or category of customers is critical to the development of an overall risk framework. In determining the risk profile of any customer, licensees should consider the following factors (which are not to be considered an exhaustive list):

(i) Significant and unexplained geographic distance between residence or business location of the customer and the location of the insurer's representative.

(ii) Frequent and unexplained movement of funds between financial institutions in various geographic locations.

(iii) Customers that are legal persons whose structure makes it difficult to identify the ultimate beneficial owner or controlling interests.

(iv) Customers who seek or accept very unfavourable account/policy/contract provisions or riders.

(v) Charities and other "not for profit" organizations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis).

(vi) "Gatekeepers" such as accountants, lawyers, or other professionals holding accounts/policies/contracts at an insurance company, acting on behalf of their clients, and where the insurance company places unreasonable reliance on the gatekeeper.

(vii) Customers who are Politically Exposed Persons (PEPs) and close associates of PEPs.

(viii) Customers where the beneficial owner of the contract is not known (i.e. certain trusts).

(ix) Customers who are introduced through non-face to face channels.

(x) Customers who use unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual), or structured monetary instruments.

(xi) Customers who seek early termination of a product, especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third party.

(xii) Customers who transfer the benefit of a product to an apparently unrelated third party.

(xiii) Customers who show little concern for the investment performance of a product, but a great deal of concern about the early termination features of the product.

(xiv) Customers who are reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information.

14.5.3-2 Similar issues, criteria or circumstances may be relevant to the ML/TF risk associated with each beneficiary of the life insurance contract.

14.5.3-3 The KYC procedures that are implemented to mitigate the risk of money laundering and terrorist financing for low risk clients/customers should do the following in accordance with the guidance set out in section 14 –

- identify the policyholder;
- verify the policyholder's identity;
- identify the person with beneficial ownership and control (if different from the policyholder's);
- verify the identity of the beneficial owners

15. VERIFICATION DETAILS AND DOCUMENTARY EVIDENCE PROCEDURES

General Duty to Verify Identity

15.1.1 A life insurance company should 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 customer should be interviewed personally.

15.1.2 Subject to the exemptions and exceptions set out in section 15 below, life insurance companies have a mandatory obligation to verify identity in the following circumstances:

(1) *Existing Facility holders*
All existing facility holders of record who are above the established threshold must verify the identity of their clients. Where doubt arises in relation to any facility holder during the business relationship, a verification of the facility holder must be undertaken.

(2) *New Facility holders*

- Before establishing a new facility, all persons authorized to operate the facility must be verified.

- Before adding someone as a facility holder to an existing facility, that person must be verified.

(3) *Persons who seek to conduct a transaction with the life insurance company via existing facilities involving cash in excess of $15,000 (an occasional transaction) and the transactor is not a client in relation to any financial intermediary services provided by the insurance company or is conducting the transaction on behalf of someone who is not.*

- Where a person, who cannot be regarded as a client holder, seeks to conduct an occasional transaction in relation to any facility, that person must be verified before such transaction is permitted.

- Where a person, who is also not a client in relation to the subject facility seeks to conduct **an occasional transaction (cash) on behalf of another** who is also not a facility holder of the firm. In addition to the transactor being verified the person on whose behalf he is acting must also be verified.

- Where a client facility holder seeks to use his own facility, which is provided by the life insurance company to conduct occasional transactions on behalf of others, (this is most commonly the case for intermediaries such as attorneys), those others must be verified.

- Where structuring of an occasional transaction is suspected to be taking place. (See Fig. 2 on page 31 for an explanation of a structuring).

15.2 Obligations Where Unable to Complete CDD

Where the insurance company is unable to complete the CDD/KYC verification procedures, it must not commence a business relationship or perform the transaction; or must suspend or terminate the business relationship until sufficient information can be obtained. The company should consider making a suspicious transaction report (STR) in relation to the customer.

15.3 Tipping Off

Where an insurance company forms a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into consideration the risk of tipping off. If when performing the CDD process, they reasonably believe that the customer may be tipped off during the process, they may elect not to pursue the CDD process; but should file an STR. Insurance companies should ensure that their employees are sensitized and made aware of these issues when conducting CDD or ongoing CDD.

Figure 2: 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 an insurance company detects that two or more cash transactions by or on behalf of someone who is not the insurance company's facility holder, have authorized 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 insurance company forms that conclusion. The insurance company 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 insurance company's financial intermediary services, which generates the obligation to verify identity.

This requirement exists whether 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 insurance company 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 transactions are or have been structured to avoid the verification procedure, the insurance company 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.

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

15.5 Regulations 3, 4 and 5 of the FTRR provide 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 companies' enhanced due diligence procedures for high risk clients. (see guidance on Enhanced Due Diligence on page 41)

15.6 Verification information and documents for individuals

15.6.1 Subject to the provisions for exemptions and exceptions set out below in section 16, the following evidence must be on record for every facility or occasional transaction that must be verified.

15.6.2 Mandatory requirements to verify an individual*:*

Full and correct name, permanent address, date and place of birth, purpose of the facility, potential activity involving the facility and written confirmation that all credits to the facility are and will be beneficially owned by the facility holder, except in the case of a facility that will be an intermediary facility as verification of beneficial ownership will have to be completed separately.

15.7 Additional means of identification for non-resident clients

A useful means of identification for non-residents is a social security, social insurance or national insurance number. Licensees are encouraged to record such information as part of the client profile.

15.8 Verification information and documents for corporate bodies (legal persons and legal arrangements)

15.8.1 *Mandatory requirements for verifying corporate entities including those that are* Non-Profit Organizations (*NPOs), whether incorporated in The Bahamas or elsewhere*: -

a. certified copy of the Certificate of Incorporation;
b. certified copy of the Memorandum and Articles of Association;
c. list of the Board of Directors;
d. resolution of the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account;
e. names of relevant persons holding a senior management position;
f. location of the registered office or agent and, the principal place of business
g. documentary evidence in accordance with paragraph 15.2 in respect of the individual identified in sub-paragraph (b) above;
h. confirmation that the corporate entity has not been struck off the register or in; the process of being wound up;
i. written confirmation that all credits to the facility are and will be owned by the client corporate entity except in the case of a facility that will be an intermediary facility in which case the beneficial ownership identification information will have to be provided separately;
j. names and addresses of all beneficial owners (the obligation to verify the identity of beneficial owners shall only extend to those with at least 10% controlling interest in the corporate entity); and
k. purpose and intended nature of the business relationship; products and/or services provided.

All information referred to in (c), (d), (e), (f) and (j) should be accurate and updated on a timely basis.

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

list of shareholders; the potential parameters of the facility including size, in the case of investment and custody accounts, balance ranges, in the case of deposit accounts and the expected transaction volume of the account; and such other official document and other information as is reasonably capable of establishing the ownership and control structure of the corporate entity.

15.8.3 References to “account” in relation to verification evidence in the case of a life insurance company should be construed to mean the facility or financial intermediary service that is being provided to the client facility.

15.8.4 The insurance company must also take reasonable measures to determine the natural persons who control the management of the corporate entity and its ownership structure. Natural person must be able to cooperate with competent authorities, providing basic information and available beneficial ownership information.

15.9 General guidance on the process for verifying corporate entities.

15.9.1 As a rule of thumb, the insurance company should verify the legal existence of the applicant company and ensure that any person purporting to act on behalf of the company is fully authorized. One of the principal requirements is to look behind the corporate entity and obtain the names and addresses of beneficial owners, except in those cases where reduced or simplified due diligence might apply. Enquiries should also be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a "shell company" where the controlling principals cannot be identified.

15.9.2 Before a facility is established, a company search or other commercial enquiries should be carried out to ensure that the applicant company has not been, or is not in the process of being dissolved, struck off, wound-up or terminated.

15.9.3 If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments on behalf of a company, further checks should be made to ascertain the reason for the changes.

15.9.4 In appropriate cases for established businesses, a copy of the latest report and accounts (audited where applicable) should be obtained.

15.9.5 A search of the file at the local Companies Registry or the firm's registered office is advisable, similarly an enquiry may be made via a business information service or an undertaking obtained from a firm of lawyers confirming that the constituent documents have been submitted to the Registrar of Companies.

15.9.6 When signatories to the facility change, care should be taken to ensure that the relevant authorized on from the company as well as the full name and addresses of the new signatories along with other supporting information as required above are obtained for the file. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes to directors/shareholders or to the original nature of the business/activity. Such changes could be significant in relation to potential money laundering activity even though authorized signatories have not changed.

15.10 Verification information and documentation for partnerships and other unincorporated associations/businesses

15.10.1 Mandatory requirements for verifying the identity of partnerships or other unincorporated businesses, including any NPOs formed by these means, the following information/documents shall be required:

a) verification of all partners or beneficial owners in accordance with para. 15;

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

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

d) documentary evidence in accordance with para. 15.6 in respect of the individual identified in paragraph I above;

e) written confirmation that all credits to the facility are and will be beneficially owned by the facility holder except in the case of a facility that will be an intermediary facility as verification of the beneficial ownership will have to be completed separately; and

f) purpose and intended nature of the business relationship.

15.10.2 General guidance on the process for verifying partnerships, clubs, societies and charities and other entities which are not incorporated

15.10.2-1 Each partner or beneficial owner of the business, as the case may be, must be verified as an individual in accordance with section 15.6.2 above.

15.10.2-2 In the case of facilities to be opened for partnerships, clubs, societies and charities and other entities which are not incorporated, an insurance company should satisfy itself as to the legitimate purpose of the entity by requesting sight of the constitution or by-laws, partnership agreement etc. and a copy thereof placed on the file. The names and addresses of all signatories to the facility should be verified initially, as well as a written mandate from the facility holders for the signatories to act on their behalf. In addition, when signatories change, care should be taken to ensure that this information is obtained before any new signatory is permitted to conduct business on behalf of the facility holder.

15.11 Verification of facilities/accounts for intermediaries[6] (nominees, fiduciaries, trustees etc.).

15.11.1 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 paragraph 15. 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 paragraph 15.6.

15.12 Additional guidance on verification requirements in the case of trusts

15.12.1 **N.B.: Occupational Pension Schemes which do not allow public participation, and which are registered locally under the Superannuation and Other Trusts Funds (Validation Scheme) Act[7], are exempted from the verification requirements under the FTRA.**

15.12.2 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 beneficial and other such information.

15.12.3 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.

[6] Regulation 8, FTRR

[7] Chapter 178, 2009 - Bahamas Statute Laws

15.12.4 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.

15.12.5 Where a person who makes a request to become a facility holder or to undertake a transaction does so as a professional adviser, business or company acting as trustee or nominee in relation to a third party, the insurance company must verify the identity of the trustee, nominee or fiduciary and the nature of their trustee or nominee capacity or duties. Enquiries should be made as to the identity of all parties for whom the trustee or nominee is acting including the settlor and any beneficiaries (except where an occasional transaction is being conducted on the beneficiary's behalf) and confirmation sought that the source of funds or assets under the trustee's control are from a legitimate source. In addition to verifying the trustee in accordance with this section, the settlor and any contributor to the trust should also be verified in accordance with this section

Where a person is appointed as a protector of the trust, the insurance company must verify the identity of such person.

15.12.6 Measures to obtain the information concerning the underlying beneficiary will need to take account of legal constraints and/or good market practice in the respective area of activity, the geographical location of the trustees and beneficiaries to which the trust facility relates and, in particular, whether it is normal practice in those areas or markets to operate on behalf of undisclosed principals. Trusts created in poorly regulated jurisdictions may warrant additional enquiries.

15.12.7 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 authorized in writing.

15.13 Verification When Providing Safe Custody and Safety Deposit Boxes

15.13.1 Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such arrangements are made available to non-clients, the identification procedures set out in These Guidelines should be followed.

15.14 Guidance on confirming the identity of a client

15.14.1 Although the primary duty to verify identity using the best evidence and means available rests with the insurance company; in exceptional circumstances an insurance company may wish to approach an eligible introducer, specifically for the purpose of satisfying itself on a verification of identity that it must complete. In these exceptional circumstances, the standard format set out in *Appendix E* should be used for making the enquiry.

15.15 Guidance on verifying address

15.15.1 In addition to the name verification, it is important that the current permanent address should also be verified. Any current documentation or identification issued by a valid government or public authority may be relied upon to establish this. It is sufficient for the officer or employee conducting the verification to certify that he has seen and is satisfied with the evidence relied upon to verify the address. It is not necessary to keep copies of documentation that establishes the permanent address, just for that purpose.

16 RELIANCE ON THIRD PARTIES TO CONDUCT CDD/KYC ON CUSTOMERS

Exemptions from the obligations to obtain full verification documentation

16.1 **Outright exemptions**

16.2 A life insurance company is exempted from having to obtain full documentary evidence (in accordance with regulations 4-7[8]) for customer verification on the following facility holders. Files should contain adequate documentation and relevant copies as evidence in satisfaction of any claim for exemption, in addition to documentation attested to by the client regarding the purpose, use, parameters, potential activity, scope and source of funds with respect to the facility:

16.3 The exemption applies to:

- Central or local government agency, statutory body. The file should contain evidence from a sufficiently senior authority in Government or the relevant statutory body authorizing the establishment and operation of the facility.
- Occupational Pension Schemes registered under the Superannuation and other Trusts (Validation Scheme) Act which do not allow public participation.
- Licensed Bahamian bank regulated by the Central Bank of The Bahamas
- Licensed Bahamian Trust Company regulated by the Central Bank of The Bahamas
- Licensed financial institution of the Gaming Board
- Licensed insurance company regulated by the Insurance Commission or its equivalent Regulator and subject to anti-money laundering and countering the financing of terrorism obligations
- Any broker-dealer or mutual fund administrator or operator regulated (including a regulated mutual fund) by the Securities Commission or its equivalent Regulator and subject to anti-money laundering and countering financing of terrorism obligations
- Any entity regulated by the Compliance Commission or its equivalent Regulator and subject to anti-money laundering and countering financing of terrorism obligations
- A publicly traded company listed on The Bahamas International Stock Exchange of any other Stock Exchange specified in the FTRR Schedule and approved by the Securities Commission of The Bahamas
- A beneficiary under a discretionary trust where a Trustee seeks, on behalf of such beneficiary, to conduct a cash transaction over $15,000 (occasional transaction) with the firm in relation to any financial intermediary services provided by the firm, and the firm is reasonably satisfied that, within this context the Trustee is acting for a beneficiary or beneficiaries under a discretionary trust.

16.4 If the insurance company is relying on a third party, then it must ensure that it can get all identification information and CDD information from the third party without delay. The company must also satisfy itself that the third party is subject to AML/CFT obligations and that they are supervised for compliance for these obligations.

[8] FTRR 2018

16.4.1 To satisfy the record-keeping obligations where an exemption is claimed, the file should include in appropriate cases, a copy of the relevant certificate or license or such similar document that supports the exempt status. The ultimate responsibility for CDD measures should remain with the insurance company relying on the third party.

16.5 Regulated Financial Institutions

16.5.1 For regulated financial institutions, it is recommended that the confirmation of its 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 or authorization to conduct the financial intermediary service business with the firm.

16.6 Verification evidence obtained on an earlier occasion that continues to be reasonably capable of establishing the identity of the verification subject

16.6.1 An insurance company can rely on verification evidence obtained on an earlier occasion where it has reasonable grounds to believe that such evidence is still reasonably capable of establishing the identity of a person, in accordance with the requirements set out in section 15.

16.7 Closing and opening a facility with the same institution (transfer of records)

16.7.1 If an existing facility holder closes one facility and establishes another with the same life insurance company, there is no need to verify identity afresh, but existing records should be transferred to the new facility. However, the opportunity should be taken to confirm the relevant customer verification information. This is particularly important if there has been no recent contact or correspondence with the customer or when a previously dormant facility has been reactivated.

16.7.2 Where the primary obligation to verify is satisfied by a verification conducted by an eligible introducer financial institution (Reliable Introductions).

16.7.3 An eligible introducer is any one of the following:

- Licensed Bahamian bank or one that is subject to anti-money laundering and countering the financing of terrorism obligations
- Licensed Bahamian trust company or one that is subject to anti-money laundering and countering the financing of terrorism obligations
- Licensed Bahamian casino or one that is subject to anti-money laundering and countering the financing of terrorism obligations
- Any broker-dealer or mutual fund administrator and operator regulated by the Securities Commission of The Bahamas or its equivalent from a country
- Any designated non-financial business and profession regulated by the Compliance Commission of the Bahamas or its equivalent

16.8 Permissible eligible introductions where a facility is being established

16.8.1 In the case of facilities, eligible introductions are permitted in the following circumstances –

a. Establishment of facilities by telephone, Internet or post.

An insurance company can establish a facility by means of telephone, Internet or post where a letter of introduction stipulating that the eligible introducer has verified the prospective client is provided. If the client has been introduced by this means, an original letter on file should reflect this fact.

b. ***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 an insurance company to receive periodic deposits on its behalf from an account that it (the client) has at an eligible introducer bank, the insurance company 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

c. Corporate Group Introductions

Reliance may be placed on the verification carried out by another insurance company of a group that is a subsidiary or parent of which the insurance company is a member and which is subject to an AML group policy, that is strictly adhered to, and which is at least consistent with the standards provided by Bahamian law, for the purpose of introducing a prospective client wishing to establish a facility in The Bahamas.

16.8.2-1 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 insurance company is obliged to ascertain 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 insurance company should also obtain copies of all verification information obtained by the parent or subsidiary for inclusion in its own files:

- 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; and

- 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 Bahamian AML laws. The letter from the eligible introducer must also provide an undertaking to supply to the insurance company upon request, immediately and without delay, copies of such evidence and documentation.

16.8.2-2 Permissible eligible introductions where an occasional transaction (i.e. sums i*n* excess of the $15,000 threshold) is being attempted/conducted.

16.8.2-2 (a) An occasional transaction is one in which the sum involved exceeds $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 insurance company.

16.8.2-2 (b) Letters of Confirmation may be used to satisfy the primary obligation on an insurance company to verify identity, when a sum in excess of $15,000 is involved in a transaction being conducted by or on behalf of a non-facility holder.

16.8.2-2 (c) Only eligible introducers can issue Letters of Confirmation, i.e. those entities outlined in section 15.9 above.

16.8.2-3 (d) The circumstances involving an occasional transaction in which reliance may be placed on a letter of confirmation issued by another eligible introducer financial institution certifying that it (the eligible introducer financial institution) has carried out the required verification are as follows:

(1) Where a deposit is made into a facility that is provided for the insurance company by an eligible introducer financial institution and the insurance company is unable to determine if such a deposit involved an occasional transaction. An example of this is where a facility holder client makes a deposit directly into a bank account of the insurance company, then the insurance company 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 cash transaction of $15,000 or more on behalf of another person with the insurance company that it (the bank) has carried out the required verification on the party on whose behalf it is acting; and

(3) An insurance company 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 an occasional transaction with the insurance company 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.[9]

17. MONITORING OF FACILITIES

17.1 ONGOING DUE DILIGENCE

Insurance companies are required to conduct ongoing due diligence on business relationships. Once the identification procedures have been completed and the client relationship is established, licensees should monitor the conduct of the relationship to ensure that it is consistent with the reason why the relationship was established when the policy contract was executed.

Insurance companies are expected to maintain systems and put controls in place to monitor the relevant activities in the course of the business relationship to ensure consistency with stated facility purposes and activities. The nature and sophistication of this monitoring will depend on the nature of the business. The purpose of this monitoring is for insurance companies 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

[9] Section 9, FTRR

measured against the stated original purpose of the facility.

Areas to monitor could be:

(a) transaction type
(b) frequency
(c) amount
(d) geographical origin/destination
(e) facility signatories

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

17.1.2 Insurance companies should, to the extent possible, examine the circumstances of complex and unusual, large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and document their findings and maintain such information for a minimum period of five years.

17.1.3 Having regard to the size, volume of financial services business and complexity of such business, insurance companies should ensure that documents, data or information collected during the due diligence process is kept up-to-date and relevant, through periodic reviews of existing records, particularly for high risk categories of customers. The process by which records are kept current should be documented as part of the record-keeping policies.

17.2 SIMPLIFIED DUE DILIGENCE

Insurance companies should apply simplified due diligence measures where they have determined according to their risk assessment of the business relationship that the risk is low and that they should obtain sufficient information on the facility holder. They do not have to collect the amount of identification information as in the case of regular CDD, on the purpose or intended nature of the business relationship of a customer, or the beneficial owner of a customer where the customer is considered to present a low risk of money laundering or terrorist financing. In addition, licensees should take into consideration the risks identified in the country risk assessment.

17.3 ENHANCED DUE DILIGENCE

Insurance companies are required to do the following:

(a) Apply enhanced due diligence measures to a business relationship or transaction with a facility holder, beneficial owner or financial institution from a jurisdiction assessed by the IRF Steering Committee or the Financial Institution. The enhanced measures should be effective and proportionate to the risks identified.

(b) Examine as far as possible the background and purpose of all complex, unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

(c) Take measures, as necessary, to counter the risks identified with respect to facility holders, beneficial owners or financial institutions assessed as high risk.

Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to Licensees. Conducting business relationships with customers who are either citizens of or domiciled in such countries

exposes the Licensee to reputational risk and legal risk. Licensees are encouraged to consult publicly available information to ensure that they are aware of countries which may pose a higher risk.

Licensees should refer to the following websites: FATF – www.fatf-gafi.org; Financial Crimes Enforcement Network (FinCEN) – www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov.ofac for information pertaining to US foreign police and national security; and Transparency International – www.transparency.org for information on countries vulnerable to corruption.

VII. RECORD KEEPING PROCEDURES

18. STATUTORY REQUIREMENTS TO MAINTAIN RECORDS

18.1 Insurance companies are required to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering or terrorist financing. 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 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, in so far as is practicable, that in any subsequent investigation, the insurance company can provide the authorities with its part of the audit trail.

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

18.3 The records prepared and maintained by any insurance company 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 money laundering 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 as to disclosure of relevant information.

18.4 Format of records

18.4.1 Retention of verification and transaction records may be by way of original documents, stored on microfiche, computer disk or in other electronic form.

18.5 Identification/verification (KYC) records

18.5.1 Section 14 sets out the evidence to be obtained for verification of identity.

18.5.2 For the purpose of verifying the identity of any person an insurance company must keep such records as are reasonably capable of enabling the FIU to readily identify the nature of the evidence used for the verification.

18.5.3 **Verification records for eligible introductions involving the confirmation of the existence of a facility**

18.5.3-1 Where an insurance company 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 retained are such that 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.

18.5.4 Retention period for verification records

18.5.4-1 In relation to any other person, records relating to the verification of the identity of any person must be kept for a period of not less than 5 years after the verification was carried out.

18.5.4-2 Records relating to the verification of the identity of facility holders must be retained for 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.

18.5.4-3 Where formalities to end a business relationship have not been undertaken, but a period of 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.

18.5.4-4 Records relating to the verification of the identity for any transaction conducted through a facility of an intermediary must be kept for a period of not less than 5 years after the intermediary ceases to be a facility holder.

18.5.4-5 Where records relate to on-going investigations, they must be retained until it is confirmed by the FIU or local law enforcement agency that the case has been closed.

18.6 Transaction records

18.6.1 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 terrorism. 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.

18.6.2 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 provided by the insurance company) directly involved in the transaction; and
- all other files and business correspondence and records connected to the facility.

18.6.3 ONGOING INVESTIGATIONS

18.6.3-1 Transaction records to be kept for a minimum period of five (5) years

Transaction records both domestic and international must be kept for a minimum period of five years after the transaction has been completed, subject to the extended

requirements where the records relate to an ongoing investigation then they must be retained until it is confirmed by the FIU or local law enforcement agency that the case has been closed.

18.6.4 Records of suspicion which were raised internally with the MLRO but not disclosed to the authorities should be retained for at least five years from the date of the transaction. Records of suspicions which the authorities have advised are of no interest should be retained for a similar period.

18.6.5 Similarly, records of the insurance company's findings regarding their enquiries into unusual activity, should be retained for a minimum of five years following the termination of the business relationship or after the date of the occasional transaction. Licensees should also retain any analysis conducted or taken of an account.

18.7 Financial Institutions to Maintain Records

18.7.1 **Special considerations for record retention on the liquidation of a financial institution**

18.7.1-1 When a financial institution enters a liquidation, the liquidator of the financial institution is required to maintain for a period of five years from the date of dissolution such information and records, including beneficial ownership information, that would otherwise have been required to be kept by the financial institution but for the liquidation.

18.8 Destruction of Records

18.8.1 The records and any copies thereof, maintained pursuant to section 17 of the FTRA must be destroyed as soon as practicable after the expiration of the retention period, unless required to be maintained beyond this period by any law, for the business purposes of the insurance company, or for investigative purposes by law enforcement or the FIU.

18.9 Failure to Keep Information and Records

It is an offence for insurance companies not to retain or properly keep information and records, including beneficial ownership information, without reasonable excuse.

19 ELECTRONIC PAYMENT TRANSFERS

19.1 The Financial Action Task Force (FATF) issued Recommendation 16 with the objective of enhancing the transparency of cross-border and domestic electronic payment transfers ("wire transfers" or "transfers") thereby making it easier for law enforcement to trace funds transferred electronically by terrorists and other criminals. Recommendation 16 has been implemented in The Bahamas through the Financial Transactions (Wire Transfers) Regulations, 2018 ("the Wire Transfers Regulations").

19.2 The Wire Transfers Regulations are intended to cover any transaction carried out on behalf of a payer through a financial institution by electronic means with a view to making funds available to a payee at a beneficiary financial institution, whether or not the payer and the payee are the same person. Generally, the Wire Transfers Regulations require financial institutions that participate in the execution of wire transfers to obtain, record and retain specified information on payers of wire transfers and to ensure that all transfers through the payment chain are accompanied by information on the payers who give the instructions for payment to be made.

19.3 Licensees that initiate wire transfers on behalf of payers ("originating financial institutions") must ensure that the payer information conveyed in the payment message or instruction is accurate and has been verified.

19.4 The verification requirement is deemed to be met for account holding customers of the originating financial institution once the customer's identity has been verified and the verification documentation has been retained in accordance with the FTRA, 2018 and the FTRR, 2018. In such cases, the originating financial institution may assign to the wire transfer a unique identifier that would like the account holding customer and his relevant identification information to the wire transfer.

19.5 Before initiating one-off wire transfers on the instructions of non-account holding customers, originating financial institutions must verify the identity and address (or a permitted alternative to address) of the payer.

Cross-border Wire Transfers – Complete Payer Information

19.6 Complete payer information must accompany all wire transfers of $1,000 or more where the beneficiary financial institution (i.e. the financial institution which receives a funds transfer on behalf of a payee) is located in a jurisdiction outside of The Bahamas. Complete payer information consists of the payer's:

(a) name;

(b) account number, if no account exists, a unique identifier or transaction number; and

(c) address, or date and place of birth, or national identity number, or customer identification number.

Domestic Wire Transfer – Reduce Payer Information

19.7 Where the originating and beneficiary financial institutions are both located within The Bahamas, wire transfers need be accompanied only by the payer's account number or a unique identifier or a transaction number which permits the transaction to be traced back to the payer. However, if requested by the beneficiary financial institution, complete payer information must be provided by the ordering financial institution within three business days of such request.

Wire Transfers via Intermediaries

19.8 Intermediary financial institutions are Licensees, other than originating or beneficiary financial institutions that participate in the execution of funds transfers. Intermediary financial institutions must ensure that all information received on the payer which accompanies a wire transfer is retained with the transfer throughout the payment chain.

Record Keeping Requirements

19.9 The particulars of the wire transfer to be recorded must be of sufficient detail so as to enable the transfer to be accurately described. All originator and beneficiary information collected in relation to the transaction, must be retained by the ordering financial institution for a period of five years from execution of the transfer.

19.10 The originating financial institution should not be allowed to execute the wire transfer if it does not comply with the payer information requirements in 19.6.

VIII. PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

20 THE FINANCIAL INTELLIGENCE UNIT (FIU)

20.1 The national agency for receiving suspicious transaction reports (STRs) is the Financial Intelligence Unit, Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas, Telephone # (242) 356-9808 or (242) 356-6327, Fax No. (242) 322-5551, website: www.bahamas.gov.bs/fiu.

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

20.3 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.

20.4 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 Guidelines, are available from the FIU's office and electronically from the FIU's website.

20.5 Mandatory requirement to appoint a Money Laundering Reporting Officer

20.5.1 All life insurance companies engaged in financial intermediary services are required by law[10] to appoint a Money Laundering Reporting Officer (MLRO) as the point of contact with the FIU, in order to handle reports of money laundering suspicions by their staff.

20.5.2 The Commission must grant approval for an individual to perform *the MLRO function*, only if the candidate satisfies fit and proper criteria.[11] The Commission will issue a letter to the insurance company indicating its decision and submit a copy of the letter to the FIU and any other joint Regulator, if applicable.

20.5.2-1 The MLRO must be registered with the FIU. Life insurance companies should ensure that any changes in this post are immediately notified to the FIU and the Commission.

20.5.3 The Role of the MLRO

20.5.3-1 The type of person appointed as MLRO will depend on the size of the insurance company and the nature of its business, but he/she should have sufficient level of authority and independence to exercise the necessary authority. Larger insurance companies may choose to appoint, as appropriate to the circumstances, a senior member of their compliance department. In small insurance companies, it may be appropriate to designate the office administrator, 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.

20.5.3-2 The MLRO is required to determine whether the information or other matters contained in the transaction report he has received give rise to a knowledge or suspicion that someone is engaged in money laundering.

---

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

[11] See The Insurance Commission's Guidelines for Assessing the Fitness and Propriety of Money Laundering Reporting Officers (MLRO) in The Bahamas.

20.5.3-3 In making this judgment, the MLRO should consider all other relevant information available within the insurance company 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.

20.5.3-4 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.

20.5.3-5 The MLRO will be expected to act honestly and reasonably and to make his determinations in good faith.

20.5.3-6 The Commission has oversight of a diverse group of business types and sizes. In practical terms, designated insurance companies 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 business.

20.5.3-7 Insurance companies 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 the money laundering and terrorist financing risks of his financial institution;
- have a basic knowledge of the Bahamian AML/CFT laws and rules;
- 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/CFT training at least once annually.

20.5.3-8 During the routine and/or random on-site examination, the Commission will determine whether the financial institution has complied with the above requirements.

20.6 Mandatory requirement to appoint a Compliance Officer

20.6.1 All life insurance companies are required, under section 20 of the FTRA, 2018, to appoint a Compliance Officer (CO). However, the insurance company may choose to combine the roles of the CO with the MLRO depending upon the size and nature of financial intermediary services that it is involved in.

20.6.2 The Compliance Officer should be appointed at a senior management level. They will be responsible for the implementation of the identified risk internal procedures and controls of the company. They will also be responsible for ongoing maintenance of the same.

20.7 Recognition of Suspicious Transactions

20.7.1 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.

20.7.2 Section 12(2) of the POCA requires that any person who knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering which is related to proceeds of drug trafficking or any related crime, and fails to report such knowledge or suspicion is guilty of an offence.

20.7.3 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 funds), 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 shall, as soon as practical after forming that suspicion, report that transaction or proposed transaction to the FIU.

20.8 Internal Reporting of Suspicious Transactions

20.8.1 The Financial Intelligence (Transactions Reporting) Regulations (FI(TR)R) requires financial institutions, which include insurance companies, 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.

20.8.2 All insurance companies offering financial intermediary services operating within or from The Bahamas are required to:

i. ensure that adequate policies and procedures are in place 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.

20.8.3 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 insurance companies 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.

20.8.4 All insurance companies have a clear obligation to ensure that:

- all agents and brokers are integrated into the company's anti-money laundering and countering the financing of terrorism programme and should monitor their compliance with the programme.

- each relevant employee knows to which person he or she should report suspicions; and

- there is a clear reporting chain under which those suspicions will be passed without delay to the MLRO.

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

20.9 Procedure for reporting suspicious transactions to the FIU

20.9.1 The form at *Appendix F* should be used for reporting suspicious transactions to the FIU, and the information should be typed[12]. These disclosures can be forwarded to the FIU in writing, by hand, by post, by facsimile message or by electronic mail, and in cases of urgency, reports may be made orally. However, this should still be followed by a written report.

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

20.9.3 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 insurance company may be required by the FIU to discontinue the transaction or cease activity related to the client's facility.

20.9.4 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 insurance company 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.

20.9.5 Access to the disclosure is restricted to financial analysts and other officers within the FIU.

20.9.6 It is also recognized that as a result of a disclosure, an insurance company may leave itself open to risks as a constructive trustee if moneys are paid away other than to the true owner. The insurance company 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.

20.9.7 Insurance companies are reminded that reporting to the Commission, the Central Bank, the Commissioner of Police and any duly authorized employee of the insurance company 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, an insurance company 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.

20.9.8 Following the submission of a disclosure report, an insurance company 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.

20.10 Feedback from the Investigating Authorities

20.10.1 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

[12] An electronic copy of the form is available from the FIU's website.

provided on a regular basis by the FIU.

20.10.2 Where applicable, insurance companies should ensure that all contact between 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 in order to establish the current status of a specific investigation.

IX. STAFF RECRUITMENT, EDUCATION AND TRAINING PROCEDURES

21 KNOW YOUR EMPLOYEE (KYE) PROCEDURES

21.1 The insurance industry in The Bahamas, as in any other jurisdiction, is challenged with managing a diverse range of risks such as legal, operational and reputational. 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 or appointing agents. In this regard, the Commission offers some guidance to its constituent financial institutions which may be useful in managing the related risks.

21.2 The screening process for hiring new employees may include:

- background and employee history checks; and
- reference checks, including police character reference (or equivalent).

21.3 Employers may also consider monitoring employees who display the following behavior:

- unusual transaction activities;
- unusual increases in business activities; and
- association with persons known to be involved in criminal activities.

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

22 STAFF AWARENESS PROGRAMMES

22.1 Insurance companies must take appropriate measures to familiarize all of 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.

22.2 Staff must be aware of their own personal AML/CFT 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.

22.3 It is important that all insurance companies covered by these Guidelines introduce adequate measures to ensure that staff members are fully aware of their responsibilities.

23. STAFF EDUCATION AND TRAINING PROGRAMMES

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

23.2 The Commission will host a few AML/CFT training seminars each year for its constituents.

23.3 The following training guideline is recommended:

23.4 New employees

23.4.1 A basic training course on money laundering, terrorist financing and proliferation 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 insurance company for the reporting of suspicious transactions.

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

23.5.1 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.

23.5.2 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 cash transactions, Travelers Cheques or postal money orders are involved. They should be reminded of the need for extra vigilance in these cases.

23.5.3 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 customer/client verification procedures. All employees should be familiarized with the financial institution's suspicious transaction reporting procedures.

23.6 Administration/operations supervisors and managers/Board of Directors

23.6.1 A higher level of instruction covering all aspects of AML/CFT policy and procedures should be provided to front line staff, Directors, and senior management with the responsibility for supervising or managing staff, and for auditing the system. Such instruction ought to 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 D*** for a summary of these offences).

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

23.7.1 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 and on new trends and patterns of criminal activity.

PART D GENERAL INSURANCE

X GENERAL INSURANCE OBLIGATIONS

24 General Insurance Companies and Intermediaries

This part of the Guidelines focuses on the obligations of general insurers and is designed to assist companies in applying provisions in the legislation consistently. The objective is to help general insurers refine current practices and to ensure that there is compliance with the FTRA, FTRR and POCA, 2018. General insurers must ensure that their intermediaries are aware of all requirements under the FTRA.

24.1 Reporting of Suspicious Transactions

24.1.1 General insurers are not defined in the FTRA as financial institutions, and as such they are not required to fulfil the same number of AML requirements as their counterparts in the life insurance sector. However, under sections 25-30 of the FTRA, general insurers are required to file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU). Regulation 14 of the FTRR, 2018, requires general insurers to file an STR where a proposal, proposer or a circumstance involving the proceeds of criminal conduct takes place. They must also file a report if the suspicion arises in relation to an offence under POCA, 2018, or if there is an identified risk. Punishment for failing to report an STR is up to five years imprisonment or a fine up to $500,000.00 or both.

24.1.2 The general insurance sector is considered to be a low risk for both money laundering and the concealment or conversion of the proceeds of crime. Nonetheless, general insurance is regarded as being at greater risk from fraudulent claims, rather than as a conduit for the proceeds of crime or money laundering. Most general insurance products do not, per se, offer obvious scope to be of use to money launderers. There is, however, scope for insurers to become unwittingly involved in criminal offences such as fraudulent claims or deliberately providing inaccurate information at inception, which may trigger provisions under the FTRA and POCA for suspicion reporting.

24.2.1 Appointment of MLRO and Compliance Officer

There is no obligation for a general insurer to appoint an MLRO or a Compliance Officer. They are, however, subject to the general requirements of the insurance legislation, and as such, have an obligation to have appropriate risk management systems and controls in place, including controls to counter the risk that the company may be used to further financial crime. Additionally, general insurers are also subject to the provisions of POCA and the Anti-Terrorism Act which establish the offences for money laundering, terrorist activities and proliferation financing.

If a company decides not to appoint an MLRO or Compliance Officer, then they **must** designate an individual who will be responsible for receiving reports of suspicious transactions and forwarding them to the FIU. Intermediaries should be advised of the name of the individual. Reporting lines must be clear, and employees must know who the designated individual is and their role in the reporting process. It is important for the company to formulate an AML/CTF policy and to implement controls and procedures

that clarify how senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. It should also identify which individuals will be responsible for implementing particular aspects of the policy.

The policy should set out how senior management undertakes the assessment of the money laundering and terrorist financing risks the company faces, and how these risks are to be managed. Doing so will provide a framework of direction to the company and its staff. Even in a small company, a summary of a high-level AML/CFT policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.

24.2.2 Risk Assessment

While the FTRA poses no obligation on general insurance companies to conduct a risk assessment, in accordance with good corporate governance principles the Commission requires that all insurance companies conduct a risk assessment. General insurers are also required to adopt a risk-based approach in consideration of their obligations under the FTRA and POCA, 2018 to report suspicious transactions. (For additional guidance please refer to sections 14.4, 14.5, 14.6.)

The comprehensive risk management system should be linked to the profile of the customer. Insurers who also offer life products will already be aware of the requirement to carry out Customer Due Diligence (CDD). A general insurer is not required to seek the equivalent level of information on their customers, however they are not exempted from utilizing best practices when conducting due diligence on its customers. The objective of CDD is to enable the insurer to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the insurer in determining when transactions are potentially suspicious. Effective CDD policies, procedures, and processes provide the critical framework that enables the insurer to comply with legislative and regulatory requirements including monitoring for and reporting of suspicious activity.

The due diligence process ought to be done at the earliest possible stage e.g., when a potential customer makes an approach or when an intermediary advises the insurer of a new customer, as well as when policies are renewed, or claims are submitted, based on the information that an insurer has available. To do this, however, requires the full commitment and support of senior management and the active co-operation across business units.

SUMMARY OF BAHAMIAN LAW ON AML/CFT

The Proceeds of Crime Act, 2018

This Act 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 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 Proceeds of Crime Act to the Financial Intelligence Unit. The Insurance Act, Chapter 347 also establishes the Insurance Commission, an independent statutory authority which has responsibility for ensuring that insurance companies comply with the provisions of the Act. These are outlined in Section 207 of the Insurance (Amendment) Act, 2009.

The Financial Transactions Reporting Regulations, 2018

The Financial Transactions Reporting Regulations, Ch. 368, 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, Ch. 367

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 Proceeds of Crime Act.

The Financial Intelligence (Transactions Reporting) Regulations, Ch.367

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.

This Act 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.

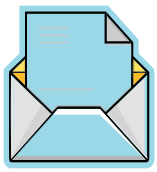
APPROVED STOCK EXCHANGES UNDER THE SCHEDULE TO THE FTRR

American Stock Exchange (AMEX)
Amsterdam Stock Exchange (Ainsterdamse Effectenbeurs)
Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)
Athens Stock Exchange (ASE) Australian Stock Exchange
Barcelona Stock Exchange (Bolsa de Valores de Barcelona)
Basle Stock Exchange (BaslerBorse)
Belgium Futures & Options Exchange (BELFOX)
Berlin Stock Exchange (Berliner Borse)
Bergen Stock Exchange (Bergen Bors)
Bermuda Stock Exchange
Bilbao Stock Exchange (Borsa de Valores de Bilbao)
Bologna Stock Exchange (Borsa Valori de Bologna)
Bordeaux Stock Exchange
Boston Stock Exchange
Bovespa (Sao Paulo Stock Exchange)
Bremen Stock Exchange (Bremener Wertpapierbarse)
Brussels Stock Exchange (Societede la Bourse des Valeurs Mobilieres/Effecten Beursvennootschap van Brussel)
Cayman Islands Stock Exchange
Cincinnati Stock Exchange
Copenhagen Stock Exchange (Kobenhayns Fondsbors)
Dusseldorf Stock Exchange (Rheinsch-westflilische Borse Zu Dusseldorf)
Florence Stock Exchange (Borsa Valori di Firenze)
Frankfurt Stock Exchange (Frankfurter Wertpapierbarse)
Geneva Stock Exchange
Genoa Stock Exchange (Borsa Valari de Genova)
Hamburg Stock Exchange (Hanseatische Vertpapier Borse Hamburg)
Helsinki Stock Exchange (Helsingen Arvapaperiporssi Osuuskunta)
Hong Kong Stock Exchange
Fukuoka Stock Exchange
Irish Stock Exchange
Johannesburg Stock Exchange
Korea Stock Exchange
Kuala Lumpur Stock Exchange
Lille Stock Exchange
Lisbon Stock Exchange (Borsa de Valores de Lisboa)
London Stock Exchange (LSE)
Luxembourg Stock Exchange (Societe de la Bourse de Luxembourg SA)
Lyon Stock Exchange
Madrid Stock Exchange (Balsa de Valores de Madrid)
Marseille Stock Exchange
Mexican Stock Exchange (Bolsa Mexicana de Valores)
Midwest Stock Exchange
Milan Stock Exchange (Borsa Valares de Milano)
Montreal Stock Exchange
Munich Stock Exchange (Bayerische Barse in Miinchen)
Nagoya Stock Exchange Nancy Stock Exchange
Nantes Stock Exchange
Naples Stock Exchange (Borsa Valori di 55apoli)
NASDAQ (The National Association of Securities Dealers Automated Quotations)
New York Stock Exchange
New Zealand Stock Exchange
Oporto Stock Exchange (Bolsa de Valores do Porto)
Osaka Stock Exchange
Oslo Stock Exchange (Oslo Bars)
Pacific Stock Exchange
Palermo Stock Exchange (Borsa Valari di Palermo)
Paris Stock Exchange
Philadelphia Stock Exchange
Rio de Janeiro Stock Exchange (BVRI)
Rome Stock Exchange (Borsa Valori di Roma)
Singapore Stock Exchange
Stockholm Stock Exchange (Stockholm Fondbors)
Stuttgart Stock Exchange (Baden-Wiirternbergische Wertpapierborse Zu Stuttgart)
Taiwan Stock Exchange
The Stock Exchange of Thailand
Tokyo Stock Exchange
Toronto Stock Exchange
Trieste Stock Exchange (Borsa Valori di Trieste)
Trondheim Stock Exchange (Trondheims Bors)
Turin Stock Exchange (Borsa Valori de Torino)
Valencia Stock Exchange (Borsa de Valares de Valencia)
Vancouver Stock Exchange
Venice Stock Exchange (Borsa Valori de Venezia)
Vienna Stock Exchange (Wiener Wertpapierbarse)
Zurich Stock Exchange (Ziircher Borse).

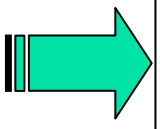
APPENDIX C

INSURANCE COMMISSION OF THE BAHAMAS
EVALUATION PROCESS FOR EXAMINATIONS

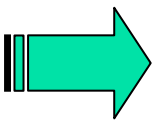
When an auditor has completed an examination of a financial institution/insurance company, the auditor is required to submit the examination form to the Insurance Commission (the Commission). The Commission will then:



Issue a notice To the financial institution (FI) that confirms that the Examination form has been received.



Evaluate the examination form and prepare a report of findings.



Issue a notice of findings and required corrective action, to FI and where Appropriate.

After an AML/CFT examination form is completed, the Commission's Examiners evaluate the financial institution's level of compliance by assigning a score to specific questions on the form. F.I.'s that score points of 95% to 100% are given a rating of "Good" while F.I.'s that score less than 80% are given a rating of "Very Poor". The table below illustrates the rating system for examinations.

Rating System for Examinations

Rating	Good	Acceptable	Poor	Very Poor
% Points	95% -100%	90%-94%	80%-89%	Less than 80%

Examinations which are rated 'Poor' or 'Very Poor' reveal that a financial institution is not in compliance with AML/CFT laws. Poorly rated financial institutions are informed about their specific deficiencies and a follow-up examination is arranged to address the weak areas.

During a follow-up examination, the financial institution is given advice on corrective action that must be taken to bring the institution in full compliance with AML/CFT laws. The entire follow-up process is completed after all plans for corrective action are discussed and executed by the financial institution.

APPENDIX D

Money Laundering /Terrorist Financing Offences, Penalties and Defenses

Money Laundering Offences

The POCA establishes several specific money laundering offences and penalties in performing their functions, Licensees 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 FCSP IS ACTING AS A FINANCIAL INSTITUTION. THEY ARE THEREFORE APPLICABLE TO RELEVANT CIRCUMSTANCES AFFECTING ALL SERVICES PROVIDED BY THE FCSP UNLIKE THE FTRA WHICH IS RESTRICTED TO THOSE CIRCUMSTANCES IN WHICH A FCSP 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 THE PROCEEDS OF CRIME ACT, 2018

For the purposes of the POCA, the term "criminal conduct" includes (1) drug trafficking, (2) bribery and corruption, (3) money-laundering, (4) any offence which may be tried in the Supreme Court of The Bahamas other than a drug trafficking offence and (5) an offence committed anywhere that, if committed in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the Proceeds of Crime Act, 2018.

The term "property" is defined under the POCA to mean, money and all other property, moveable or immoveable, including things in action and other intangible and incorporeal property.

Offence	*Penalties*	*Defenses*
Concealing, Transferring or Dealing with The Proceeds Of Criminal Conduct (Section 9) It is an offence to use, transfer, send or deliver to any person or place, or to dispose of or otherwise deal with any property, for the purpose of concealing or disguising such property, knowing, suspecting or having a reasonable suspicion that the property (in whole or in part, directly or indirectly) is the proceeds of criminal conduct or any identified risk activity. For this offence references to concealing or disguising property includes concealing or disguising the nature, source, location, disposition, movement or ownership or any rights with respect to the property. This section applies to a person's own proceeds of criminal conduct or where he knows or has reasonable grounds to suspect that the property he is dealing with represents the proceeds of another's criminal conduct.	On summary conviction - imprisonment for a term not exceeding 7 years or a maximum fine of $500,000, or both. On conviction on indictment – imprisonment for a term not exceeding 20 years or to an unlimited fine or both.	**It is a defense that the person concerned did not know, suspect or have reasonable ground to suspect that the funds in question are the proceeds of serious criminal conduct or any identified risk activity, or that he intended to disclose to a police officer his suspicion, belief or any matter on which such suspicion or belief is based, but there is a reasonable excuse for his failure to make a disclosure.**
Assisting Another to Conceal the Proceeds of Criminal Conduct (Section 9). It is an offence for any person to provide assistance to a criminal for the purpose of obtaining, concealing, retaining or investing funds, knowing or suspecting, or having reasonable grounds to suspect that those funds are the proceeds of serious criminal conduct and/ or a "relevant criminal offence".	On summary conviction - imprisonment for a term not exceeding 7 years or a maximum fine of $500,000, or both. On conviction on indictment – imprisonment for a term not exceeding 20 years or to an unlimited fine or both.	**It is a defense that the person concerned did not know, suspect or have reasonable ground to suspect that the funds in question are the proceeds of serious criminal conduct or any identified risk activity, or that he intended to disclose to a police officer his suspicion, belief or any matter on which such suspicion or belief is based, but there is a reasonable excuse for his failure to make a disclosure.**

Offence	*Penalties*	*Defenses*
Acquisition, Possession or Use (Section 11) It is an offence to acquire, use or possess property which are the proceeds (whether wholly or partially, directly or indirectly) of criminal conduct, knowing, suspecting or having reasonable grounds to suspect that such property are the proceeds of criminal conduct. Having possession is construed to include doing any act in relation to the property.	On summary conviction - imprisonment for a term not exceeding 7 years or a maximum fine of $500,000, or both. On conviction on indictment – imprisonment for a term not exceeding 20 years or to an unlimited fine or both.	That the property in question was obtained for adequate consideration. **[NB: The provisions of goods or services which assist in the criminal conduct does not qualify as consideration for the purposes of this offence.]**
Failure to Disclose (Section 12 and 13) It is an offence if a person fails to disclose to the FIU or a police officer that another person is engaged in money laundering related to proceeds of drug trafficking or a relevant offence where he knows, suspects or has reasonable grounds to suspect that such is the case and that knowledge or suspicion came to his attention in the course of his trade, profession, business or employment. Disclosure to the MLRO will suffice as disclosure to the authorities under this section.	On summary conviction – imprisonment for a term not exceeding 12 years or to a maximum fine of $500,000, or both. On conviction on indictment - imprisonment for a term not exceeding 20 years or to an unlimited fine or both.	It is a defense there is a reasonable excuse for not disclosing the information or other matter. It is also a defense to prove that the defendant took all reasonable steps to ensure that he complied with the statutory requirement to report a transaction or proposed transaction to the Financial Intelligence Unit; or that in the circumstances of the particular case, he could not reasonably have been expected to comply with the provision.
Tipping Off (Section 14) It is also an offence for anyone who knows suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering, to prejudice an investigation by so informing the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action. Preliminary enquiries of a customer 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 a suspicious transaction report has been submitted in respect of that customer unless the enquirer knows that an investigation is underway, or the enquiries are likely to prejudice an investigation. Where it is known or suspected that a suspicious transaction report has already been disclosed to the Financial Intelligence Unit, the Police or other authorized agencies and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.	On summary conviction - 12 years imprisonment or a maximum fine of $500,000, or both; On conviction on information - imprisonment for a term not exceeding 20 years or to an unlimited fine or both.	It is a defense if the person making the disclosure did not know or suspect that the disclosure was likely to prejudice the investigation, or that the disclosure was made under a lawful authority or with reasonable excuse.

(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 **FI(TR)R)**	Maximum fine on summary conviction is $50,000.	That all reasonable steps to comply with the provision have been satisfied, having regard to the nature of the financial institution and its activities. Having further regard to the existence and adequacy of any procedures of the institution, i.e. staff training and independent audits, and external guidelines from the FIU and the Commission.
Verification Offences **(FTRA s. 11)** It is an offence in each case to proceed to allow for the provision of a new facility or the conduct of any occasional transaction as the case may be without having verified the identity of the customer and any person on whose behalf he may be acting as required.	On summary conviction: maximum fine of $500,000 or imprisonment of 2 years or both; for legal persons a maximum fine of $1,000,000.	Same as above
Failure to do risk assessment **(FTRA. s.5)**	On summary conviction, imprisonment for a term of up to 5 years or a maximum fine of $500,000 or both.	Same as above
Identification and Due Diligence Offences **(FTRA. ss. 6, 12, 13, 16, 19-23)** 1) Opening an anonymous or fictitious account. 2) Failure to maintain books and records; destroying or removing such records. 3) Failure to make such information available in a timely manner upon a lawful request. 4) Failure to conduct ongoing due diligence. 5) Failure to maintain internal control programs.	On summary conviction, imprisonment for a term of up to 5 years or a maximum fine of $500,000 or both	Same as above
Recordkeeping Offences **(FTRA s. 18)** Failure to maintain records as required.	On summary conviction $20,000 maximum fine in the case of an individual and $100,000 maximum fine in the case of a corporation.	Same as above

Suspicious Transactions Reporting Offences **(FTRA s. 25)** (1) Failure to make an STR in circumstances that would require that a report be made. (2) Knowingly making any statement that is false or misleading in a material particular; or knowingly omitting from any statement any matter or thing without which the statement is false or misleading in a material particular. (3) Disclosing information about the contemplation or existence of an STR - (a) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for yourself or any other person; or (b) intentionally to prejudice any investigation into the commission or possible commission of a money laundering offence.	On summary conviction a maximum fine of up to $500,000 or a term of imprisonment of up to 5 years or both. On summary conviction a maximum fine of up to $500,000 or a term of imprisonment of up to 5 years or both. On summary conviction 12 years imprisonment a maximum fine of $500,000 or both. On conviction on indictment, imprisonment of up to 20 years or to a fine or both.	Same as the defense for failing to verify.
Failure to comply with any regulation under the Financial Intelligence (Transactions Reporting) Regulations or comply with any guideline, code of practice, directive, rules or other instructions issued by the FIU or a Regulator e.g. Maintain Internal Reporting Procedures, appoint an MLRO, and provide staff education and training programmes in the detection and prevention of money laundering.	Punishable by a fine of $10,000 on summary conviction or $50,000 for a first offence, and $100,000 for any subsequent offence on conviction in the Supreme Court.	It is a defense to for the financial institution to prove that it took all reasonable steps and exercised due diligence to comply with the requirements of the regulations, guidelines, codes or instructions as the case may be.

(3) (a) TERRORIST FINANCING OFFENCES UNDER THE ANTI-TERRORISM ACT (ATA), 2018

Offence	*Penalties*	*Defenses*
Offence of weapons training (s. 5) – Providing, receiving or inviting another to receive instruction or training in the making or use of firearms, explosives, chemical, biological or nuclear weapons or other weapons or mans of mass destruction whether it takes place inside or outside of The Bahamas or by electronic means. ***(EXCEPTIONS (s. 10):*** *if the act is done in the course of armed conflict in the defence of The Bahamas or for the purpose of preserving law and order in The Bahamas.)*	On summary conviction: a fine of $400,000 or imprisonment for 10 years or both. On conviction on indictment: a fine of $1,000,000 or imprisonment for 30 years or both.	
Use of chemical or nuclear weapons (s. 7, 8) Using a chemical agent solid, liquid or gaseous substance that produces an effect on a living organism by acting on the body tissue, or in an environment with air, water, or soil, inside or outside of The Bahamas. Using a nuclear weapon is also an offence.	On conviction on indictment: Imprisonment for life.	
Offence of Terrorism (s. 14) The carrying out (or aiding, abetting, counseling, procuring, inciting, conspiring or soliciting the carrying out) of an act: (a) that constitutes an offence under in any of the Treaties listed in the Schedule; or (b) for the purpose of intimidating the public or compelling a government or 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 whether public or private; or e. prejudice to national security or disruption of public safety.	Where the offence constitutes the offence of murder or treason, the punishment shall be death or in any other case, imprisonment for life.	
Offences of Terrorist Financing (s. 15) Providing or collecting funds; or providing financial services or making such services available to persons, whether by means that are direct or indirect, unlawful and willful (including through aiding, abetting, counseling, procuring, inciting, conspiring or soliciting in relation thereto) with the intention that the funds or services are to be used or with the knowledge that the funds or services are to be used in full or in part in order to carry out an offence of terrorism under section 14.	On conviction on information: a fine of $25,000,000- and 25-years imprisonment.	
Liability of a legal entity (Anti-Terrorism Act 2018 s. 41) Where an offence referred to under sections 14 or 15 is committed by a person responsible for the management or control of an entity located or registered in The Bahamas or in any other way organized under the laws of The Bahamas, that entity is also liable, in circumstances where the person committed the offence while in that capacity.	On conviction on information: a fine of $25,000,000.	
Liability of a director, manager, etc. **(ATA, 2018, s. 42)** Where an offence referred to under sections 5, 6, 7, 8, and 9 is committed by a director, manager, secretary or other similar officer of the body corporate; or any person purporting to act in such a capacity of an entity located or registered in The Bahamas or in any other way organized under the laws of The Bahamas, that entity is also liable, in circumstances where the person committed the offence while in that capacity.	On conviction: imprisonment for 25 years **and** a maximum fine of $5,000,000.	
Duty to Report (s. 49) Failure to report, where there are reasonable grounds to suspect that funds or financial services are related to or are to be used to facilitate an offence under the Act.	On summary conviction: a maximum fine of $250,000.	

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 terrorist 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 Licensees under the FTRA and the FIUA. Section 7 of the ATA requires the reporting of offences under the Act to be made to the Commissioner of Police.

(3) (b) SCHEDULE TO THE ATA - LIST OF TREATIES RELATIVE TO TERRORISM

- Convention on offences and certain other acts committed on Board Aircraft signed at Tokyo 14th September 1963.
- Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16th December 1970.
- Convention for the Succession of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23rd September 1971.
- 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.
- International Convention against the taking of Hostages, adopted by the General Assembly of the United Nations 17th December 1979.
- Convention on the Physical Protection of Nuclear Material adopted at Vienna on 3rd March 1980.
- 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, done at Montreal on 24th February 1988.
- Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10th March 1988.
- 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.
- Convention on the Marking of Plastic Explosives for the Purpose of Detection signed at Montreal on 1st March 1991.
- International Convention for the Suppression of Terrorist Bombings adopted by the General Assembly of the United Nations on 15th December 1997.
- International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9th December 1999.
- The Biological Weapons Convention entered into force on 26 March 1975; and
- The Chemical Weapons Convention (CWC) adopted by the Conference on Disarmament in Geneva on 3 September 1992.

.

APPENDIX E

To: From: (stamp of branch sending the letter)

Dear Sirs:

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

In accordance with the Money Laundering Guidelines for licensed financial institutions we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer _____

Title: (MR/MRS/MISS/MS) specify _____

Address including postal code _____

(as given by customer) _____

Date of birth _____ **Account Number**..... *(if known)*

Example of customer's signature_____

Please respond positively and promptly by returning the tear-off portion below

.....

To: The Manager (originating branch) **From:** (branch stamp)

Request for verification of the identity of (title and full name of customer)

With reference to your enquiry dated _____ we:

1) Confirm that the above customer *is/is not known to us.
2) *Confirm/cannot confirm the address shown in your enquiry.
3) *Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

The above information is given in strict confidence, for your private use only, and without any guarantee or responsibility on the part of this financial institution or its officials.

*Delete as applicable.

SUSPICIOUS TRANSACTION REPORT

Completed forms should be forwarded by hand, facsimile or courier to the Financial Intelligence Unit,
3rd Floor, Norfolk House, Frederick Street, P.O. Box SB-50086 Nassau, The Bahamas
Telephone No.: (242) 356-9808 or (242) 356-6327, Facsimile No.: (242) 322-5551

For Official Use Only FIU Reference Number:_____

To: **Financial Intelligence Unit – Fax: (242) 322-5551**

Date: _____ No. of Pages: _____

NB: Persons who report suspicious transactions are required, pursuant to section 25 of the Financial Transactions Reporting Act, 2018 to provide the Financial Intelligence Unit with the following information:

[A] Disclosing Institution

Disclosure Type:
- Proceeds of Crime ☐
- Drug Trafficking ☐
- Terrorism Finance ☐
- Identified Risk ☐
- Other ☐

Report No.:_____
Type of Transaction: _____

Name of Disclosing Institution: _____

Full Address: _____

_____

Sort Code: _____

Name of Person Handling Transaction:_____

Name of Money Laundering Reporting Officer/Focal Point Officer: _____

Direct Telephone No.: _____ Fax: _____

E-mail Address: _____

[B] Subject(s) of Disclosure - Individual

Full Name (Individual):_____

Date and Place of Birth:_____

Occupation/Business/Principal activity: _____

Full Address: _____

Telephone No. (Work) _____ Telephone No. (Home):_____

Fax: _____ E-mail Address: _____

[C] Subject(s) of Disclosure - Company

Company Name: _____

Type of Business: _____

Full Address: _____

_____

Telephone No.: _____ Fax No.: _____

E-mail Address: _____

Identification Documents (e.g., certificate of incorporation, memorandum and articles of association, etc. *if available*): _____

[D] Beneficial Owner(s)

(of the assets being the subject(s) of disclosure – if different from the subject(s) of disclosure above)

Full Name: _____

Date and Place of Birth (Individual): _____

Type of Business/Occupation: _____

Full Address: _____

_____

_____

Telephone No. (Work) _____ Telephone No. (Home): _____

Fax: _____ E-mail Address: _____

[E] Authorized Signatories

Information on authorized signatories and/or persons with power of attorney. (List further persons in an annex in the same manner as required below)

Full Name: _____

Date and Place of Birth (Individual): _____

Type of Business/Occupation: _____

Full Address _____

_____

_____

Telephone No. (Work) _____ Telephone No. (Home): _____

Fax: _____ E-mail Address: _____

[F] Intermediaries

Full Name (Individual): _____

Occupation: _____

Full

Address: _____

_____

Telephone No. (Work) _____ Telephone No. (Home): _____

Fax: _____ E-mail Address: _____

[G] Account Information/Activity

Type of Account: (e.g., individual/joint, trust, loan, etc.): _____

Account number: _____

Type of Currency: _____

Date Opened: _____

Date Closed: _____

Assets Held: _____

_____

_____

_____

Jurisdiction Where Assets Are Held: _____

Other Accounts Held by any of the Parties Involved: _____

REASONS FOR SUSPICION

Details of Sums Arousing Suspicion Indicating Debit or Credit Source and Currency Used	Amount	Debit or Credit	Date	Source	Currency

Please describe the details of the transaction(s) and the activity that promoted the report, giving reason for your suspicion and any steps that have already been taken (e.g., own investigations). Include information on any third party(ies) involved (e.g., payee, payer, deliverer of checks, stocks, guarantee beneficiary, guarantee surety, third party security creditors). Please add continuation sheets as necessary.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Submitted By: _____

Position Held: _____

You are asked to assist with completing the attached statistical analysis, which will help us to give you feedback – Thank you!

STATISTICAL INFORMATION

Nature of Institution	Please tick	Grounds for Disclosure? *Please tick all that apply*	Please tick
Bank		Media / Publicity	
Fund Manager		Internet Research	
Bureau Des Changes		Group Information	
Stockbroker		3rd Party Information	
Financial Advisor		Service of Production, Charging or Monitoring Order	
Insurance Company		Police enquiry	
Trust Company		Account Activity Not in Keeping with KYC	
Corporate Service Provider		Evidence of Forged Documentation	
Lawyer		Cash Transactions	
Accountant		Transitory Accounts – Immediate Layering	
Casino		High Risk Jurisdictions	
Real Estate Agent/Broker		Purchase and Surrender of Insurance Policy	
Credit Union		Unusual Forex Transactions	
Alternative Remittance		Repeat disclosures	
Local Regulator		Failure to comply with due diligence checks	
Other Regulator		Politically Exposed Persons (PEPs)	
Other (specify)		Other (specify)	
		Criminality Suspected	
Customer/Transaction		Drugs	
Involving at least one		Terrorism	
Long Standing Customer		Fraud	
New Customer		Attempted Fraud	
Electronic Banking		Revenue Fraud	
EURO Transaction		Insider Dealing	
Other (specify)		Corruption	
		Trafficking in Persons	
What currency was		Weapons and Ammunition Trafficking	
GBP		Ponzi Schemes and Lotteries	
USD		Possession, Theft and/or Trafficking in Stolen Gold or other precious metals	
EUR		Financing of Proliferation of Weapons of Mass	
CAD		United Nations Security Council Resolutions	
JPY		Illegal gambling	
BSD		Cyber crimes	
BRL		Regulatory Matters	
SEK		Tax Matters	
CHF		Unknown/undetermined	
Other (specify)		Other (specify)	

Completed forms should be forwarded to:
The Financial Intelligence Unit,
3rd Floor, Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas
Telephone No: (242) 356-9808 or (242) 356-6327, Fax No. (242) 322-5551

INSURANCE COMPANIES – TYPOLOGIES

LIFE INSURANCE

Case 1: Use of single premium policies

A fraudulently bankrupt subject used an account in the name of a family member to pay cash in and withdraw it our via a cheque to a lawyer. The lawyer then gave some money back in a cheque to the family member while the rest went to the subject's single premium life policy which was immediately surrendered. The surrender value was paid out to the family member's account.

Case 2: Use of single insurance policies

In 1990, a British insurance sales agent convicted of violating a money laundering statute. The insurance was involved in a money laundering scheme in which over USD 1.5 million was initially place with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute.

Case 3: Use of funds from proceeds of criminal activity – drug trafficking

On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank accounts and the transferred to an account in another jurisdiction. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

Case 4: Early policy redemption/cancellation

An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

Case 5: Cash payments to purchase insurance

Two subjects who lived outside the jurisdiction concerned deposited large cash sums in 4 single premium life policies. Subsequent premiums came from bank accounts which had been previously investigated for trade in illegal narcotics from Latin America to Western Europe.

Case 6: Fraud

A customer contracted life insurance of a 10-year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.

Case 7: Life insurance bought with proceeds of criminal activity

A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of USD 1 million in case of death. The other was a mixed insurance with value of over half this amount.

Case 8: PEP beneficiary

A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around USD 7 mission. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary – an alias – turned out to be a PEP.

Case 9: Third party payments of premiums
A husband and wife had taken out a life-insurance policy in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policy-holders but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organized tax fraud for which the couple involved was known.

Case 10: Collusion of customer intermediary and/or insurance company employee
A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in this policy.

GENERAL INSURANCE

Case 1: Fraud involving vessel
A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.

Case 2: General insurance claim fraud in insurance involving high value goods which were purchased with illicit funds.
In Norway in January 2004 a person reported a break-in in his house to his insurance company. The person reported that some of the stolen goods were jewelry worth NOK 110,000. Pursuant to his report he had sold a boat for NOK 2.7m and received jewelry worth NOK 500,000 as part of the payment for the sales amount. This person was on a low income and had no assets. In 2000 he had no income or assets at all. In 2001 his income was NOK 43,000 and in 2002 his income increased to NOK 233,000. Either it was not possible for him to have been the real owner of this valuable boat or it was the case that he paid for the boat with illicit funds.

Case 2: Fraud/Collusion
An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an 'accident' with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual,
confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organization running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of $2 million from similar fraud schemes carried out by terrorist groups.

INTERMEDIARIES

Case 1: Paying for life insurance with proceeds of criminal activity
A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for make the financial investment, three cheques from a bank account under his name, totaling USD 250,000, thus avoiding the raising suspicions with the insurance company.

Case 2: Accepting payments without performing adequate due diligence checks
Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run a couple of years before being closed with the request that the payment be made to a third party. This was often paid with receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Case 3: Inadequate due diligence and ongoing monitoring
An insurance company was established by a well-established insurance management operation.
One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

Case 4: Early withdrawal
A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around USD4000,000 deposited with a life insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out than an employee of the consulting company was involved in several similar cases. The account is frozen.

REINSURANCE

Case 1: Purchasing insurance with proceeds of crime
An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was
bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsure. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

Return Premiums
There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time
- a number of policies entered into by the same insurer/intermediary for small
- return premium being credited to an account different from the original account
- requests for return premiums in currencies different to the original premium, and
- regular purchase and cancellation of policies.

Claims

A claim is one of the principal methods of laundering money through insurance. Following are examples of where claims have resulted in reports of suspected money laundering and terrorist financing:[13]

- A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest "dirt money" for a profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organized by the purchasers to ensure a claim occurred and that they received "clean" money as a claim's settlement.

- During an on-site visit, an insurance supervisor was referred to a professional indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurer's papers, which identified one of the bank's clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.

- Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

[13] IAIS - Examples of money laundering and suspicious transactions involving insurance - October 2004