



INSURANCE COMMISSION
OF THE BAHAMAS



AUGUST 2026



GUIDELINES FOR THE INSURANCE INDUSTRY

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

This consultative paper is issued by the Insurance Commission of The Bahamas for the purpose of public consultation. It remains the property of the Insurance Commission of The Bahamas. Any reproduction, distribution, or use of this document, whether in whole or in part, is prohibited without the express written permission of the Insurance Commission of The Bahamas. The views expressed in this paper are for consultation purposes only and do not represent a final position or policy decision of The Insurance Commission of The Bahamas.



Silk Cotton House, Prospect Ridge Road - P.O. Box N-4844 - New Providence, The Bahamas
Tel: (242) 603-4183 - Email: info@icb.gov.bs - Website: www.icb.gov.bs

FOLLOW US



@INSURANCECOMMISSIONBAH

INSURANCE COMMISSION OF THE BAHAMAS

Silk Cotton House,
Prospect Ridge Road
P.O. Box N-4844
Nassau, Bahamas

Tel: (242) 603-4183
E-mail: amlcomp@icb.gov.bs
Website: www.icb.gov.bs

PURPOSE, SCOPE AND APPLICATION

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

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 and companies registered to carry on insurance business in and from within The Bahamas.

Notwithstanding any exemptions from certain AML/CFT/CPF obligations applicable to general insurance companies under the legislative framework, all persons and companies registered to carry on general insurance business are expected to implement appropriate AML/CFT/CPF controls consistent with the nature of their business. In particular, they shall have regard to the guidance contained in these Guidelines relating to customer due diligence, know-your-customer (KYC) measures, risk assessment and risk management.

The Commission expects all licensees to implement the measures set out in these Guidelines using a risk-based approach that is commensurate with the size, nature, and complexity of their insurance business. Licensees shall also have regard to applicable industry best practices to ensure that their AML/CFT/CPF frameworks remain effective and proportionate to the risks identified.

For the purposes of these Guidelines, requirements expressed as “shall” or “must” constitute mandatory minimum supervisory requirements. The terms “should” and “may” identify recommended practices or circumstances in which a registrant or licensee may adopt a proportionate risk-based approach. A registrant or licensee remains responsible for demonstrating to the Commission that its AML/CFT/CPF framework complies with applicable legislation and is effective and proportionate to its ML/TF/PF risks.

These Guidelines are intended to assist licensees in understanding and implementing their obligations under the applicable AML/CFT/CPF legislative framework. They provide practical guidance and examples of sound practices to support the development and maintenance of effective policies, procedures, systems, and controls. These Guidelines also support the Commission's supervisory objective of preserving the integrity and reputation of The Bahamas as a well-regulated international financial centre that maintains zero tolerance for money laundering, terrorist financing, proliferation financing, and other financial crime.

Unless the context otherwise requires, words importing the masculine gender include the feminine gender, words importing the feminine gender include the masculine gender, and words importing the singular include the plural, and vice versa.

The Commission may issue directives, guidance notes, advisories, or other supervisory communications from time to time to supplement or clarify these Guidelines, having regard to legislative amendments, evolving international standards, emerging risks, and supervisory expectations.

DRAFT

TABLE OF CONTENTS

PART	PAGE
A DEFINITIONS	10
B BACKGROUND	13
I MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING	13
1 Money Laundering	13
2 Terrorism Financing	13
3 Proliferation Financing	13
4 Vulnerabilities in the Insurance Sector	14
4.2 General Areas of Vulnerability	15
4.3 Product-Specific Vulnerabilities	15
4.4 Life Insurance and Investment-Related Products	15
4.5 Property, Motor, Marine, Liability, and Casualty Insurance	16
4.6 Marine Insurance and Commercial Insurance Activities	16
4.7 Life Insurance and Investment-Related Product Vulnerabilities	16
5 Application of the AML/CFT/CPF Legislative Framework to the Insurance Sector	17
6 International Standards and Supervisory Framework	18
6.1 The Financial Action Task Force (FATF)	18
6.2 The Caribbean Financial Action Task Force (CFATF)	18
6.3 International Association of Insurance Supervisors	18
II THE LEGISLATIVE AND REGULATORY STRUCTURE FOR AML/CFT IN THE BAHAMAS	19
7 AML/CFT/CPF Legislative and Supervisory Framework	19
8 Supervisory Responsibilities within the AML/CFT/CPF Framework	20
III INSURANCE COMPANIES AS FINANCIAL INSTITUTIONS	22
9 When is an insurance company a financial institution?	22
9.1 Application of the AML/CFT/CPF legislative framework	22
9.2 Life insurance companies	22
9.3 General insurance companies	23
9.4 Responsibilities relating to intermediaries	23
IV SUPERVISORY FRAMEWORK OF THE COMMISSION	24
10 The Commission	24
10.1 Establishment and supervisory mandate	24
10.2 AML/CFT/CPF supervisory framework	24
11 AML/CFT/CPF Examination Framework	24
11.1 Purpose and Scope of AML/CFT/CPF Examinations	24
11.2 Risk-based Supervisory Approach	25
11.3 Application of the AML/CFT/CPF Examination Framework	25
11.4 Types of AML/CFT/CPF Examinations	26
11.5 Routine Examinations	26
11.5.1 Purpose of Routine Examinations	26
11.5.2 Frequency of Examinations	26
11.5.3 Scope of Routine Examinations	27
11.5.4 Routine On-Site Examinations	27
11.5.5 Routine Off-Site Examinations	28
11.6 Waiver from a Routine On-Site Examination	28
11.6.1 Purpose of a Waiver	28

11.6.2	Request for a Waiver	28
11.6.3	Eligibility for a Waiver	28
11.6.4	Conduct of an Off-Site Examination Following a Waiver	29
11.6.5	Effect of a Waiver	29
11.7	Follow-Up Examinations	30
11.7.1	Purpose of Follow-Up Examinations	30
11.7.2	Circumstances Giving Rise to a Follow-Up Examinations	30
11.7.3	Conduct of Follow-Up Examinations	30
11.8	Random Examinations	30
11.8.1	Purpose of Random Examinations	30
11.8.2	Scope of Random Examinations	31
11.9	Special Examinations	31
11.9.1	Purpose of Special Examinations	31
11.9.2	Circumstances Giving Rise to a Special Examination	31
11.10	AML/CFT/CPF Risk Assessments	31
11.10.1	Purpose of AML/CFT/CPF Risk Assessments	31
11.10.2	Assessment Outcomes	32
11.11	Supervisory Findings, Remediation and Enforcement Action	32
11.11.1	Supervisory Findings	32
11.11.2	Remediation Plans	32
11.11.3	Failure to Remediate	31
11.12	Registrant and Licensee Responsibilities During Supervisory Assessments	30
11.12.1	Cooperation with the Commission	30
11.12.2	Maintenance of Effective AML/CFT/CPF Frameworks	30
11.12.3	Implementation of Corrective Measures	30
12	Industry Engagement and Supervisory Outreach	30
C	ESTABLISHING AN EFFECTIVE AML/CFT/CPF FRAMEWORK	34
V.	INTERNAL AML/CFT/CPF GOVERNANCE, CONTROLS AND PROCEDURES	34
13.	Internal AML/CFT/CPF Framework	
13.1	Establishment of an AML/CFT/CPF Framework	34
13.2	AML/CFT/CPF Risk Assessment and Risk Management	35
13.3	New Products, Business Practices and Technologies	35
13.4	Senior Management Responsibility and Culture of Compliance	36
13.5	Internal AML/CFT/CPF Policies, Procedures and Controls	36
13.6	Group-Wide AML/CFT/CPF Programmes	37
13.7	Foreign Branches and Subsidiaries	38
13.8	Independent Testing and Review	38
VI.	CUSTOMER DUE DILIGENCE (CDD) AND KNOW YOUR CUSTOMER (KYC) REQUIREMENTS	39
14	CUSTOMER IDENTIFICATION, VERIFICATION AND DUE DILIGENCE REQUIREMENTS	39
14.1	Purpose of Customer Due Diligence	39
14.2	Application of CDD Requirements Across the Insurance Sector	39
14.3	Exemptions and Exceptions to Customer Due Diligence Requirements	40
14.3.5	Publicly Traded Companies	40
14.4	Customer Identification and Verification	40
14.5	Identification and Verification of Legal Persons and Legal Arrangements	41
14.6	Beneficial Ownership and Control	41
14.7	Customer Due Diligence for Beneficiaries of Life and Invest-Related Insurance Policies	42
14.8	Politically Exposed Persons	42
14.8.4	Foreign PEPs	43
14.8.5	Domestic PEPs	43
14.8.6	International Organisation PEPs	43
14.8.7	Family Members and Close Associates	43

14.8.8	PEP-Connected Legal Persons and Legal Arrangements	43
14.9	Enhanced Due Diligence Measures for PEPs	44
14.10	Ongoing Due Diligence and Updating Customer Information	44
14.11	Risk-Based Customer Assessment	45
14.12	Customer Risk Categorisation	45
14.13	General Insurance Companies and Intermediaries	45
14.14	Reliability and Updating of Customer Information and Documentation	46
14.15	Reliance on Customer Due Diligence Performed by Third Parties	46
14.16	Failure to Complete Customer Due Diligence	47
14.17	Tipping Off During Customer Due Diligence	47
15	HIGHER-RISK COUNTRIES, JURISDICTIONS AND CROSS-BORDER RELATIONSHIPS	47
15.1	General Principles	47
15.2	Geographic Risk Factors	47
15.3	Higher-Risk Countries and Jurisdictions	48
15.4	Enhanced Measures for Higher-Risk Geographic Exposure	48
15.5	Cross-Border Relationships and Transactions	49
15.6	Foreign Intermediaries, Reinsurers, Insurance Managers, and other Counterparties	49
16	SANCTIONS SCREENING AND TARGETED FINANCIAL SANCTIONS (TFS)	50
16.1	General Obligations	50
16.2	Sanctions Screening Requirements	50
16.3	Sanctions Screening Shall Be Conducted	50
16.4	Sanctions Screening Systems and Controls	51
16.5	Management of Potential Sanctions Matches	51
16.6	Record Keeping and Training	52
17	CUSTOMER IDENTIFICATION VERIFICATION AND DOCUMENTARY EVIDENCE REQUIREMENTS	52
17.1	General Requirements for Verification of Identity	52
17.2	Timing of Verification	52
17.3	Verification Information and Documentation for Natural Persons	53
17.4	Verification of Legal Persons	53
17.5	Verification of Partnerships, Unincorporated Associations, Charities and Other Similar Organisations	54
17.6	Verification of Legal Arrangements	54
17.7	Verification of Persons Acting on Behalf of Customers	54
17.8	Additional Verification Consideration for Non-Resident Customers	54
17.9	Reliability and Updating of Verification Information	55
17.10	Verification Through Third Parties	55
17.11	Confidentiality and Risk of Tipping Off During Verification	55
18	ONGOING DUE DILIGENCE AND MONITORING OF CUSTOMER RELATIONSHIPS	55
18.1	Purpose and Application of Ongoing Due Diligence	55
18.2	Ongoing Monitoring of Customer Relationships	56
18.3	Updating Customer Information	56
18.4	Review of Customer Information and Risk Assessment	57
18.5	Simplified Due Diligence	58
18.6	Enhanced Due Diligence	58
18.7	Monitoring of Higher-Risk Customer Relationships	59
18.8	Identification of Structuring and Other Unusual Activity	59
19.	RELIANCE ON THIRD PARTIES FOR CUSTOMER DUE DILIGENCE MEASURES	59
19.1	General Principles	59
19.2	Conditions for Reliance on Third Parties	59
19.3	Eligible Third Parties	60
19.4	Reliance Within Corporate Groups	60
19.5	Written Confirmation and Evidence of Reliance	60

19.6	Limitations on Reliance	61
19.7	Reliance Does Not Transfer Responsibility	61
VII.	RECORD KEEPING PROCEDURES	61
20	RECORD KEEPING REQUIREMENTS	61
20.1	Purpose and General Principles	61
20.2	Records to be Maintained	61
20.3	Customer Identification and Verifications Records	62
20.4	Records Relating to Transactions	62
20.5	Records Relating to Suspicious Activity	63
20.6	Records Maintained in Electronic Form	63
20.7	Reliance on Third Parties	63
20.8	Retention Period	63
20.9	Destruction of Records	63
20.10	Failure to Maintain Records	64
21	ELECTRONIC PAYMENT TRANSFERS	64
21.1	General Requirements	64
21.2	Information Accompanying Electronic Payment Transfers	64
21.3	Cross Border Electronic Payment Transfers	64
21.4	Domestic Electronic Payment Transfers	65
21.5	Monitoring and Record Retention	65
21.6	Compliance with Applicable Legislation	65
VIII.	PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS	65
22	THE FINANCIAL INTELLIGENCE UNIT (THE FIU)	65
22.1	Role of the Financial Intelligence Unit	65
22.2	Obligation to Report Suspicious Transactions	65
22.3	Recognition of Identification of Suspicious Activity	66
22.4	Internal Reporting of Suspicious Transactions	67
22.5	Appointment and Role of the Money Laundering Reporting Officer or Designated Reporting Officer	67
22.5.1	Appointment of Reporting Officer	67
22.5.2	Authority, Independence and Access	68
22.5.3	Responsibilities of the MLRO or DRO	68
22.5.4	MLRO Assessment and Decision -Making	68
22.6	Appointment and Role of the Compliance Officer (CO)	69
22.7	Submission of Suspicious Transaction Reports to the FIU	69
22.8	Confidentiality and Tipping Off	70
22.9	Feedback from the FIU and Communication with Competent Authorities	70
IX.	STAFF RECRUITMENT, EMPLOYEE SCREENING, EDUCATION AND TRAINING	71
23	Know Your Employee (KYE) Procedures	71
23.1	General Principles	71
23.2	Employee Screening	71
23.3	Ongoing Employee Integrity	71
23.4	Responsibility of Senior Management	72
24	AML/CFT/CPF EDUCATION, TRAINING AND AWARENESS	72
24.1	General Requirements	72
24.2	Training Content	72
24.3	Role-Specific Training	73
24.4	Ongoing Awareness	73
24.5	Training Records and Effectiveness	73

APPENDICES

A	Overview of the Bahamian AML/CFT/CPF Legislative Framework	74
B	AML/CFT/CPF Examination Process and Supervisory Assessment	75
C	Minimum Information to Support the Submission of a Suspicious Transaction Report (STR)	77
D	Examples of AML/CFT/CPF Typologies, Risks and Red Flags in the Insurance Sector	80
E	AML/CFT/CPF Information Resources	83

DRAFT

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.

“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.

“DRO” means Designated Reporting Officer

“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” or **“foreign branch”** 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.

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

“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.

“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.

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

“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, intermediaries and associations and AML/CFT/CPF education and training initiatives 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 their 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; 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.”¹
- 2.3 The United Nations Security Council (UNSC) imposes targeted financial sanctions, including asset freezes, travel bans, and arms embargoes, on individuals, groups, undertakings, and entities designated under the ISIL (Da’esh) and Al-Qaida sanctions regime established pursuant to United Nations Security Council Resolution (UNSCR) 1267 and its successor resolutions. The sanctions list identifies designated persons and entities associated with terrorism.

¹ UN 1999 International Convention for the Suppression of the Financing of Terrorism

- 2.4 Registrants and Licensees must ensure that their AML/CFT/CPF policies, procedures, and controls give full effect to the obligations prescribed under Part IV – Implementation of United Nations Security Council Resolutions (sections 43–49) of the Anti-Terrorism Act, 2018 as amended, including the identification of designated persons and entities and the implementation of applicable targeted financial sanctions without delay.
- 2.5 Registrants and licensees are advised that the United Nations Security Council sanctions list is updated periodically. Upon receipt by the Office of the Attorney General, updates to the list of individuals and entities designated by the United Nations Security Council as terrorist entities, together with their associates where applicable, are circulated by the National Identified Risk Framework Coordinator, who is also responsible for maintaining the updated list in accordance with section 43 of the Anti-Terrorism Act, 2018, as amended. Registrants and Licensees shall ensure that their sanctions screening processes are updated promptly to reflect any revisions to the list.

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, agents, and brokers must establish, implement, and maintain effective internal controls, policies, and procedures to mitigate the risk of proliferation financing. They must ensure that all relevant employees receive ongoing training and are aware of their responsibilities for implementing and complying with these measures.
- 3.4 Registrants and licensees are encouraged to refer to the *FATF Guidance on Counter Proliferation Financing* (www.fatf-gafi.org) and the GFSR's Counter Proliferation Financing Guidelines (www.icb.gov.bs)

4. VULNERABILITIES IN THE INSURANCE SECTOR

- 4.1 Insurance products and services may be misused to launder criminal proceeds, finance terrorism, or facilitate proliferation financing. Their vulnerability depends on factors such as product type and complexity, contractual features, distribution channels, payment methods, customer profile, geographic exposure, and the nature of the business relationship. These factors shall be considered when assessing ML/TF/PF risks associated with insurance activities. The vulnerability of a product or service also depends on its specific characteristics, the customer relationship, and the circumstances in which it is offered or used.

4.2 General Areas of Vulnerability

- 4.2.1 The insurance sector may be vulnerable to money laundering, terrorist financing, and proliferation financing where products, services, distribution channels, or payment mechanisms are misused. Areas of potential vulnerability across the insurance sector include:

- the use of insurance products, intermediaries, or complex ownership structures to obscure the identity of customers, beneficial owners, beneficiaries, or other parties to a transaction;
- the acceptance of cash or other higher-risk payment methods for premiums, refunds, or claim settlements;
- cross-border transactions involving customers, beneficiaries, intermediaries, counterparties, or funds, particularly where higher-risk jurisdictions are involved;
- the movement of illicit funds through premium payments, refunds, claims payments, settlements, or other insurance-related transactions;
- fraudulent or inflated claims, including attempts to convert illicit funds into legitimate-looking proceeds;
- payments to or from unrelated third parties without a clear economic or legitimate purpose; and
- weaknesses in customer due diligence, beneficial ownership identification, ongoing monitoring, sanctions screening, and the detection and reporting of suspicious transactions.

4.3 Product-Specific Vulnerabilities

- 4.3.1 Certain insurance products and activities may present increased vulnerability to money laundering, terrorist financing, and proliferation financing due to their features, the movement of funds associated with them, or the manner in which they are distributed and used. While the level of risk varies depending on factors such as the nature of the product, customer profile, distribution channel, payment methods, and geographic exposure, licensees should be aware of the potential vulnerabilities associated with different classes of insurance business. Product-specific vulnerabilities include:

4.4 Life Insurance and Investment-Related Products

- 4.4.1. Life insurance products with savings, investment, or cash value features may present heightened money laundering risks due to their ability to accumulate value and generate legitimate-looking proceeds. Vulnerabilities may arise through:

- the purchase of policies using illicit funds with the intention of later surrendering the policy or receiving policy proceeds;
- the use of policy loans, withdrawals, refunds, or surrender payments to convert illicit funds into apparently legitimate assets;
- the use of beneficiaries, policy owners, or other parties to obscure the identity of the person who ultimately controls or benefits from the policy; and
- third-party payments, changes in ownership or beneficiaries, and other transactions that lack a clear legitimate purpose.

- 4.4.2 Certain life insurance products may involve activities where the insurer facilitates the movement, transfer, or management of funds on behalf of policyholders, beneficiaries, or other parties. Where a long-term insurance company acts as an agent, intermediary, or conduit for the movement of funds, such activities may fall within the scope of financial intermediary services under the Financial Transactions Reporting Act, 2018.

In such circumstances, licensees shall ensure that appropriate AML/CFT/CPF measures are applied, including customer due diligence, risk assessment, ongoing monitoring, and reporting obligations, where applicable.

4.5 Property, Motor, Marine, Liability, and Casualty Insurance

4.5.1 General insurance products generally present lower inherent money laundering and terrorist financing risks than investment-related products; however, they may still be vulnerable to misuse. Potential vulnerabilities include:

- fraudulent, inflated, or staged claims designed to generate payments that may appear to be legitimate proceeds;
- the use of insurance products to cover assets acquired through illicit activities;
- premiums, refunds, or claims payments involving unexplained third parties or parties unrelated to the policy;
- complex ownership arrangements or corporate structures used to conceal the identity of customers, beneficial owners, or beneficiaries; and
- cross-border transactions involving customers, intermediaries, counterparties, or assets located in higher-risk jurisdictions.

4.6 Marine Insurance and Commercial Insurance Activities

4.6.1 Marine and other commercial insurance activities may present additional vulnerabilities due to the involvement of international trade, complex contractual arrangements, multiple parties, and cross-border transactions. Risks may arise from:

- the use of insurance arrangements connected to goods, vessels, or transactions associated with illicit activities;
- involvement of sanctioned persons, entities, vessels, or jurisdictions;
- complex ownership structures or intermediaries that obscure the parties involved in the transaction; and
- exposure to proliferation financing risks where insurance services support activities connected to sanctioned goods, materials, or jurisdictions.

Registrants and Licensees should apply a risk-based approach when assessing these vulnerabilities and implement appropriate measures to identify, assess, and mitigate ML/TF/PF risks associated with their products, services, customers, and distribution channels.

4.7 Life Insurance and Investment-Related Product Vulnerabilities

4.7.1 Certain life insurance and investment-related products may present increased vulnerability to money laundering and terrorist financing due to their ability to accumulate value, facilitate the movement of funds, or provide access to legitimate-looking proceeds.

4.7.2 The level of vulnerability associated with an insurance product may vary depending on factors including, but not limited to, the nature and complexity of the contract, product features, distribution channels, payment methods, customer profile, geographic exposure, and the nature of the business relationship.

Examples of life insurance products that may present increased vulnerability include:

- unit-linked or with-profit single premium contracts;

- single premium life insurance policies with cash value features;
- fixed and variable annuities; and
- transferred or second-hand endowment policies.

4.7.3 These products may be susceptible to misuse where illicit funds are used to purchase policies, where policies are surrendered or mature to provide access to apparently legitimate proceeds, or where changes to ownership, beneficiaries, or payment instructions are used to obscure the source or destination of funds.

5. APPLICATION OF THE AML/CFT/CPF LEGISLATIVE FRAMEWORK TO THE INSURANCE SECTOR

5.1 The AML/CFT/CPF legislative framework applicable to the insurance sector in The Bahamas varies according to the nature of the insurance business conducted and the legislative provisions applicable to the different classes of insurance business.

5.2 Life insurance companies and external insurance companies that are defined as financial institutions under the Financial Transactions Reporting Act, as amended (FTRA), together with their agents, brokers, and salespersons acting in relation to those activities, are subject to the AML/CFT/CPF requirements applicable to financial institutions under the FTRA, the Financial Intelligence Unit Act, 2023, the Financial Transactions Reporting Regulations, 2018, and any regulations, codes, and guidelines issued pursuant to those enactments.

5.3 General insurance companies are not defined as financial institutions under the FTRA. However, general insurance companies, together with their agents, brokers, and salespersons, are required to comply with the applicable provisions of the Financial Transactions Reporting Regulations, 2018, and remain subject to the Proceeds of Crime Act, 2018, the Anti-Terrorism Act, 2018, and other applicable AML/CFT/CPF legislation, including obligations relating to suspicious transaction reporting, targeted financial sanctions, and other statutory requirements.

5.4 In addition to applicable legislative requirements, all insurance companies and insurance intermediaries are expected to adopt a risk-based approach to the management of ML/TF/PF risks. This includes establishing, implementing, and maintaining effective AML/CFT/CPF policies, procedures, systems, and controls that are proportionate to the nature, size, complexity, and risk profile of their business activities.

5.5 Insurance companies are responsible for ensuring that their distribution channels, including agents, brokers, and salespersons, are aware of and understand their AML/CFT/CPF obligations and are provided with appropriate guidance, training, and oversight to support compliance with applicable requirements. Insurance companies shall also ensure that intermediaries acting on their behalf operate within an appropriate AML/CFT/CPF framework.

5.6 Insurance intermediaries, including agents and brokers, are responsible for establishing and maintaining their own AML/CFT/CPF policies, procedures, systems, and controls appropriate to their own business activities and risk exposure. While these frameworks may incorporate or align with elements of an insurer's AML/CFT/CPF Programme, intermediaries remain responsible for ensuring that their own obligations are adequately addressed, including customer due diligence, record-keeping, employee training, ongoing monitoring, sanctions screening, and the identification and reporting of suspicious transactions.

5.7 Accordingly, compliance with AML/CFT/CPF obligations is a shared responsibility across the insurance sector. Insurance companies and intermediaries must ensure that appropriate measures are implemented to identify, assess, manage, and mitigate ML/TF/PF risks arising from their

products, services, customers, distribution channels, and geographic exposure.

6. INTERNATIONAL STANDARDS AND SUPERVISORY FRAMEWORK

6.1 The Financial Action Task Force (FATF)

- 6.1.1. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Group of Seven (G7) countries to develop and promote policies to protect the global financial system from money laundering. Over time, the FATF's mandate has expanded to include combating terrorist financing and proliferation financing. The FATF is the global standard-setting body for anti-money laundering, countering the financing of terrorism, and countering the financing of proliferation (AML/CFT/CPF), and develops internationally recognised standards and guidance to assist jurisdictions in establishing effective frameworks to address these risks.
- 6.1.2 The FATF Recommendations, first issued in 1990 and subsequently revised, provide a comprehensive framework of measures that jurisdictions should implement to combat money laundering, terrorist financing, and proliferation financing. The Recommendations establish global standards covering areas including criminalisation, preventive measures for financial institutions and designated non-financial businesses and professions, supervision, transparency of beneficial ownership, sanctions, financial intelligence, law enforcement, and international cooperation. The FATF Recommendations are intended for universal application and are implemented by jurisdictions through their respective legal, regulatory, and supervisory frameworks.
- 6.1.3 The FATF works closely with a network of FATF-style regional bodies (FSRBs) and other international partners to promote the effective implementation of the FATF Recommendations globally. These regional bodies support awareness, conduct mutual evaluations, and assist jurisdictions in strengthening their AML/CFT/CPF frameworks. Through this network, the FATF promotes a consistent and coordinated global approach to addressing ML/TF/PF risks.

6.2 The Caribbean Financial Action Task Force (CFATF)

- 6.2.1 The Caribbean Financial Action Task Force (CFATF) is a FATF-Style Regional Body (FSRB) comprising jurisdictions from the Caribbean Basin, Central America, and South America. Established in 1992, the CFATF promotes the effective implementation of international standards to combat money laundering, terrorist financing, and proliferation financing. As a member of the FATF Global Network, the CFATF supports its members in implementing the FATF Recommendations and strengthening their AML/CFT/CPF frameworks.
- 6.2.2 The principal objective of the CFATF is to promote the effective implementation of the FATF Recommendations through mutual evaluations, follow-up processes, typology studies, technical assistance, training, and regional cooperation. The CFATF also facilitates collaboration among its members to identify and address emerging ML/TF/PF risks and to strengthen the effectiveness of AML/CFT/CPF systems across the region.
- 6.2.3 The Bahamas is a founding member of the CFATF and is committed to implementing the FATF Recommendations through its legislative, regulatory, and supervisory framework. As part of the CFATF mutual evaluation process, The Bahamas periodically undergoes assessments to determine the extent to which its AML/CFT/CPF framework complies with the FATF Recommendations and effectively mitigates ML/TF/PF risks. The outcomes of these evaluations inform legislative reforms, regulatory enhancements, and supervisory practices across all sectors, including the insurance industry.
- 6.2.4 Further information on the CFATF, its work, and the FATF Global Network is available on the CFATF website.

6.3 International Association of Insurance Supervisors (IAIS)

The International Association of Insurance Supervisors (IAIS) is the global standard-setting body for the insurance sector. Its mission 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 and to contribute to global financial stability.

The Bahamas, through the Insurance Commission of The Bahamas, is a member of the IAIS and is committed to implementing internationally recognised supervisory standards, including the Insurance Core Principles (ICPs). The ICPs provide a globally accepted framework for the regulation and supervision of insurers and address key areas such as corporate governance, risk management, supervisory review, group-wide supervision, and cooperation and information sharing.

These Guidelines have been developed having regard to the FATF Recommendations, the IAIS Insurance Core Principles, and the applicable legislative framework of The Bahamas, with the objective of promoting effective AML/CFT/CPF risk management practices within the insurance sector.

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

7. AML/CFT/CPF LEGISLATIVE AND SUPERVISORY FRAMEWORK

7.1 The Bahamian substantive law relating to AML/CFT/CPF is contained in the:

- Proceeds of Crime Act, 2018 as amended
- Financial Transactions Reporting Act, 2018 as amended
- Financial Transactions Reporting Regulations, 2018 as amended
- Financial Transaction Reporting (Wire Transfers) Regulations, 2018
- Financial Intelligence Unit Act, 2023
- Financial Intelligence (Transactions Reporting) Regulations, 2000; and
- Anti-Terrorism Act, 2018 as amended

7.2 The AML/CFT/CPF legislative framework, including all amendments and subsidiary legislation, establishes the measures that registrants and licensees are required to implement to prevent, detect, and deter money laundering, terrorist financing, and proliferation financing. These measures are designed to ensure that registrants and licensees identify and assess ML/TF/PF risks, apply appropriate customer due diligence and ongoing monitoring measures, maintain adequate records, implement effective internal controls, comply with targeted financial sanctions, and identify and report suspicious transactions to the appropriate authorities. Collectively, these measures support the integrity of the financial system and ensure that relevant information is available to assist competent authorities in the investigation and prosecution of financial crimes.

7.3 In addition to the principal legislation and subsidiary legislation, registrants and licensees shall have regard to relevant supervisory guidance issued by the Insurance Commission of The Bahamas. Such guidance supports the effective implementation, governance, and oversight of AML/CFT/CPF frameworks within the insurance sector.

7.4 Relevant supervisory guidance includes the Commission's Guidelines for the Compliance Function, the Corporate Governance and Assessment Criteria, and the Risk-Based Supervisory Framework Guidance. Collectively, these guidelines provide additional guidance regarding the responsibilities of the Board, senior management, compliance function, and other relevant stakeholders in establishing effective governance structures, risk management frameworks, internal controls, and processes that support compliance with AML/CFT/CPF obligations.

The Commission's Risk-Based Supervision framework supports a proportionate approach to

supervision by considering the nature, scale, complexity, and ML/TF/PF risk profile of each licensee when assessing the effectiveness of its AML/CFT/CPF framework.

8. SUPERVISORY RESPONSIBILITIES within the AML/CFT/CPF FRAMEWORK

- 8.1 The Insurance Commission of The Bahamas is responsible for the prudential and AML/CFT/CPF supervision of the insurance sector and conducts AML/CFT/CPF on-site examinations of insurance companies and insurance intermediaries within its regulatory remit. The Commission's authority to supervise insurance companies and conduct supervisory activities is derived from sections 8 and 207 of the Insurance Act, Chapter 347, and section 45 of the External Insurance Act, Chapter 348.
- 8.2 The national AML/CFT/CPF framework assigns supervisory responsibility for different sectors of the financial system and designated non-financial businesses and professions (DNFBPs) to the relevant competent authorities. Within this framework, the Central Bank of The Bahamas supervises the banking and trust companies sector; the Securities Commission of The Bahamas supervises the securities and investment funds sector; the Inspector of Financial and Corporate Services supervises financial and corporate service providers; the Compliance Commission supervises designated non-financial businesses and professions (DNFBPs); and the Gaming Board For The Bahamas supervises casinos and gaming houses.
- 8.3 The Financial Intelligence Unit (FIU) is the agency responsible for receiving, analysing, and disseminating suspicious transaction reports and other financial intelligence in accordance with its statutory mandate. The FIU plays a central role in supporting the detection, prevention, and investigation of money laundering, terrorist financing, and proliferation financing activities.

TABLE 1: Competent Authorities Responsible for AML/CFT/CPF Supervision in The Bahamas

Competent Authority	Sector Supervised	Primary AML/CFT/CPF Supervisory Responsibility
Insurance Commission of The Bahamas (ICB)	Insurance companies and insurance intermediaries, medical plan service providers, pension fund service providers.	Supervises compliance with the AML/CFT/CPF legislative framework, including risk-based implementation of AML/CFT/CPF measures by insurance companies and intermediaries.
Central Bank of The Bahamas (CBOB)	Banks, trust companies, money transmission businesses and credit unions	Supervises financial institutions within its jurisdiction for compliance with AML/CFT/CPF legislative and regulatory requirements.
Securities Commission of The Bahamas (SCB)	Investment funds, securities firms and the securities industry, financial and corporate service providers and digital asset business and service providers.	Supervises securities sector participants for compliance with applicable AML/CFT/CPF obligations.
Compliance Commission (CC)	Designated Non-Financial Businesses and Professions (DNFBPs), excluding casinos	Supervises designated non-financial businesses and professions for compliance with AML/CFT/CPF legislative requirements.
Gaming Board for The Bahamas	Casinos and gaming houses	Supervises casinos and gaming houses for compliance with AML/CFT/CPF legislative and regulatory requirements.
Financial Intelligence Unit (FIU)	All reporting entities	Receives, analyses and disseminates Suspicious Transaction Reports (STRs) and other financial intelligence in accordance with the Financial Intelligence Unit Act. The FIU is not the AML/CFT/CPF supervisory authority for reporting entities.

Note: The Office of the Attorney General has the overall responsibility for national policy relating to the AML/CFT/CPF framework. Operational AML/CFT/CPF supervision is undertaken by the competent supervisory authorities listed above in accordance with their respective legislative mandates.

III. THE INSURANCE COMPANIES AS FINANCIAL INSTITUTIONS

9. When is an insurance company a financial institution?

9.1 Application of the AML/CFT/CPF legislative framework

For AML/CFT/CPF purposes, an insurance company is subject to the requirements of the AML/CFT/CPF legislative framework where the nature of the insurance business it conducts falls within the definition of a financial institution under the Financial Transactions Reporting Act (FTRA), 2018 as amended.

The AML/CFT/CPF framework recognises that certain insurance activities may present ML/TF/PF risks due to the acceptance, management or payment of funds, the nature of the products offered, the involvement of intermediaries, and the potential use of insurance products to place, layer or move illicit funds.

Accordingly, insurance companies and intermediaries carrying on activities that fall within the scope of the AML/CFT/CPF legislative framework are required to establish and maintain appropriate policies, procedures and controls to identify, assess, manage and mitigate ML/TF/PF risks associated with their business relationships, products and services.

The sections below outline the circumstances in which insurance companies are considered financial institutions for AML/CFT/CPF purposes and the resulting obligations applicable to them.

Supervisory Principle

The Commission considers the effective identification, assessment and management of ML/TF/PF risks to be fundamental to an insurer's ability to detect and report suspicious transactions. Accordingly, all insurance companies are expected to maintain risk-based AML/CFT/CPF systems and controls that are commensurate with the nature, size and complexity of their business and the risks to which they are exposed.

9.2 Life insurance companies

Life insurance companies are considered financial institutions for AML/CFT/CPF purposes where they carry on long-term insurance business. Long-term insurance business is defined under the Insurance Act, Chapter 347 and includes the classes of insurance business identified under that legislation.

Pursuant to the FTRA, a company carrying on long-term insurance business, as defined under the Insurance Act, Chapter 347, is included within the definition of a financial institution and is therefore subject to the AML/CFT/CPF obligations prescribed under the relevant legislation.

Accordingly, life insurance companies are required to establish and maintain an effective AML/CFT/CPF framework that is appropriate to the nature, size and complexity of their business and the ML/TF/PF risks to which they are exposed. This includes, among other things:

- conducting and documenting ML/TF/PF risk assessments;
- implementing customer due diligence (CDD) and know-your-customer (KYC) measures, including procedures to ensure customer information remains accurate and current;
- maintaining appropriate systems and controls for ongoing monitoring and sanctions screening;
- establishing written AML/CFT/CPF policies, procedures and internal controls;
- identifying, investigating and reporting suspicious transactions;
- maintaining appropriate records; and

- providing ongoing AML/CFT/CPF training to directors, management, employees and relevant intermediaries.

The Commission supervises life insurance companies for compliance with these AML/CFT/CPF obligations through a risk-based supervisory approach, including off-site monitoring, on-site examinations, thematic reviews, regulatory guidance and ongoing engagement with the industry.

9.3 General insurance companies

Although general insurance companies are not included within the definition of a financial institution under section 3 of the Financial Transactions Reporting Act (FTRA), they are required to comply with the suspicious transaction reporting obligations prescribed under sections 25 to 30 of the FTRA.

To effectively discharge these statutory obligations, general insurance companies are expected to establish and maintain an AML/CFT/CPF framework that is commensurate with the nature, size and complexity of their business and the ML/TF/PF risks to which they are exposed. Such a framework should enable the insurer to identify, assess, monitor and report suspicious activity and shall include, at a minimum:

- documented ML/TF/PF risk assessments;
- customer due diligence (CDD) and know-your-customer (KYC) measures, including procedures to ensure customer information remains accurate and up to date;
- systems and controls for sanctions screening and compliance with targeted financial sanctions requirements;
- internal policies, procedures and controls designed to mitigate ML/TF/PF risks;
- ongoing monitoring of customer relationships and transactions, where appropriate;
- procedures for identifying, investigating and reporting suspicious transactions; and
- ongoing AML/CFT/CPF training for directors, management, employees and relevant intermediaries.

The Commission expects general insurance companies to adopt these measures as fundamental components of sound governance and effective risk management. These controls support the timely identification, assessment and reporting of suspicious activity and assist insurers in fulfilling their statutory reporting obligations.

9.4 Responsibilities relating to intermediaries

Insurance companies remain responsible for managing the ML/TF/PF risks arising from the distribution of their products through intermediaries. Accordingly, insurers shall ensure that intermediaries acting on their behalf understand the ML/TF/PF risks associated with the insurer's business, products, services and customers and are provided with appropriate guidance to enable them to identify and escalate suspicious activity.

Insurance companies shall also ensure that intermediaries receive adequate AML/CFT/CPF training on a regular basis, including training that is appropriate to the nature of the intermediary's role and responsibilities.

Intermediaries likewise have independent responsibilities to establish and maintain effective AML/CFT/CPF risk management measures. These should include conducting and documenting ML/TF/PF risk assessments, implementing written AML/CFT/CPF policies, procedures and controls appropriate to their business, maintaining effective customer due diligence measures and participating in ongoing AML/CFT/CPF training to ensure that their knowledge remains current and effective.

IV. SUPERVISORY FRAMEWORK OF THE COMMISSION

10. The Commission

10.1 Establishment and Supervisory Mandate

10.1.1 Section 4 of the Insurance Act, Chapter 347 establishes the Insurance Commission of The Bahamas ("the Commission") as a body corporate responsible for administering and enforcing the Insurance Act, Chapter 347 and the External Insurance Act, Chapter 348. The Commission comprises the Superintendent, Deputy Superintendent and three to five Commissioners appointed by the Governor-General.

In addition to its responsibilities under the insurance legislation, section 8 of the Insurance Act empowers the Commission to supervise life insurance companies for compliance with the AML/CFT/CPF legislative framework and to take such measures as are necessary to ensure compliance with those requirements.

10.2 AML/CFT/CPF Supervisory Framework

The Commission adopts a risk-based approach to AML/CFT/CPF supervision and employs a combination of supervisory tools to assess and promote compliance with the applicable legislative and regulatory requirements. These include:

- off-site supervisory reviews;
- on-site inspections;
- thematic and targeted examinations;
- the issuance of guidelines, notices and other supervisory communications;
- industry outreach, education and awareness initiatives; and
- ongoing engagement with regulated entities and industry representative bodies.

The Commission also maintains a structured programme of engagement with the insurance industry through periodic meetings, consultations and other forums. These engagements provide an opportunity to discuss emerging risks, regulatory developments, supervisory expectations and matters affecting AML/CFT/CPF compliance within the insurance sector.

11. AML/CFT/CPF EXAMINATION FRAMEWORK

11.1 Purpose and Scope of AML/CFT/CPF Examinations

The Commission conducts AML/CFT/CPF examinations as an integral component of its risk-based supervisory framework for registrants and licensees. The purpose of an examination is to assess whether a registrant or licensee has established and effectively implemented an AML/CFT/CPF framework that enables it to comply with the applicable AML/CFT/CPF legislative and regulatory requirements and effectively identify, assess, manage and mitigate its money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks.

11.1-1 The examination process enables the Commission to assess the effectiveness of a registrant's or licensee's AML/CFT/CPF framework, evaluate its understanding and management of ML/TF/PF risks, identify deficiencies or areas requiring improvement, and determine whether further supervisory action is necessary.

11.1-2 In conducting AML/CFT/CPF examinations, the Commission assesses compliance with the applicable statutory and regulatory framework, including the AML/CFT/CPF legislation, regulations, regulatory instruments, the Commission's AML/CFT/CPF Guidelines and any other applicable guidance issued by the Commission.

11.1-3 The Commission's AML/CFT/CPF Guidelines establish the regulatory requirements and supervisory expectations applicable to registrants and licensees and provide the framework against which compliance with AML/CFT/CPF obligations is assessed. Registrants and licensees are expected to ensure that their AML/CFT/CPF policies, procedures, systems and controls are consistent with the requirements and expectations established in these Guidelines and are effectively implemented in practice.

11.1-4 A registrant or licensee's compliance with the AML/CFT/CPF framework is not determined solely by the existence of documented policies and procedures. The Commission will assess whether the AML/CFT/CPF framework is operating effectively and whether the measures implemented are appropriate and proportionate to the nature, size, complexity and ML/TF/PF risk profile of the business.

11.1-5 Failure to comply with the requirements and expectations established in these Guidelines may result in supervisory action or enforcement measures by the Commission.

11.2 Risk-based Supervisory approach

11.2.1 The Commission adopts a risk-based approach to AML/CFT/CPF supervision, which allows supervisory resources to be directed toward areas presenting greater ML/TF/PF risks. The Commission's supervisory approach recognizes that registrants and licensees may present differing levels and types of ML/TF/PF risk depending on factors such as the nature of their products and services, customer base, distribution channels, geographic exposure, business activities and governance arrangements.

11.2.2 The nature, scope, frequency and intensity of an AML/CFT/CPF examination will be determined having regard to the registrant's or licensee's risk profile, compliance history, previous supervisory findings, changes in business activities and other relevant supervisory considerations.

11.2.3 The Commission conducts AML/CFT/CPF supervision through a combination of on-site examinations, off-site examinations, AML/CFT/CPF risk assessments and other supervisory activities. These activities enable the Commission to evaluate compliance, assess the effectiveness of AML/CFT/CPF frameworks, identify emerging risks and determine whether additional supervisory measures are required.

11.3 Application of the AML/CFT/CPF Examination Framework

11.3.1 The Commission applies a consistent risk-based examination framework when assessing compliance with AML/CFT/CPF requirements across the insurance sector. Unless otherwise specified, the examination principles and assessment considerations outlined in these Guidelines apply to all registrants and licensees subject to AML/CFT/CPF supervision by the Commission, including life insurance companies, external insurers, general insurance companies and insurance intermediaries.

11.3.2 While the scope and frequency of an examination may vary depending on the nature, size, complexity and risk profile of the registrant or licensee, all registrants and licensees are expected to maintain AML/CFT/CPF policies, procedures, systems and controls that are appropriate to the ML/TF/PF risks associated with their business.

11.3.3 The Commission will assess whether the registrant or licensee has implemented effective measures to comply with its AML/CFT/CPF obligations, including measures relating to:

- governance and oversight of AML/CFT/CPF compliance;
- identification, assessment and understanding of ML/TF/PF risks;
- customer due diligence and know-your-customer requirements;
- beneficial ownership identification and verification;
- enhanced due diligence measures;
- ongoing monitoring of customer relationships and transactions;

- targeted financial sanctions compliance;
- suspicious transaction identification, escalation and reporting;
- record keeping;
- employee screening and training; and
- oversight of intermediaries and other relevant third parties.

The assessment of compliance will take into consideration the extent to which the registrant or licensee has implemented measures that are effective, risk-based and appropriate to its business model.

11.4 Types of AML/CFT/CPF Examinations

11.4.1 As part of its AML/CFT/CPF supervisory programme, the Commission conducts the following types of examinations:

- **Routine examinations**, which may be conducted either on-site or off-site;
- **Follow-up examinations**, conducted to assess whether deficiencies identified during previous examinations or supervisory reviews have been appropriately addressed;
- **Random examinations**, which are conducted on-site; and
- **Special examinations**, which are conducted on-site where circumstances warrant.

11.4.2 The type of examination conducted by the Commission will depend on the purpose of the review, the supervisory circumstances and the Commission's assessment of the registrant's or licensee's AML/CFT/CPF risk profile, compliance history and other relevant factors.

11.4.3 A registrant or licensee may also be subject to an AML/CFT/CPF Risk Assessment conducted by the Commission. Such assessments form part of the Commission's risk-based supervisory framework and are designed to evaluate the ML/TF/PF risks present within the registrant's or licensee's business and the effectiveness of the measures implemented to manage those risks.

11.4.4 Further details regarding the specific types of examinations are provided in the sections below.

11.5 Routine Examinations

11.5.1 Purpose of Routine Examinations

11.5.1-1 A routine examination is the Commission's annual AML/CFT/CPF supervisory assessment of a registrant's or licensee's compliance with the applicable AML/CFT/CPF legislative and regulatory framework.

11.5.1-2 The purpose of a routine examination is to assess whether the registrant or licensee has established and effectively implemented an AML/CFT/CPF framework that is appropriate to the nature, size, complexity and ML/TF/PF risks associated with its business.

11.5.1-3 A routine examination enables the Commission to evaluate the effectiveness of the registrant's or licensee's AML/CFT/CPF governance arrangements, risk assessment processes, policies, procedures, systems and controls implemented to identify, assess, manage and mitigate ML/TF/PF risks.

11.5.1-4 A routine examination also provides the Commission with information to determine whether further supervisory engagement, corrective action or other supervisory measures may be required.

11.5.2 Frequency of Examinations

11.5.2-1 The Commission conducts routine examinations on an annual basis as part of its AML/CFT/CPF

supervisory programme.

- 11.5.2-2 Unless otherwise approved by the Commission, the routine examination covers the registrant's or licensee's AML/CFT/CPF framework and activities for the annual reporting period January 1 to December 31 of the relevant examination year.
- 11.5.2-3 The routine examination may be conducted either on-site or off-site, as determined by the Commission, or where applicable, following the granting of a waiver under section 11.6 of these Guidelines.
- 11.5.2-4 The completed examination and supporting documentation must be submitted to the Commission **within four (4) months following the end of the registrant's or licensee's financial year** or within such other period as the Commission may specify.

11.5.3 Scope of Routine Examination

- 11.5.3-1 A routine examination assesses the effectiveness of the registrant's or licensee's AML/CFT/CPF framework and compliance with applicable AML/CFT/CPF requirements.
- 11.5.3-2 The Commission may assess, among other things:
- the registrant's or licensee's understanding and assessment of its ML/TF/PF risks;
 - governance arrangements and oversight responsibilities for AML/CFT/CPF compliance;
 - the appointment, authority and effectiveness of the Compliance Officer and Money Laundering Reporting Officer (MLRO), where applicable;
 - AML/CFT/CPF policies, procedures and internal controls;
 - customer due diligence (CDD) and know-your-customer (KYC) processes;
 - customer identification and verification measures;
 - beneficial ownership identification and verification;
 - enhanced due diligence measures;
 - ongoing monitoring of customer relationships and transactions;
 - targeted financial sanctions screening and compliance measures;
 - suspicious transaction identification, escalation and reporting arrangements;
 - record-keeping requirements;
 - employee screening and AML/CFT/CPF training;
 - independent testing, audit or review arrangements; and
 - oversight of insurance intermediaries and other relevant third parties.

The scope of the examination will be proportionate to the nature, size, complexity and ML/TF/PF risk profile of the registrant or licensee.

11.5.4 Routine On-Site Examinations

- 11.5.4-1 A routine examination may be conducted on-site where the Commission, or an external auditor acting on behalf of the Commission, conducts an assessment at the premises of the registrant or licensee.
- 11.5.4-2 Pursuant to section 69 of the Insurance Act, Chapter 347, the Commission has the authority to conduct on-site examinations of insurance companies and intermediaries.
- 11.5.4-3 An AML/CFT/CPF on-site examination is a supervisory assessment of the effectiveness of the registrant's or licensee's AML/CFT/CPF framework. It is not a financial audit of the registrant's or licensee's business activities.

- 11.5.4-4 Rather, the examination assesses whether the AML/CFT/CPF policies, procedures, systems and controls implemented by the registrant or licensee are sufficient and effective to identify, assess, manage and mitigate ML/TF/PF risks.
- 11.5.4-5 Where the routine on-site examination is conducted by an external auditor, the completed examination form must be submitted to the Commission by the external auditor within four (4) months following the end of the registrant's or licensee's financial year.
- 11.5.4-6 The external auditor should also provide the registrant or licensee with a copy of the completed examination documentation for its records.
- 11.5.4-7 The Commission will review the completed examination submission and determine whether further supervisory action is necessary.

11.5.5 Routine Off-Site Examinations

- 11.5.5-1 A routine examination may also be conducted on an off-site basis where approved by the Commission.
- 11.5.5-2 An off-site examination is a supervisory assessment conducted through the review and analysis of information, documentation and responses submitted by the registrant or licensee without the need for an on-site visit.
- 11.5.5-3 An off-site examination does not reduce or remove the registrant's or licensee's AML/CFT/CPF obligations. The registrant or licensee remains responsible for ensuring that it maintains an effective AML/CFT/CPF framework and complies with all applicable requirements.
- 11.5.5-4 Where the Commission approves an off-site routine examination, the registrant or licensee must complete the prescribed examination documentation and submit it to the Commission for assessment.
- 11.5.5-5 For life insurance companies and external insurers eligible for this process, the off-site routine examination is conducted following the granting of a waiver from the routine on-site examination requirement.
- 11.5.5-6 The completion and submission requirements applicable to off-site routine examinations are set out in section 11.6.

11.6 Waiver from a Routine On-Site Examination

11.6.1 Purpose of a Waiver

- 11.6.1-1 The Commission may, in appropriate circumstances, grant a waiver from the requirement for a routine on-site examination.
- 11.6.1-225 A waiver permits the routine examination to be conducted through an off-site examination process during the relevant examination period. A waiver does not exempt a registrant or licensee from AML/CFT/CPF supervision, nor does it relieve the registrant or licensee of its obligation to comply with all applicable AML/CFT/CPF legislative and regulatory requirements.
- 11.6.1-3 The granting of a waiver is intended to allow the Commission to apply a proportionate, risk-based supervisory approach while ensuring that the registrant or licensee remains subject to effective AML/CFT/CPF oversight.

11.6.2 Request for a Waiver

- 11.6.2-1 A registrant or licensee seeking to conduct a routine examination on an off-site basis must submit a written request for a waiver to the Commission.
- 11.6.2-2 The request should provide sufficient information to enable the Commission to determine whether the registrant or licensee continues to present an appropriate risk profile for an off-site examination.
- 11.6.2-3 The granting of a waiver remains at the sole discretion of the Commission and will be determined on a case-by-case basis having regard to the registrant's or licensee's ML/TF/PF risk profile, compliance history, previous examination results and other relevant supervisory considerations.

11.6.3 Eligibility for a Waiver

- 11.6.3-1 In determining whether to grant a waiver, the Commission will consider whether the registrant or licensee has demonstrated an effective AML/CFT/CPF framework and satisfactory compliance with applicable requirements.
- 11.6.3-2 A waiver may be granted where the Commission is satisfied that the registrant or licensee:
- has previously undergone at least one (1) routine on-site examination;
 - has demonstrated compliance with applicable AML/CFT/CPF legislation, regulations and the Commission's AML/CFT/CPF Guidelines;
 - has established and maintained effective AML/CFT/CPF policies, procedures, systems and controls appropriate to its ML/TF/PF risk profile;
 - has adequately addressed any deficiencies or weaknesses identified during previous examinations or supervisory reviews;
 - has demonstrated effective processes for customer identification, verification, record keeping, suspicious transaction reporting, sanctions screening and other applicable AML/CFT/CPF obligations; and
 - has not introduced material changes to its business activities, including the addition or expansion of classes of insurance business, products, services or distribution channels that may materially affect its ML/TF/PF risk profile.
- 11.6.3-3 The Commission may consider any other relevant information when determining whether an off-site examination is appropriate.

11.6.4 Conduct of an Off-Site Examination Following a Waiver

- 11.6.4-1 Where a waiver is granted, the registrant or licensee remains responsible for completing the routine examination documentation and submitting the required information to the Commission within the timeframe specified.
- 11.6.4-2 The examination documentation must be completed by the Compliance Officer, Money Laundering Reporting Officer (MLRO), or another Senior Officer approved by the Commission for this purpose.
- 11.6.4-3 The registrant or licensee is responsible for ensuring that all information submitted to the Commission is complete, accurate and supported by appropriate documentation.
- 11.6.4-4 The completed examination documentation must be submitted to the Commission within four (4) months following the end of the financial year.
- 11.6.4-5 The Commission will assess the information submitted in the same manner as information obtained during an on-site routine examination. Where the Commission identifies deficiencies, weaknesses or areas requiring improvement, the findings will be communicated to the registrant or licensee, and the Commission may require appropriate corrective action.

11.6.5 Effect of a Waiver

- 11.6.5-1 A waiver from a routine on-site examination does not exempt a registrant or licensee from AML/CFT/CPF supervision or from complying with the applicable AML/CFT/CPF framework.
- 11.6.5-2 The registrant or licensee remains subject to the Commission's ongoing supervisory oversight and must continue to maintain effective AML/CFT/CPF policies, procedures, systems and controls.
- 11.6.5-3 The granting of a waiver does not prevent the Commission from requiring a subsequent on-site examination where circumstances warrant.
- 11.6.5-4 A registrant or licensee that has been granted a waiver may also be selected for a follow-up examination, random examination or special examination where the Commission determines that such examination is necessary based on supervisory findings, changes in risk profile, compliance concerns or other relevant circumstances.

11.7 Follow-Up Examinations

11.7.1 Purpose of Follow-Up Examinations

- 11.7.1-1 A follow-up examination is conducted to assess whether a registrant or licensee has appropriately addressed deficiencies, weaknesses or areas requiring improvement identified during a previous examination, AML/CFT/CPF Risk Assessment or other supervisory review.
- 11.7.1-2 The purpose of a follow-up examination is to determine whether the corrective measures implemented by the registrant or licensee are sufficient to address the concerns identified by the Commission and whether the registrant or licensee's AML/CFT/CPF framework has been strengthened as a result.
- 11.7.1-3 A follow-up examination does not replace the registrant's or licensee's ongoing responsibility to maintain effective AML/CFT/CPF policies, procedures, systems and controls.

11.7.2 Circumstances Giving Rise to a Follow-Up Examination

- 11.7.2-1 The Commission may require a follow-up examination where:
- significant deficiencies or weaknesses have been identified;
 - a registrant or licensee has failed to adequately address findings within the timeframe specified by the Commission;
 - the corrective actions submitted by the registrant or licensee require further assessment;
 - the Commission determines that additional supervisory review is necessary; or
 - other circumstances indicate that further assessment of the registrant's or licensee's AML/CFT/CPF framework is warranted.
- 11.7.2-2 The scope and timing of a follow-up examination will be determined by the Commission having regard to the nature and severity of the deficiencies identified and the registrant's or licensee's overall ML/TF/PF risk profile.

11.7.3 Conduct of Follow-Up Examinations

- 11.7.3-1 Where a follow-up examination is required, the Commission will notify the registrant or licensee of the matters to be reviewed and the purpose of the examination.
- 11.7.3-2 The Commission may require the registrant or licensee to provide evidence demonstrating that deficiencies identified during a previous examination, AML/CFT/CPF Risk Assessment or other supervisory review have been effectively addressed.

- 11.7.3-3 The Commission may verify the implementation of corrective measures through an on-site examination, review of documentation, meetings with management or any other supervisory activity considered appropriate.
- 11.7.3-4 Where the Commission is satisfied that the identified deficiencies have been adequately remediated, no further supervisory action may be required in relation to those matters.
- 11.7.3-5 Where deficiencies have not been adequately addressed within the timeframe specified by the Commission, or where additional deficiencies are identified, the Commission may require further corrective action or take such supervisory or enforcement measures as it considers appropriate under the applicable legislation.

11.8 Random Examinations

11.8.1 Purpose of Random Examinations

- 11.8.1-1 A random examination is an on-site examination conducted by the Commission as part of its risk-based supervisory programme.
- 11.8.1-2 Random examinations provide the Commission with an additional mechanism to assess compliance across the insurance sector and to confirm that registrants and licensees continue to maintain effective AML/CFT/CPF frameworks.
- 11.8.1-3 A registrant or licensee may be selected for a random examination regardless of whether it has recently undergone another type of examination or has been granted a waiver from a routine on-site examination.

11.8.2 Scope of Random Examinations

- 11.8.2-1 The scope of a random examination will be determined by the Commission having regard to relevant supervisory considerations, including the registrant's or licensee's ML/TF/PF risk profile, previous examination results, changes in business activities or other information available to the Commission.
- 11.8.2-2 A random examination may assess compliance with any applicable AML/CFT/CPF requirements, including the effectiveness of the registrant's or licensee's governance arrangements, policies, procedures, systems and controls.

11.9 Special Examinations

11.9.1 Purpose of Special Examinations

- 11.9.1-1 A special examination is an on-site examination conducted by the Commission where circumstances warrant additional supervisory review.
- 11.9.1.2 A special examination may be undertaken where the Commission identifies concerns regarding a registrant's or licensee's AML/CFT/CPF framework, compliance with applicable requirements or management of ML/TF/PF risks.

11.9.2 Circumstances Giving Rise to a Special Examination

- 11.9.2-1 The Commission may conduct a special examination where, among other things:
- information received by the Commission indicates potential weaknesses in AML/CFT/CPF compliance;
 - there are concerns regarding the effectiveness of the registrant's or licensee's AML/CFT/CPF systems and controls;
 - significant changes have occurred in the registrant's or licensee's business activities,

ownership, governance structure, products, services or distribution channels;

- deficiencies identified through examinations, risk assessments or other supervisory activities require further review; or
- the Commission considers that additional supervisory action is necessary to protect the integrity of the insurance sector.

11.9.2.-2 The scope of a special examination will be determined by the Commission based on the circumstances giving rise to the examination.

11.10 AML/CFT/CPF Risk Assessments

11.10.1 Purpose of AML/CFT/CPF Risk Assessments

11.10.1-1 As part of its risk-based supervisory framework, the Commission conducts AML/CFT/CPF Risk Assessments to evaluate the ML/TF/PF risks associated with registrants and licensees and assess the effectiveness of measures implemented to manage those risks.

11.10.1-2 The purpose of the AML/CFT/CPF Risk Assessment is to assist the Commission in understanding sectoral and entity-specific risks, determining supervisory priorities and ensuring that supervisory resources are directed toward areas presenting greater risk.

11.10.1-3 The Commission's AML/CFT/CPF Risk Assessment process considers relevant risk factors, including the nature of products and services offered, customer base, distribution channels, geographic exposure, business activities, governance arrangements and the effectiveness of the registrant's or licensee's AML/CFT/CPF framework.

11.10.2 Assessment Outcomes

11.10.2-1 Following an AML/CFT/CPF Risk Assessment, the Commission may communicate the results and any identified areas requiring improvement to the registrant or licensee.

11.10.2-2 Where deficiencies or weaknesses are identified, the Commission may require the registrant or licensee to develop and implement a remediation plan outlining the corrective measures to be undertaken.

11.10.2-3 The results of an AML/CFT/CPF Risk Assessment may also inform the Commission's supervisory approach, including the frequency, scope and intensity of future supervisory activities.

11.11 Supervisory Findings, Remediation and Enforcement Action

11.11.1 Supervisory Findings

11.11.1-2 The Commission will communicate findings arising from AML/CFT/CPF examinations, AML/CFT/CPF Risk Assessments and other supervisory reviews to the relevant registrant or licensee.

11.11.1-3 Findings may identify deficiencies, weaknesses, areas requiring improvement or other matters requiring corrective action to ensure that the registrant's or licensee's AML/CFT/CPF framework remains effective and appropriate for its ML/TF/PF risk profile.

11.11.1-4 Deficiencies may arise where a registrant or licensee:

- fails to comply with applicable AML/CFT/CPF legislation, regulations or regulatory requirements;
- fails to comply with the requirements or provisions of the Commission's AML/CFT/CPF Guidelines;
- does not adequately identify, assess, manage or mitigate its ML/TF/PF risks; or
- has implemented policies, procedures, systems or controls that are not sufficiently

effective.

11.11.2 Remediation Plans

- 11.11.2-1 Where deficiencies are identified, the Commission may require the registrant or licensee to implement a remediation plan.
- 11.11.2-2 A remediation plan will identify the deficiencies requiring attention, specify the corrective actions required, establish timelines for completion and may require the registrant or licensee to provide evidence demonstrating that corrective measures have been implemented.
- 11.11.2-3 Registrants and licensees are expected to address identified deficiencies within the timeframe specified by the Commission and to ensure that corrective actions are sustainable and effective.

11.11.3 Failure to Remediate

- 11.11.3-1 Failure by a registrant or licensee to adequately address identified deficiencies within the timeframe specified by the Commission may result in further supervisory action.
- 11.11.3-2 Where appropriate, the Commission may take regulatory or enforcement action, including the imposition of administrative penalties, sanctions, fines or other measures available under applicable legislation.
- 11.11.3-3 In determining whether further action is warranted, the Commission may consider the nature, severity and duration of the deficiencies, the registrant's or licensee's cooperation, the effectiveness of corrective actions taken and any previous supervisory findings.
- 11.11.3-4 Where deficiencies are not adequately addressed, the Commission may escalate its supervisory response in accordance with its supervisory framework, including the application of Ladder of Intervention and any other regulatory or enforcement measures available under the applicable legislation.

11.12 Registrant and Licensee Responsibilities During Supervisory Assessments

11.12.1 Cooperation with the Commission

- 11.12.1-1 Registrants and licensees are expected to cooperate fully with the Commission during AML/CFT/CPF examinations, AML/CFT/CPF Risk Assessments and other supervisory activities undertaken by the Commission.
- 11.12.1-2 A registrant or licensee must provide the Commission with timely access to information, documentation, records and other materials necessary for the Commission to assess compliance with applicable AML/CFT/CPF requirements.
- 11.12.1-3 Registrants and licensees are responsible for ensuring that information provided to the Commission is complete, accurate and not misleading. Where requested by the Commission, a registrant or licensee must provide clarification, supporting documentation or additional information necessary to assist the Commission in completing its supervisory assessment.

11.12.2 Maintenance of Effective AML/CFT/CPF Frameworks

- 11.12.2-1 Registrants and licensees remain responsible for ensuring that their AML/CFT/CPF frameworks are maintained on an ongoing basis and remain appropriate to the nature, size, complexity and ML/TF/PF risks associated with their business.
- 11.12.2-2 The responsibility to comply with AML/CFT/CPF obligations is not limited to periods during which

a registrant or licensee is subject to an examination or supervisory review. Registrants and licensees are expected to continuously monitor and assess the effectiveness of their AML/CFT/CPF policies, procedures, systems and controls and make improvements where necessary.

11.12.3 Implementation of Corrective Measures

- 11.12.3-1 Where deficiencies, weaknesses or areas requiring improvement are identified by the Commission, the registrant or licensee is responsible for implementing appropriate corrective measures within the timeframe specified by the Commission.
- 11.12.3-2 A registrant or licensee must ensure that remediation actions address the underlying cause of identified deficiencies and are sufficient to prevent recurrence.
- 11.12.3.3 The implementation of corrective measures does not remove the Commission's ability to conduct further supervisory reviews or take additional action where the Commission determines that deficiencies have not been adequately addressed or that further measures are necessary.

12. INDUSTRY ENGAGEMENT AND SUPERVISORY OUTREACH

- 12.1 The Commission recognises that effective AML/CFT/CPF supervision extends beyond examinations and other supervisory measures. Accordingly, the Commission maintains an ongoing programme of industry engagement and supervisory outreach to promote understanding of AML/CFT/CPF obligations, communicate emerging ML/TF/PF risks, clarify regulatory expectations and support the consistent implementation of effective AML/CFT/CPF frameworks across the insurance sector.
- 12.2 As part of this programme, the Commission may communicate with registrants and licensees through supervisory meetings, industry briefings, forums, training sessions, notices, guidance papers, circulars and other supervisory communications. The Commission may also engage with industry associations, representative bodies and other competent authorities to promote a coordinated approach to AML/CFT/CPF compliance.
- 12.3 The Commission may publish or communicate the results of sectoral or thematic AML/CFT/CPF Risk Assessments, emerging risk trends, typologies and common supervisory findings to assist registrants and licensees in understanding evolving ML/TF/PF risks and strengthening their AML/CFT/CPF frameworks.
- 12.4 Registrants and licensees are expected to have regard to the information, guidance and supervisory communications issued by the Commission and to ensure that their directors, senior management, Compliance Officers, Money Laundering Reporting Officers (MLROs) and relevant employees remain informed of developments affecting their AML/CFT/CPF obligations.
- 12.5 Supervisory outreach and engagement complement, but do not replace, a registrant's or licensee's responsibility to comply with applicable AML/CFT/CPF legislation and to establish, implement and maintain effective AML/CFT/CPF policies, procedures, systems and controls appropriate to its ML/TF/PF risks.

C. ESTABLISHING AN EFFECTIVE AML/CFT/CPF FRAMEWORK

V. INTERNAL AML/CFT/CPF GOVERNANCE, CONTROLS AND PROCEDURES

13. Internal AML/CFT/CPF Framework

13.1 Establishment of an AML/CFT/CPF Framework

- 13.1.1 Registrants and licensees must establish and maintain effective internal AML/CFT/CPF controls and procedures that are appropriate and proportionate to their ML/TF/PF risks, having regard to the nature, size and complexity of their business activities.
- 13.1.2 Internal AML/CFT/CPF controls should enable registrants and licensees to identify, assess, manage and mitigate ML/TF/PF risks and to comply with applicable AML/CFT/CPF legislation, regulations and the requirements of these Guidelines.
- 13.1.3 The effectiveness of an AML/CFT/CPF framework depends on the implementation of appropriate governance arrangements, policies, procedures and controls that are embedded throughout the organization and supported by senior management.
- 13.1.4 Internal AML/CFT/CPF controls and procedures should include, as appropriate:
- (a) an AML/CFT/CPF compliance programme that establishes clear responsibilities for managing AML/CFT/CPF obligations, including the appointment of a Compliance Officer (CO), Money Laundering Reporting Officer (MLRO), or Designated Reporting Officer (DRO) where applicable;
 - (b) appropriate governance arrangements to ensure oversight and accountability by senior management and, where applicable, the Board of Directors;
 - (c) procedures for the identification, assessment and management of ML/TF/PF risks associated with customers, products, services, transactions, delivery channels and geographic exposure;
 - (d) customer due diligence and ongoing monitoring procedures, including procedures to ensure that customer information remains accurate and current;
 - (e) procedures for the identification and verification of beneficial owners, where applicable;
 - (f) procedures for identifying, escalating and reporting suspicious transactions or suspicious activity;
 - (g) procedures for screening customers, beneficial owners and other relevant persons against applicable targeted financial sanctions obligations;
 - (h) appropriate employee screening procedures to ensure that persons performing relevant functions are suitable and appropriate;
 - (i) ongoing AML/CFT/CPF training programmes that are appropriate to employees' roles and responsibilities; and
 - (j) independent testing or review arrangements to assess the effectiveness of AML/CFT/CPF policies, procedures, systems and controls.

13.2 AML/CFT/CPF Risk Assessment and Risk Management

- 13.2.1 Registrants and licensees must establish and maintain a documented risk-based approach to identify, assess, understand, manage and mitigate the ML/TF/PF risks to which they are exposed.
- 13.2.2 The risk assessment process should enable the registrant or licensee to understand the ML/TF/PF risks arising from its customers, products, services, transactions, delivery channels, geographic exposure and other relevant factors.
- 13.2.3 In conducting their risk assessments, registrants and licensees shall have regard to relevant information, including the National Risk Assessment, sectoral risk assessments, supervisory guidance issued by the Commission, applicable money laundering, terrorist financing and proliferation financing typologies, and other information issued by competent authorities.

- 13.2.4 Registrants and licensees shall document their assessment of the ML/TF/PF risks facing their business and ensure that the results of the assessment inform the development and implementation of their AML/CFT/CPF policies, procedures, systems and controls.
- 13.2.5 Where risks are identified, registrants and licensees must implement appropriate measures to manage and mitigate those risks. The nature and extent of mitigating measures should be proportionate to the level and nature of the risks identified.
- 13.2.6 The registrant's or licensee's AML/CFT/CPF business risk assessment shall be documented and approved by the Board of Directors or senior management acting under authority delegated by the Board. The assessment shall be reviewed at least annually and whenever there is a material change in the registrant's or licensee's business, ownership or control, risk profile, products or services, distribution arrangements, geographic exposure, technology, regulatory environment or identified ML/TF/PF risks.
- 13.2.7 A review of the business risk assessment shall also be undertaken before the introduction of a material new product, business practice, delivery mechanism or technology and following any major event or development affecting the management, ownership, structure or operation of a group of which the registrant or licensee forms part.
- 13.2.8 In assessing geographic and cross-border risk, registrants and licensees shall consider whether the jurisdiction, transaction structure or use of foreign intermediaries, reinsurers, insurance managers, counterparties or service providers may reduce effective oversight, limit access to reliable customer or beneficial ownership information, or otherwise impair the application of effective AML/CFT/CPF controls. Appropriate enhanced measures shall be applied where such risks are identified. Where such risks are identified, registrants and licensees shall apply measures in accordance with section 15.

13.3 New Products, Business Practices and Technologies

- 13.3.1 Registrants and licensees are expected to identify and assess the ML/TF/PF risks associated with new or developing products, business practices, delivery mechanisms and technologies before they are introduced or implemented.
- 13.3.2 This assessment shall also apply to material changes to existing products, services or delivery channels where those changes may affect the registrant's or licensee's ML/TF/PF risk profile.
- 13.3.3 Where risks are identified, registrants and licensees shall implement appropriate policies, procedures, systems and controls to effectively manage and mitigate those risks before the product, service, business practice or technology is introduced.
- 13.3.4 Registrants and licensees shall periodically review the effectiveness of those controls to ensure that they remain appropriate as products, technologies, customer behaviour and ML/TF/PF risks evolve.
- 13.3.5 For the purposes of this section, relevant technologies and business practices include, where applicable, digital or remote onboarding, electronic identity verification, automated underwriting, artificial intelligence, application programming interfaces, cloud-based services, RegTech solutions, outsourced technology arrangements and other third-party systems used to perform or support AML/CFT/CPF controls. Risks arising from such arrangements shall be assessed before implementation and subject to ongoing oversight.

13.4 Senior Management Responsibility and Culture of Compliance

- 13.4.1 Senior management plays a critical role in ensuring the effective implementation of an AML/CFT/CPF framework. Senior management should establish and promote a culture of compliance in which AML/CFT/CPF obligations are understood, supported and integrated into the operations of the registrant or licensee.

13.4.2 Senior management is responsible for ensuring that adequate resources, systems, processes and personnel are available to effectively manage ML/TF/PF risks.

13.4.3 A culture of compliance should include:

- (a) active oversight of AML/CFT/CPF risks and compliance matters;
- (b) timely consideration of legislative, regulatory and supervisory developments;
- (c) regular review and updating of AML/CFT/CPF policies, procedures and controls;
- (d) appropriate escalation and resolution of AML/CFT/CPF concerns; and
- (e) ensuring that employees understand their responsibilities in relation to preventing and detecting ML/TF/PF activities.

13.4.4 The Board of Directors shall retain ultimate oversight of the registrant's or licensee's AML/CFT/CPF framework. The Board shall approve the AML/CFT/CPF framework and business risk assessment, ensure that adequate resources are provided, receive periodic reporting on material AML/CFT/CPF risks and compliance matters, and oversee the timely remediation of material deficiencies identified through internal review, audit, examination or supervisory assessment.

Policies, procedures and controls are effective only when they are supported by senior management and implemented throughout the organization.

13.5 Internal AML/CFT/CPF Policies, Procedures and Controls

13.5.1 Registrants and licensees must establish, implement and maintain documented AML/CFT/CPF policies, procedures and internal controls that are appropriate to the nature, size, complexity and ML/TF/PF risk profile of their business. The policies, procedures and controls shall be approved by senior management and reviewed periodically to ensure that they remain effective and appropriate.

13.5.2 The AML/CFT/CPF framework should be designed to enable the registrant or licensee to identify, assess, manage and mitigate ML/TF/PF risks, comply with the applicable AML/CFT/CPF legislative framework and these Guidelines, and support the timely identification, escalation and reporting of suspicious transactions and activities.

13.5.3 The policies, procedures and internal controls should be risk-based and proportionate to the nature and complexity of the registrant's or licensee's operations and should be supported by appropriate governance, oversight and reporting arrangements.

13.5.4 At a minimum, the AML/CFT/CPF framework should address, where applicable:

- a) governance arrangements, including clearly defined roles, responsibilities and reporting lines;
- b) the appointment and responsibilities of the Compliance Officer and the Money Laundering Reporting Officer (MLRO);
- c) enterprise-wide ML/TF/PF risk assessment and risk management procedures;
- d) customer due diligence (CDD), customer identification and verification, including the identification and verification of beneficial ownership;
- e) customer acceptance, customer risk classification and ongoing monitoring procedures;
- f) enhanced due diligence measures for higher-risk customers, products, services or business relationships;
- g) sanctions screening and compliance with targeted financial sanctions obligations;
- h) procedures for identifying, investigating, escalating and reporting suspicious transactions and suspicious activities;
- i) record-keeping and document retention requirements;
- j) procedures governing the use of intermediaries, outsourcing arrangements and reliance on third parties, where applicable;

- k) employee screening, integrity and fit and proper considerations;
- l) an ongoing AML/CFT/CPF training and awareness programme that is proportionate to the nature, size, complexity and ML/TF/PF risk profile of the registrant's or licensee's business, and which ensures that directors, senior management, employees and relevant intermediaries understand their AML/CFT/CPF obligations, the risks associated with the business activities they perform, and their respective responsibilities under the registrant's or licensee's AML/CFT/CPF framework;
- m) independent testing and periodic review of the effectiveness of the AML/CFT/CPF framework; and
- n) procedures for identifying, documenting and addressing deficiencies identified through internal reviews, audits, examinations or supervisory assessments.

13.5.5 Registrants and licensees should ensure that their AML/CFT/CPF policies and procedures are effectively communicated throughout the organisation and that employees, management and relevant intermediaries understand their respective responsibilities for implementing and complying with those policies and procedures.

13.5.6 The AML/CFT/CPF framework shall be reviewed periodically and updated where necessary to reflect changes in legislation, the Commission's Guidelines, the registrant's or licensee's business activities, products, services, delivery channels, technologies, or identified ML/TF/PF risks.

13.5.7 Registrants and licensees remain responsible for ensuring that their AML/CFT/CPF framework is effectively implemented and operating in practice. The existence of documented policies and procedures alone will not be regarded as sufficient where those policies and procedures are not effectively implemented, understood or consistently applied throughout the organisation.

13.6 Group-Wide AML/CFT/CPF Programmes

13.6.1 Where a registrant or licensee forms part of a group, the registrant or licensee shall implement group-wide AML/CFT/CPF programmes that are appropriate to the structure, activities and ML/TF/PF risks of the group.

13.6.2 Group-wide AML/CFT/CPF programmes should, where applicable, include:

- (a) policies and procedures that facilitate the sharing of information necessary for customer due diligence, risk management and compliance purposes;
- (b) arrangements that permit appropriate oversight by group-level compliance, audit or other relevant functions, including access to customer, account and transaction information where necessary for AML/CFT/CPF purposes;
- (c) procedures for communicating relevant risk information, unusual activity indicators and compliance concerns between group entities where appropriate; and
- (d) adequate safeguards to protect the confidentiality and proper use of information exchanged, including measures to prevent tipping-off.

13.7 Foreign Branches and Subsidiaries

13.7.1 Registrants and licensees that operate through foreign branches or subsidiaries should ensure that effective AML/CFT/CPF policies, procedures and controls are implemented consistently throughout their operations and are appropriate to the ML/TF/PF risks associated with the jurisdictions in which they operate.

13.7.2 Where customer identification or verification documents originate from a foreign jurisdiction, registrants and licensees are expected to take appropriate measures to satisfy themselves that

such documents are authentic, reliable and suitable for AML/CFT/CPF purposes, having regard to the ML/TF/PF risks associated with the customer and the jurisdiction concerned.

Where documents are not in English, certified translations or other reliable translations should be obtained where necessary to facilitate their proper review, verification and assessment.

- 13.7.3 Registrants and licensees should ensure that customer information obtained from foreign jurisdictions is subject to the same standards of customer due diligence, ongoing monitoring and periodic review as customer information obtained within The Bahamas.
- 13.7.4 Where the AML/CFT/CPF requirements of The Bahamas are more stringent than those of the host jurisdiction, registrants and licensees should ensure that their foreign branches and subsidiaries apply the higher AML/CFT/CPF standard, to the extent permitted by the laws of the host jurisdiction.
- 13.7.5 Where a foreign branch or subsidiary is unable to implement AML/CFT/CPF measures that are consistent with the requirements of the AML/CFT/CPF legislative framework or these Guidelines² because of legal or regulatory restrictions in the host jurisdiction, the registrant or licensee shall implement appropriate additional measures to effectively identify, assess, manage and mitigate the resulting ML/TF/PF risks.
- 13.7.6 Where appropriate additional measures are insufficient to effectively manage the identified ML/TF/PF risks, the registrant or licensee shall notify the Commission and, where applicable, its home supervisor or other relevant competent authority, and consider whether additional supervisory, operational or business measures are necessary to address those risks.

13.8 Independent Testing and Review

- 13.8.1 Registrants and licensees shall conduct periodic independent testing or reviews of their AML/CFT/CPF policies, procedures, systems and controls to assess their effectiveness and identify areas requiring improvement.
- 13.8.2 The nature, scope and frequency of independent testing should be proportionate to the registrant's or ML/TF/PF risk profile, size, complexity and nature of business activities.
- 13.8.3 Independent testing may be performed by an internal audit function, where available, or by suitably qualified persons who are independent of the AML/CFT/CPF functions being reviewed.
- 13.8.4 The results of independent testing or reviews should be documented, reported to appropriate levels of management, and corrective action should be taken to address identified deficiencies within an appropriate timeframe.
- 13.8.5 Registrants and licensees should maintain records of such reviews and make them available to the Commission or its appointed representatives upon request.

VI. CUSTOMER DUE DILIGENCE (CDD) AND KNOW YOUR CUSTOMER (KYC) REQUIREMENTS

14. CUSTOMER IDENTIFICATION, VERIFICATION AND DUE DILIGENCE REQUIREMENTS

14.1 Purpose of Customer Due Diligence

- 14.1.1 Customer Due Diligence ("CDD"), also referred to as Know Your Customer ("KYC"), is a fundamental component of an effective AML/CFT/CPF framework. CDD enables registrants and licensees to establish and verify the identity of their customers, understand the nature and

² Including the **Guidelines for the Compliance Function, 2026**.

purpose of the business relationship, identify ownership and control structures, assess ML/TF/PF risks and identify activity that may require further investigation or reporting.

- 14.1.2 An effective CDD framework supports the ability of registrants and licensees to comply with their AML/CFT/CPF obligations, including the identification, monitoring and reporting of suspicious transactions.
- 14.1.3 Registrants and licensees must implement CDD measures that are proportionate to the nature, size and complexity of their business, and the ML/TF/PF risks identified through their risk assessment process.
- 14.1.4 CDD must form part of the registrant's or licensee's broader AML/CFT/CPF framework, including its risk assessment, policies, procedures, internal controls and ongoing monitoring processes.
- 14.1.5 For the purposes of these Guidelines, references to customers and customer relationships should be interpreted broadly to include facility holders and other relevant persons associated with an insurance relationship. The term "facility" is used where reference is made to the terminology contained in the Financial Transactions Reporting Act and related legislation, and includes insurance policies, annuities and other arrangements that fall within the statutory definition of a facility.

14.2 Application of CDD Requirements Across the Insurance Sector

- 14.2.1 Life insurance companies and other financial institutions are subject to customer due diligence obligations under the Financial Transactions Reporting Act, 2018 ("FTRA") as amended, and the Financial Transactions Reporting Regulations, 2018 ("FTRR") as amended.
- 14.2.2 While general insurance companies are not defined as financial institutions under the FTRA, this does not exempt them from understanding their customers, assessing ML/TF/PF risks or maintaining appropriate measures to identify and report suspicious transactions.
- 14.2.3 General insurance companies and intermediaries must obtain sufficient information regarding policyholders, customers and relevant parties to enable them to:
- understand the nature and purpose of the insurance relationship;
 - assess customer and policyholder risk;
 - identify unusual or suspicious activity;
 - comply with applicable AML/CFT/CPF obligations, including suspicious transaction reporting requirements.
- 14.2.4 The Commission expects all registrants and licensees to apply a risk-based approach to customer information gathering and due diligence measures that is appropriate to the nature of the insurance business conducted.
- 14.2.5 Where a registrant or licensee conducts different classes of insurance business, the level of CDD applied should reflect the risks associated with each class of business, product, service and customer relationship.

14.3 Exemptions and Exceptions to Customer Due Diligence Requirements

- 14.3.1 The obligation to conduct customer due diligence applies to all registrants and licensees. However, applicable legislation may permit exemptions or exceptions from certain customer identification and verification requirements in specified circumstances.
- 14.3.2 Where a registrant or licensee applies an exemption or exception permitted under applicable legislation, it shall:
- confirm that the circumstances satisfy the relevant legislative requirements;
 - obtain sufficient information to establish the basis for applying the exemption or

exception;

- maintain appropriate documentation supporting the decision; and
- continue to apply appropriate risk-based measures to manage any ML/TF/PF risks associated with the relationship.

14.3.3 Examples of circumstances where exemptions or exceptions may apply include certain relationships involving:

- government entities or statutory bodies;
- regulated financial institutions subject to AML/CFT/CPF obligations and supervision;
- publicly traded companies meeting applicable requirements; and
- other persons or entities specified under applicable legislation.

14.3.4 Registrants and licensees shall not apply exemptions or exceptions where there are circumstances indicating increased ML/TF/PF risk or where the basis for applying the exemption cannot be satisfactorily established.

14.3.5 Publicly Traded Companies

14.3.5-1 Where permitted under applicable legislation, registrants and licensees may apply simplified identification and verification measures in relation to publicly traded companies that are subject to adequate regulatory oversight and transparency requirements.

14.3.5-2 In determining whether simplified measures are appropriate, registrants and licensees should consider factors including the regulatory framework applicable to the securities exchange, the jurisdiction in which the company is established, the transparency of ownership and control information, and the availability of reliable information concerning the company.

14.3.5-3 A registrant or licensee shall not apply simplified measures solely because an entity is publicly traded where other factors indicate an increased ML/TF/PF risk.

14.4 Customer Identification and Verification

14.4.1 Registrants and licensees shall obtain sufficient information to identify each customer and verify the customer's identity using reliable and independent source documents, data or information.

14.4.2 Customer identification and verification procedures shall be undertaken:

- when establishing a business relationship;
- when carrying out occasional transactions, where applicable;
- when there is doubt regarding previously obtained identification information;
- when there are changes to customer circumstances that may affect the risk profile; or
- where the registrant or licensee otherwise determines that updated information is necessary.

14.4.3 The identification and verification process shall enable the registrant or licensee to establish, as appropriate:

- the identity of the customer;
- the identity of persons acting on behalf of the customer;
- the ownership and control structure of legal persons or legal arrangements;
- the identity of beneficial owners; and
- the purpose and intended nature of the business relationship.

14.4.4 A registrant or licensee shall not establish or continue a business relationship where it is unable to obtain sufficient information to identify the customer, understand the ownership and control structure, or adequately manage the associated ML/TF/PF risks.

14.4.5 At the commencement of a business relationship, registrants and licensees shall obtain sufficient information to establish the expected nature and pattern of the customer's insurance-related

activity, including, where relevant, the anticipated level and frequency of premium payments and the expected use of policy features, transactions or other insurance-related activity, such as claims, surrenders, refunds, policy loans, settlements, transfers and other material movements of funds.

The information obtained shall form part of the customer's expected activity profile and provide a baseline against which subsequent activity may be assessed for consistency with the customer's known circumstances, risk profile and the purpose and intended nature of the business relationship.

14.5 Identification and Verification of Legal Persons and Legal Arrangements

14.5.1 Where the customer is a legal person or legal arrangement, registrants and licensees should obtain sufficient information to understand the nature of the entity and its ownership and control structure.

The information obtained should include where applicable:

- legal name;
- registration details;
- registered office or principal place of business;
- nature of business activities;
- ownership structure;
- controlling persons;
- authorised representatives;
- beneficial owners.

14.5.2 Registrants and licensees shall take reasonable measures to identify and verify the natural persons who ultimately own or control the customer.

14.5.3 Where the ownership or control structure is complex, unusual or prevents the identification of the beneficial owner, the registrant or licensee shall consider the relationship to present a higher ML/TF/PF risk and apply appropriate enhanced measures.

14.6 Beneficial Ownership and Control

14.6.1 Beneficial ownership refers to the natural person(s) who ultimately owns or controls a customer or on whose behalf a transaction or activity is conducted.

14.6.2 Registrants and licensees shall take reasonable measures to identify and verify beneficial owners and should not rely solely on information relating to legal ownership.

14.6.3 Where beneficial ownership cannot be satisfactorily established, the registrant or licensee shall document the steps taken, assess the associated risks and determine whether the relationship may be established, continued or require enhanced measures.

14.6.4 For the purposes of these Guidelines, ultimate effective control includes control, influence or decision-making power exercised directly or indirectly through a chain of ownership, voting rights, contractual rights, agreements, economic interests or other arrangements that enable a natural person to determine or substantially influence the actions or business activities of a legal person or legal arrangement.

14.6.5 Where no natural person can be identified as the beneficial owner through ownership interests, the registrant or licensee shall identify and take reasonable measures to verify the natural person, if any, exercising control through other means. Where no such natural person can be identified after reasonable measures have been taken, the registrant or licensee shall identify and verify the relevant senior managing official and document the measures undertaken and the basis for its conclusion.

Particular attention should be given to:

- complex ownership structures;
- nominee arrangements;
- trusts and other legal arrangements;
- customers with ownership structures involving multiple jurisdictions; and
- customers where ownership information is inconsistent, unavailable or difficult to verify.

14.7 Customer Due Diligence for Beneficiaries of Life Insurance and Investment-Related Insurance Policies

- 14.7.1 In addition to conducting CDD measures on the policyholder and beneficial owner, life insurance companies shall conduct appropriate due diligence measures in relation to beneficiaries of life insurance policies and other investment-related insurance products.
- 14.7.2 The beneficiary of a life insurance policy or investment-related insurance policy shall be considered a relevant risk factor in determining the ML/TF/PF risk associated with the policy and the overall business relationship.
- 14.7.3 Where a beneficiary is identified or designated, the insurance company shall obtain sufficient information concerning the beneficiary to enable identification and verification at the appropriate stage.
- 14.7.4 Where the beneficiary is:
- (a) a specifically named natural person, legal person or legal arrangement, the insurance company shall obtain the name of the beneficiary; or
 - (b) designated by characteristics, class or other means, the insurance company shall 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 payout.
- 14.7.5 Verification of the identity of the beneficiary shall be completed at or before the time the beneficiary becomes entitled to receive policy proceeds or exercises vested rights under the policy, and in all cases prior to the payment of policy proceeds.
- 14.7.6 Where a beneficiary is identified as presenting a higher ML/TF/PF risk, the insurance company shall apply enhanced due diligence measures. Where the beneficiary is a legal person or legal arrangement, enhanced measures should include reasonable measures to identify and verify the beneficial owner of the beneficiary. Before making a payout under a higher-risk life insurance or investment-related policy, the insurer should ensure that the identity of the beneficiary and, where applicable, the beneficial owner of the beneficiary have been established and verified to the extent required by the risk.
- 14.7.7 Where higher risks are identified, the insurance company shall:
- obtain appropriate senior management approval before payment of policy proceeds;
 - conduct enhanced due diligence on the policyholder and the beneficiary, where appropriate;
 - consider whether the circumstances give rise to a suspicion requiring submission of a suspicious transaction report; and
 - apply enhanced monitoring to the relationship.

14.8 POLITICALLY EXPOSED PERSONS

- 14.8.1 Politically Exposed Persons (“PEPs”) are individuals who are or have been entrusted with prominent public functions, whether domestically or in a foreign jurisdiction.

14.8.2 PEPs present higher risks due to the possibility that their position or influence may be abused for personal gain or to facilitate money laundering, terrorist financing or proliferation financing activities.

14.8.3 Registrants and licensees shall implement appropriate risk management systems to determine whether a customer, beneficial owner, beneficiary or person acting on behalf of a customer is a PEP.

PEPs include:

14.8.4 Foreign PEPs

14.8.4.1 Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, including:

- Heads of State or Government;
- senior politicians;
- senior government officials;
- judicial or military officials;
- senior executives of state-owned corporations; and
- important political party officials.

14.8.5 Domestic PEPs

14.8.5.1 Domestic PEPs are individuals who are or have been entrusted with prominent public functions within The Bahamas, including persons holding positions equivalent to those identified above.

14.8.6 International Organisation PEPs

14.8.6.1 International organisation PEPs are persons who are or have been entrusted with prominent functions by an international organisation, including:

- members of senior management;
- directors;
- deputy directors;
- board members; or
- persons performing equivalent functions.

14.8.7 Family Members and Close Associates

14.8.7.1 The requirements applicable to PEPs also extend to:

- immediate family members;
- persons related through marriage or similar forms of partnership; and
- close associates.

14.8.7.2 A close associate includes persons who are publicly known to maintain a close relationship with a PEP or who are in a position to conduct substantial financial transactions on behalf of a PEP.

14.8.8 PEP-Connected Legal Persons and Legal Arrangements

14.8.8.1 Where a customer is a legal person or legal arrangement, registrants and licensees shall take reasonable measures to determine whether a beneficial owner, controlling person, director, officer, founder, partner, trustee, settlor, protector, authorised signatory or other person exercising

effective control is a PEP, family member or close associate of a PEP.

- 14.8.8.2 Where a PEP relationship is identified and presents higher ML/TF/PF risk, registrants and licensees shall obtain appropriate senior management approval, take reasonable measures to establish and, where warranted by risk, verify source of wealth and source of funds, and apply enhanced ongoing monitoring proportionate to the risk.

14.9 Enhanced Due Diligence Measures for PEPs

- 14.9.1 In addition to standard CDD measures, registrants and licensees shall apply enhanced measures where a customer, beneficial owner or beneficiary is identified as a PEP or presents a higher level of ML/TF/PF risk.

- 14.9.2 Enhanced measures shall include, where applicable:

- (a) obtaining senior management approval before establishing a business relationship or continuing an existing business relationship;
- (b) taking reasonable measures to establish the source of wealth and source of funds;
- (c) conducting enhanced ongoing monitoring of the relationship; and
- (d) documenting the basis for the risk assessment and measures applied.

- 14.10.3 A person who is no longer entrusted with a prominent public function should not automatically be removed from consideration as a PEP. Registrants and licensees should assess the continuing risk posed by the individual based on relevant factors, including:

- the seniority of the position previously held;
- the level of influence the individual may continue to exercise;
- the connection between the former public function and current activities; and
- the overall risk profile of the relationship.

14.10 Ongoing Due Diligence and Updating Customer Information

- 14.10.1 CDD is an ongoing process and shall continue throughout the business relationship.

- 14.10.2 Registrants and licensees shall undertake ongoing monitoring to ensure that transactions, activities and customer information remain consistent with the registrant's or licensee's understanding of:

- the customer;
- the customer's business activities;
- the source of funds;
- the expected nature of transactions; and
- the identified ML/TF/PF risk.

- 14.10.3 Registrants and Licensees shall ensure that ongoing monitoring and periodic reviews are conducted on a risk-sensitive basis, with higher-risk customers, products and business relationships being subject to more frequent review and enhanced scrutiny. Customer information should be reviewed and updated periodically and whenever there is a material change in circumstances, including:

- changes in ownership or control;
- changes in beneficiaries;

- changes in business activities;
- unusual transactions or claims activity;
- changes in geographic exposure; or
- information indicating increased ML/TF/PF risk.

14.10.4 For renewing customers, registrants and licensees should confirm that previously obtained CDD information remains accurate, updated and relevant.

14.10.5 Where changes are identified, appropriate due diligence should be undertaken and the customer's risk profile reassessed.

14.11 Risk-Based Customer Assessment

14.11.1 Registrants and licensees shall adopt a risk-based approach when assessing customer relationships, including the characteristics, products, services, delivery channels and geographic exposure.

14.11.2 Customer risk assessments should consider factors including:

- the identity and background of the customer;
- occupation or business activity;
- geographic connections including countries of residence, nationality, incorporation, principal business activities, source or destination of funds, and other relevant jurisdictional connections;
- ownership and control structure;
- beneficial ownership;
- product or service being provided;
- payment methods;
- transaction activity;
- use of intermediaries or third parties; and
- whether the customer, beneficial owner or beneficiary is a PEP.

14.11.3 Registrants and licensees should also consider relevant information from:

- the current National Risk Assessment;
- the Commission's sector risk assessments;
- published ML/TF/PF typologies;
- sanctions information; and
- other credible sources of risk information.

14.12 Customer Risk Categorisation

14.12.1 Registrants and licensees shall establish procedures to categorise customers and relationships according to their level of ML/TF/PF risk.

14.12.2 Risk categories may include:

- low risk;
- medium risk; and
- high risk.

14.12.3 The risk classification assigned shall determine the level of due diligence and monitoring required.

14.12.4 Where higher risks are identified, registrants and licensees shall apply enhanced measures proportionate to the identified risk.

- 14.12.5 Risk assessments shall be documented, retained and reviewed periodically to ensure that risk ratings remain appropriate.

14.13 General Insurance Companies and Intermediaries

- 14.13.1 General insurance companies and intermediaries shall obtain sufficient information concerning policyholders to enable them to understand customer relationships, assess risk and identify circumstances that may require further review or suspicious transaction reporting.

- 14.13.2 At a minimum, and proportionate to the identified ML/TF/PF risk, general insurers and intermediaries shall obtain information necessary to assess:

- identity of the policyholder;
- address and location;
- nationality, where applicable;
- occupation or business activity;
- ownership and control structure for legal persons;
- beneficial ownership;
- source of funds or source of wealth where risk warrants;
- whether the customer or beneficial owner is a PEP; and
- other information relevant to determining the customer's risk profile.

For legal persons, information should include, where applicable:

- certificate of incorporation or registration;
- business licence;
- ownership information;
- authorised representatives; and
- beneficial owners.

- 14.13.3 General insurers and intermediaries shall apply enhanced due diligence where information obtained indicates that a customer presents a higher ML/TF/PF risk.

14.14 Reliability and Updating of Customer Information and Documentation

- 14.14.1 Licensees must maintain sufficient, accurate and reliable customer information to enable effective management of ML/TF/PF risks and must take appropriate action where information is outdated, unreliable or cannot be obtained.

- 14.14.2 Registrants and licensees should ensure that information relied upon for CDD purposes is obtained from reliable and independent sources.

- 14.14.3 Where identification documents are outdated, expired or otherwise no longer reliable for verification purposes, registrants and licensees should assess whether additional information or updated documentation is required based on the circumstances and risk presented.

- 14.14.4 The acceptance of outdated documentation without appropriate justification may impair the effectiveness of the CDD process and should be supported by documented risk-based reasoning.

- 14.14.5 Registrants and licensees shall maintain customer information that is sufficiently current, accurate and reliable to enable effective identification, verification and management of ML/TF/PF risks throughout the business relationship. The frequency and extent of reviews and updates shall be determined on a risk-sensitive basis, taking into account the nature of the customer relationship, the product or service provided and the customer's risk profile.

14.15 Reliance on Customer Due Diligence Performed by Third Parties

- 14.15.1 Where permitted by law, registrants and licensees may rely on a third party to perform certain customer due diligence measures, including the identification and verification of customers, beneficial owners, beneficiaries or other relevant parties.
- 14.15.2 Reliance on a third party does not relieve the registrant or licensee of its responsibility for complying with its AML/CFT/CPF obligations. The registrant or licensee remains ultimately responsible for ensuring that appropriate customer due diligence measures are applied and that sufficient information is obtained to manage its money laundering, terrorist financing and proliferation financing risks.
- 14.15.3 Before relying on a third party, the registrant or licensee shall satisfy itself that the third party is subject to AML/CFT/CPF requirements and supervision, where applicable, and has appropriate systems and controls in place to perform the required customer due diligence measures.
- 14.15.4 The registrant or licensee shall ensure that customer identification and verification information, including information relating to beneficial ownership and control, is made available promptly upon request and that adequate records are maintained to demonstrate compliance with applicable AML/CFT/CPF obligations.
- 14.15.5 A registrant or licensee shall not rely on a third party where such reliance would prevent it from effectively managing its AML/CFT/CPF risks or complying with applicable legislative and regulatory requirements.

14.16 Failure to Complete Customer Due Diligence

- 14.16.1 Where a registrant or licensee is unable to complete the required customer due diligence measures in accordance with these Guidelines, it shall not establish a business relationship, carry out a transaction, or, where a business relationship has already commenced, shall suspend or terminate the relationship, as appropriate, until the required information has been obtained and verified.
- 14.16.2 Where a registrant or licensee is unable to complete the required customer due diligence measures, it shall consider whether the circumstances give rise to a suspicion of money laundering, terrorist financing or proliferation financing requiring the submission of a suspicious transaction report to the Financial Intelligence Unit. The frequency and extent of reviews and updates shall be proportionate to the nature of the relationship, the product or service provided and the customer's ML/TF/PF risk profile.
- 14.16.3 Where a registrant or licensee is unable to obtain updated customer information after taking reasonable steps, it shall assess the risks associated with maintaining the relationship and determine appropriate measures to mitigate those risks. The assessment and resulting actions shall be documented.

14.17 Tipping Off During Customer Due Diligence

- 14.17.1 Where a registrant or licensee forms a suspicion of money laundering, terrorist financing or proliferation financing while conducting customer due diligence or ongoing due diligence, it shall take appropriate measures to avoid tipping off the customer or any other person.
- 14.17.2 Where a registrant or licensee reasonably believes that conducting or completing the customer due diligence process would alert the customer to the existence of a suspicion or a potential suspicious transaction report, it may elect not to pursue the customer due diligence process and shall consider whether a suspicious transaction report shall be submitted in accordance with applicable legislative requirements.
- 14.17.3 Registrants and licensees shall ensure that employees, officers and relevant representatives are aware of tipping-off obligations and receive appropriate training on managing circumstances where suspicion arises during customer due diligence activities.

15. HIGHER-RISK COUNTRIES, JURISDICTIONS AND CROSS-BORDER RELATIONSHIPS

15.1 General Principles

- 15.1.1 Registrants and licensees shall identify, assess and manage ML/TF/PF risks arising from geographic exposure, higher-risk countries and jurisdictions, and cross-border relationships and transactions.
- 15.1.2 Geographic and cross-border risks shall be assessed in conjunction with other relevant risk factors, including customer, product, service, delivery channel, ownership and transaction risks.
- 15.1.3 The nature and extent of measures applied to manage geographic and cross-border risks shall be proportionate to the risks identified.

15.2 Geographic Risk Factors

- 15.2.1 In assessing geographic and cross-border risk, registrants and licensees should consider, where relevant:
 - (a) the country of residence, nationality, incorporation or principal place of business of the customer;
 - (b) the location of beneficial owners, beneficiaries and persons acting on behalf of the customer;
 - (c) the countries in which the customer conducts material business activities;
 - (d) the source and destination of funds;
 - (e) the location of intermediaries, reinsurers, insurance managers, counterparties and other relevant parties;
 - (f) jurisdictions associated with the ownership or control structure of the customer or other relevant parties;
 - (g) the nature, complexity and purpose of cross-border transactions or arrangements; and
 - (h) any other jurisdictional factors that may affect the registrant's or licensee's ability to understand, monitor or manage ML/TF/PF risks.

15.3 Higher-Risk Countries and Jurisdictions

- 15.3.1 A country or jurisdiction may present increased ML/TF/PF risk having regard to relevant information from credible and reliable sources, including:
 - (a) the National Risk Assessment;
 - (b) the Commission's sectoral risk assessments;
 - (c) FATF public statements and other relevant FATF information;
 - (d) information issued by relevant FATF-style regional bodies;
 - (e) information issued by competent authorities, including the IRF Steering Committee;
 - (f) the effectiveness of the jurisdiction's AML/CFT/CPF framework;
 - (g) corruption, financial crime, transparency and beneficial ownership risks;

- (h) the effectiveness of financial crime supervision and enforcement; and
- (i) other credible information indicating increased ML/TF/PF risk.

15.3.2 Where a jurisdiction is identified by the FATF as subject to a Call for Action, or is otherwise identified by the IRF Steering Committee as requiring enhanced measures, registrants and licensees shall apply enhanced due diligence and other appropriate risk mitigation measures proportionate to the risks identified, having regard to any applicable countermeasures or other measures applicable to the jurisdiction specified by the FATF, the IRF Steering Committee or other competent authorities.

15.3.3 Where a jurisdiction is identified by the FATF as subject to Increased Monitoring, registrants and licensees shall take the information into account in assessing the ML/TF/PF risks associated with the jurisdiction and shall determine, on a risk-sensitive basis, whether enhanced due diligence or other risk mitigation measures are warranted.

15.3.4 Where a jurisdiction presents material risks relating to sanctions, corruption, transparency, beneficial ownership, financial crime, supervisory effectiveness or other factors relevant to ML/TF/PF risk, registrants and licensees shall assess the nature and extent of the risks and apply appropriate risk mitigation measures.

15.4 Enhanced Measures for Higher-Risk Geographic Exposure

15.4.1 Registrants and licensees shall apply enhanced measures to business relationships and transactions involving countries or jurisdictions presenting increased ML/TF/PF risk, where such measures are warranted by the nature and extent of the risks identified.

15.4.2 Such measures may include:

- (a) obtaining additional information concerning the customer and relevant parties;
- (b) obtaining additional information concerning the purpose and intended nature of the relationship or transaction;
- (c) obtaining information concerning source of funds and, where appropriate, source of wealth;
- (d) obtaining information concerning the source and destination of funds;
- (e) obtaining additional information concerning jurisdictional connections;
- (f) additional information concerning foreign intermediaries, reinsurers, insurance managers, counterparties or service providers;
- (g) increasing the frequency and intensity of ongoing monitoring;
- (h) increasing the frequency of customer and risk reviews;
- (i) obtaining senior management approval, where appropriate; and
- (j) such other measures as are appropriate to manage the identified risks.

15.4.3 The nature and extent of measures applied, and the basis for their application, shall be documented.

15.5 Cross-Border Relationships and Transactions

15.5.1 Where a business relationship or transaction involves a customer, beneficial owner, beneficiary, intermediary, reinsurer, insurance manager, counterparty, service provider or other relevant

party located outside The Bahamas, registrants and licensees shall obtain sufficient information to understand the nature and purpose of the cross-border relationship or transaction and assess the associated ML/TF/PF risks.

15.5.2 Registrants and licensees should consider whether the cross-border relationship or transaction:

- (a) limits access to reliable customer or beneficial ownership information;
- (b) reduces effective regulatory or supervisory oversight;
- (c) involves complex or opaque structures;
- (d) involves jurisdictions presenting increased ML/TF/PF risks;
- (e) involves foreign intermediaries or other third parties whose roles or responsibilities are unclear;
- (f) involves movement of funds through jurisdictions unrelated to the customer or insurance relationship; or
- (g) otherwise impairs the effective application of AML/CFT/CPF controls.

15.6 Foreign Intermediaries, Reinsurers, Insurance Managers and Other Counterparties

15.6.1 Where a registrant or licensee enters into or maintains an arrangement involving a foreign intermediary, reinsurer, insurance manager, counterparty or other service provider, it shall assess the ML/TF/PF risks arising from the jurisdiction, nature and structure of the arrangement.

15.6.2 The assessment should consider, where relevant:

- (a) the jurisdiction in which the party operates;
- (b) the party's regulatory and supervisory status;
- (c) the nature and purpose of the relationship;
- (d) the availability and reliability of relevant customer and beneficial ownership information;
- (e) the movement and destination of funds;
- (f) the respective AML/CFT/CPF responsibilities of the parties;
- (g) whether the arrangement limits effective oversight; and
- (h) whether additional measures are necessary to manage the identified risks.

15.6.3 Where the risks associated with such an arrangement cannot be adequately managed, the registrant or licensee shall take appropriate measures to mitigate the risks and consider whether the arrangement should be restricted, modified or discontinued.

16. SANCTIONS SCREENING AND TARGETED FINANCIAL SANCTIONS (TFS)

16.1 General Obligations

16.1.1 Registrants and licensees shall establish and maintain policies, procedures and controls to ensure compliance with applicable targeted financial sanctions (TFS) obligations relating to terrorism financing (TF) and proliferation financing (PF).

16.1.2 Registrants and licensees shall implement effective sanctions screening processes to identify and manage the risk of establishing or maintaining business relationships, or processing transactions or payments involving persons or entities subject to applicable sanctions measures.

16.1.3 Sanctions screening controls shall form part of the registrant's or licensee's broader AML/CFT/CPF framework and shall be proportionate to the nature, size, complexity and risk profile of the business.

16.2 Sanctions Screening Requirements

16.2.1 Registrants and licensees shall conduct sanctions screening of relevant persons and entities associated with a business relationship or transaction, including, where applicable:

- prospective and existing customers;
- policyholders;
- beneficial owners;
- beneficiaries;
- persons exercising control or significant influence over a customer;
- directors, officers, trustees, settlors, protectors and other connected parties;
- intermediaries, agents and business partners; and
- other relevant parties associated with the relationship or transaction.

16.3 Sanctions Screening Shall Be Conducted:

- prior to establishing a business relationship;
- prior to processing relevant payments, including premiums, claims payments, refunds, surrenders, loans, settlements or other disbursements, where applicable;
- periodically during the course of an ongoing business relationship, at intervals commensurate with the registrant's or licensee's risk assessment; and
- upon updates to applicable sanctions lists or where there are material changes to customer, ownership or control information.

16.3.2 Registrants and licensees shall ensure that screening processes are capable of identifying potential matches, including variations in names, aliases, changes in ownership or control, and other relevant identifying information.

16.4 Sanctions Screening Systems and Controls

16.4.1 Registrants and licensees shall implement sanctions screening systems, processes and controls that are appropriate to the nature, size, complexity and risk profile of their business and that are effective in identifying potential matches against applicable sanctions lists.

16.4.2 Sanctions screening may be conducted through automated systems or manual processes, provided that the method adopted is effective, reliable, appropriately documented and capable of meeting applicable TFS obligations.

16.4.3 Where automated sanctions screening systems are not used, registrants and licensees shall ensure that manual screening processes are sufficiently robust to mitigate the risk of errors, omissions or delays. Such processes shall include, at a minimum:

- clearly documented screening procedures;
- defined responsibility for conducting and reviewing screening;
- appropriate frequency of screening;
- appropriate escalation procedures for potential matches; and
- retention of records evidencing that screening was performed.

16.4.4 Where automated sanctions screening systems are used, registrants and licensees shall ensure that:

- the system is appropriately configured and maintained;
- applicable sanctions lists are updated promptly;
- screening parameters and matching criteria are periodically reviewed;
- potential matches are appropriately investigated and resolved; and
- screening records are retained.

16.4.5 Registrants and licensees shall periodically review and assess the effectiveness of their sanctions screening processes and controls and address any identified deficiencies.

16.5 Management of Potential Sanctions Matches

16.5.1 Registrants and licensees shall establish documented procedures for the review, escalation and management of potential sanctions matches.

16.5.2 Where a potential match is identified, the registrant or licensee shall conduct appropriate review to determine whether the match is a true match or a false positive.

16.5.3 Confirmed or suspected sanctions matches shall be escalated to the appropriate responsible officer, including the Compliance Officer, Money Laundering Reporting Officer (MLRO), or Designated Reported Officer (DRO) for AML/CFT/CPF compliance.

16.5.4 Where a confirmed match is identified, registrants and licensees shall take appropriate action in accordance with applicable legal requirements, including, where required, freezing funds or other assets, restricting transactions and making any required notifications or reports to the relevant competent authority.

16.5.5 Registrants and licensees shall not disclose to customers or other persons that a potential sanctions match has been identified, or that related action is being considered or taken, where such disclosure is prohibited by law.

16.5.6 Where a person or entity is confirmed to be subject to an applicable targeted financial sanction requiring asset freezing, registrants and licensees shall, without delay and without prior notice, freeze the funds or other assets held or controlled by them in accordance with the Anti-Terrorism Act, 2018 and any other applicable legal requirements.

16.5.7 The freezing obligation shall extend, as required by law, to funds or other assets owned or controlled wholly or jointly, directly or indirectly, by a designated person or entity; funds or other assets derived or generated from such property; and funds or other assets of persons or entities acting on behalf of, or at the direction of, a designated person or entity.

16.5.8 Registrants and licensees shall make all notifications and reports required by law to the Attorney General, the Financial Intelligence Unit or other competent authority and shall not make funds or other assets available, directly or indirectly, to or for the benefit of a designated person or entity except as authorised by law. These requirements apply, where relevant, to premiums, claims payments, refunds, surrenders, policy loans, maturity proceeds, annuity payments, commissions, settlements and other insurance-related payments or benefits.

16.6 Record Keeping and Training

16.6.1 Registrants and licensees shall maintain records evidencing sanctions screening conducted, including:

- the date and time of screening;
- the persons or entities screened;
- the sanctions lists used;
- the outcome of screening;
- the review and resolution of potential matches; and

- any actions taken.

16.6.2 Registrants and licensees shall ensure that relevant employees and representatives receive appropriate training regarding sanctions obligations, sanctions screening procedures, escalation requirements and the consequences of non-compliance.

16.6.3 Registrants and licensees shall comply with all targeted financial sanctions screening notices issued by the Commission from time to time. Such notices may require registrants and licensees to conduct screening, provide confirmations, submit information, or undertake other actions within specified deadlines. Failure to comply with a notice, or failure to meet the applicable reporting deadlines, may constitute a breach of AML/CFT/CPF obligations and may result in enforcement action by the Commission.

17. CUSTOMER IDENTIFICATION VERIFICATION AND DOCUMENTARY EVIDENCE REQUIREMENTS

17.1 General Requirements for Verification of Identity

17.1.1 Customer identification and verification is a fundamental component of the customer due diligence process. Registrants and licensees shall obtain sufficient information and evidence to reasonably satisfy themselves as to the identity of customers, beneficial owners, beneficiaries and persons acting on behalf of customers.

17.1.2 Information obtained for verification purposes shall be derived from reliable and independent sources, including documentary evidence, electronic means or other reliable sources of information appropriate to the nature and risk of the relationship.

17.1.3 The nature and extent of information and documentation obtained shall be proportionate to the customer's risk profile, taking into account the nature, size and complexity of the business relationship, the products or services provided and the ML/TF/PF risks identified.

17.1.4 Registrants and licensees shall maintain sufficient records of the information and documentation relied upon to demonstrate that appropriate identification and verification measures have been completed.

17.2 Timing of Verification

17.2.1 Registrants and licensees shall complete verification of identity before establishing a business relationship or carrying out an occasional transaction, except where delayed verification is permitted under applicable legislation and appropriate safeguards are implemented.

17.2.2 Where verification cannot be satisfactorily completed, the requirements set out in Section 14.14 (Failure to Complete Customer Due Diligence) shall apply.

17.2.3 Where a registrant or licensee identifies circumstances that cast doubt on previously obtained identification information, it shall undertake appropriate measures to verify or update the information and reassess the associated ML/TF/PF risks.

17.3 Verification Information and Documentation for Natural Persons

17.3.1 Registrants and licensees shall obtain sufficient information to establish and verify the identity of natural persons who are customers, beneficial owners, beneficiaries or persons acting on behalf of customers.

17.3.2 Information obtained may include, where applicable:

- full legal name;
- date and place of birth;

- residential address;
- nationality;
- occupation or business activity;
- purpose and intended nature of the business relationship;
- source of funds or source of wealth, where required based on risk; and
- government-issued identification or other reliable evidence of identity.

17.3.3 Where a customer presents a higher ML/TF/PF risk, registrants and licensees shall obtain additional information or documentation necessary to establish identity, understand the customer relationship and manage the identified risks.

17.4 Verification of Legal Persons

17.4.1 Where a customer is a legal person, registrants and licensees shall obtain sufficient information and documentation to understand the nature of the entity, verify its existence and establish its ownership and control structure.

17.4.2 Information obtained should include, where applicable:

- a) certificate of incorporation or registration;
- b) registered office and principal place of business;
- c) nature of business activities;
- d) constitutional documents;
- e) directors or persons performing equivalent functions;
- f) authorised representatives;
- g) ownership structure;
- h) beneficial owners; and
- i) purpose and intended nature of the business relationship.

17.4.3 Registrants and licensees shall take reasonable measures to verify that any person acting on behalf of a legal person is authorised to do so.

17.4.4 Where a legal person has a complex, unusual or opaque ownership or control structure, registrants and licensees shall obtain sufficient information to identify the natural persons who ultimately own or control the entity and assess whether enhanced due diligence measures are required.

17.4.5 Registrants and licensees should take reasonable measures to confirm the legal existence and current status of a legal person using reliable and independent sources. Such measures may include consulting an official company registry or other authoritative records, obtaining a certificate of good standing or equivalent documentation, or relying on other independent sources capable of confirming the entity's legal status.

17. Verification of Partnerships, Unincorporated Associations, Charities and Other Similar Organisations

17.5.1 Where the customer is a partnership, unincorporated association, charity, non-profit organisation or other similar entity, registrants and licensees shall obtain sufficient information to:

- establish the existence and purpose of the organisation;
- identify persons authorised to act on its behalf;
- understand its ownership, governance or control structure, as applicable;
- identify persons exercising effective control over the organisation; and
- apply appropriate customer due diligence measures commensurate with the identified ML/TF/PF risks.

17.5.2 Registrants and licensees should obtain appropriate constitutional or governing documents,

mandates or other reliable information sufficient to verify the existence of the organisation and the authority of persons acting on its behalf.

17.6 Verification of Legal Arrangements

17.6.1 Where a customer is a legal arrangement, including a trust or similar arrangement, registrants and licensees shall obtain sufficient information to understand the nature of the arrangement and identify the relevant parties.

17.6.2 Information obtained should include, where applicable:

- the settlor(s);
- trustee(s);
- protector(s), where applicable;
- beneficiaries or classes of beneficiaries;
- persons exercising ultimate control; and
- any other relevant persons connected to the arrangement.

17.6.3 Registrants and licensees shall obtain appropriate documentation evidencing the existence of the legal arrangement and the authority of persons acting on behalf of the arrangement.

17.6.4 Where the structure or circumstances of a legal arrangement presents a higher ML/TF/PF risk, registrants and licensees shall apply enhanced due diligence measures proportionate to the identified risk.

17.7 Verification of Persons Acting on Behalf of Customers

17.7.1 Where a person acts on behalf of a customer, registrants and licensees shall verify:

- a) the identity of the person acting on behalf of the customer; and
- b) the authority of that person to act.

17.7.2 Where a customer acts through an intermediary, nominee, fiduciary or other representative arrangement, registrants and licensees shall apply the requirements relating to third-party reliance and intermediary relationships contained in these Guidelines.

17.8 Additional Verification Considerations for Non-Resident Customers

17.8.1 Where customers, beneficial owners or beneficiaries are located outside The Bahamas, registrants and licensees should consider whether additional information is required to understand the customer's geographic exposure and associated ML/TF/PF risks.

17.8.2 Additional information may include, where relevant:

- country of residence;
- nationality;
- tax residency;
- jurisdictional connections;
- source of funds or source of wealth; and
- information relating to the purpose and nature of the relationship.

17.8.3 Where the information obtained indicates increased geographic or cross-border ML/TF/PF risk, the registrant or licensee shall apply the measures set out in Section 15.

17.9 Reliability and Updating of Verification Information

17.9.1 Registrants and licensees shall maintain sufficient, accurate and reliable customer information to enable effective management of ML/TF/PF risks and shall take appropriate action where

information becomes outdated, unreliable or cannot be obtained.

17.9.2 The need to update identification information and documentation shall be determined using a risk-based approach, taking into consideration:

- the nature and duration of the relationship;
- the customer's risk classification;
- changes in customer circumstances;
- changes in ownership or control;
- changes in beneficiaries;
- unusual activity; and
- other factors indicating increased ML/TF/PF risk.

17.9.3 The expiration of an identification document does not, by itself, require automatic termination of a relationship where the registrant or licensee can otherwise reasonably satisfy itself that the customer's identity remains established and the ML/TF/PF risks continue to be effectively managed.

17.9.4 Where updated information cannot be obtained after reasonable efforts, registrants and licensees shall document the steps taken, reassess the relationship risk and determine appropriate measures, which may include enhanced monitoring, restrictions on services or termination of the relationship.

17.10 Verification Through Third Parties

17.10.1 Where a registrant or licensee relies on another person to perform elements of customer identification and verification, the requirements set out in the Third-Party Reliance section of these Guidelines shall apply.

17.11 Confidentiality and Risk of Tipping Off During Verification

17.11.1 Where concerns arise during the customer identification or verification process that may result in the submission of a suspicious transaction report, registrants and licensees shall ensure that actions taken do not disclose or otherwise alert the customer to the existence of a suspicion or potential report.

17.11.2 Registrants and licensees shall ensure that employees involved in customer identification, verification and due diligence processes are aware of confidentiality obligations and the risks associated with tipping off.

18. ONGOING DUE DILIGENCE AND MONITORING OF CUSTOMER RELATIONSHIPS

18.1 Purpose and Application of Ongoing Due Diligence

18.1.1 Customer due diligence is an ongoing process that extends throughout the duration of a business relationship. Registrants and licensees shall maintain an understanding of their customers, facility holders, beneficial owners, beneficiaries and other relevant parties to ensure that ML/TF/PF risks are effectively identified, assessed and managed.

18.1.2 Registrants and licensees shall undertake ongoing due diligence measures to ensure that information obtained through the customer identification and verification process remains sufficient, accurate and reliable and continues to support the effective management of ML/TF/PF risks.

18.1.3 The extent, frequency and intensity of ongoing due diligence measures shall be proportionate to the level of ML/TF/PF risk associated with the customer relationship, taking into consideration the nature, size and complexity of the business relationship, products or services provided, and

other relevant risk factors.

- 18.1.4 Ongoing due diligence measures form part of the registrant's or licensee's broader AML/CFT/CPF framework and should be supported by appropriate policies, procedures, systems and controls.

18.2 Ongoing Monitoring of Customer Relationships

- 18.2.1 Registrants and licensees shall undertake ongoing monitoring of customer relationships, including facilities where applicable, to determine whether transactions, activities and other relevant events remain consistent with their understanding of:

- the customer;
- the customer's business activities;
- the purpose and intended nature of the relationship;
- the expected source of funds;
- the expected pattern of activity; and
- the identified ML/TF/PF risk.

- 18.2.2 Monitoring measures shall be appropriate to the nature, size and complexity of the business conducted and shall take into consideration the risks associated with insurance products, services and activities.

- 18.2.3 Depending on the nature of the relationship, monitoring may include consideration of:

- premium payments;
- policy amendments;
- changes in ownership;
- beneficiary changes;
- policy assignments;
- policy loans;
- surrender requests;
- withdrawals;
- refunds;
- claims payments;
- third-party payments; and
- other transactions or activities involving movement of funds.

- 18.2.4 Registrants and licensees shall establish appropriate processes to identify unusual or inconsistent activity and determine whether further investigation, enhanced due diligence or suspicious transaction reporting obligations may be required.

18.3 Updating Customer Information

- 18.3.1 Registrants and licensees shall maintain sufficient, accurate and reliable customer information to enable effective management of ML/TF/PF risks and shall take appropriate action where information becomes outdated, unreliable or cannot be obtained.

- 18.3.2 The frequency and extent of customer information updates shall be determined using a risk-based approach and should take into consideration:

- the customer's risk classification;
- the nature and duration of the relationship;
- the products or services provided;
- changes in customer circumstances;
- changes in ownership or control;
- changes in beneficiaries;

- unusual transactions or activity;
- changes in geographic exposure; and
- other information indicating increased ML/TF/PF risk.

18.3.3 Registrants and licensees shall take reasonable measures to obtain updated customer information where necessary to maintain an accurate understanding of the customer relationship.

18.3.4 Reasonable measures may include, where appropriate:

- a) contacting the customer using available communication channels;
- b) requesting updated documentation or information;
- c) obtaining information from reliable independent sources;
- d) reviewing information already available within the registrant's or licensee's records; and
- e) considering information obtained through ongoing monitoring or other legitimate sources.

18.3.5 Where updated information cannot be obtained after reasonable efforts have been made, registrants and licensees shall document the circumstances, reassess the ML/TF/PF risk and determine appropriate risk mitigation measures.

18.3.6 The expiration or unavailability of a particular identification document does not, by itself, mean that a customer relationship must automatically be terminated where the registrant or licensee can otherwise reasonably satisfy itself that the customer's identity remains established and the associated risks can continue to be effectively managed.

18.3.7 Where risks cannot be adequately managed due to outdated, unreliable or unavailable information, registrants and licensees shall consider appropriate action, which may include:

- applying enhanced monitoring;
- obtaining additional information;
- restricting certain activities where appropriate;
- declining additional products or services;
- reviewing whether the relationship should continue; or
- terminating the relationship.

18.4 Review of Customer Information and Risk Assessment

18.4.1 Registrants and licensees shall review customer information and reassess ML/TF/PF risks when circumstances arise that may affect the risk profile of the relationship.

18.4.2 Circumstances requiring review may include:

- material changes to customer circumstances;
- changes in ownership or control;
- changes to beneficiaries;
- changes in the nature or purpose of the relationship;
- unusual or unexpected transactions or activity;
- adverse information concerning the customer or relevant parties;
- changes relating to sanctions, PEP status or other risk indicators;
- changes in geographic exposure; or
- information identified through ongoing monitoring.

18.4.3 The frequency and scope of reviews should be proportionate to the level of ML/TF/PF risk associated with the customer relationship.

18.4.4 Registrants and licensees shall establish and document periodic review cycles appropriate to each customer-risk category. Higher-risk customer relationships shall be reviewed more frequently than standard- or lower-risk relationships, having regard to the nature, complexity and level of ML/TF/PF risk associated with the relationship.

18.4.5 Periodic reviews shall not replace or limit event-driven reviews, which shall be undertaken whenever material changes or other relevant information arise that may affect the customer's risk profile, the nature or purpose of the relationship, or the ability of the registrant or licensee to adequately manage the associated ML/TF/PF risks.

18.5 Simplified Due Diligence

18.5.1 Where a registrant or licensee identifies a lower ML/TF/PF risk, it may apply simplified due diligence measures that are proportionate to the identified risk.

18.5.2 Simplified due diligence does not remove the obligation to understand the customer relationship or to obtain sufficient information to identify and manage ML/TF/PF risks.

18.5.3 Registrants and licensees shall document the basis for applying simplified due diligence measures and ensure that such measures remain appropriate throughout the relationship.

18.5.4 Simplified due diligence shall not be applied where there is suspicion of money laundering, terrorist financing or proliferation financing, or where higher-risk circumstances exist.

18.5.5 A registrant or licensee that applies simplified due diligence shall maintain a documented SDD methodology approved by senior management. The methodology shall identify the lower-risk circumstances in which SDD may be used, the simplified measures permitted, the circumstances in which SDD is prohibited and the arrangements for ongoing monitoring. The Commission may require the methodology or any proposed SDD process to be submitted for prior review or approval where warranted by the registrant's or licensee's risk profile, supervisory history, business model or the nature of the proposed simplified measures.

18.6 Enhanced Due Diligence

18.6.1 Registrants and licensees shall apply enhanced due diligence measures where a customer relationship presents a higher ML/TF/PF risk.

18.6.2 Enhanced due diligence measures shall be proportionate to the identified risk and may include:

- obtaining additional information concerning the customer, beneficial owners, beneficiaries or other relevant parties;
- obtaining information concerning source of wealth and source of funds;
- obtaining senior management approval where appropriate;
- increasing the frequency and intensity of monitoring;
- conducting more frequent reviews of customer information; and
- applying additional controls to mitigate identified risks.

18.6.3 Registrants and licensees shall document the basis for applying enhanced due diligence measures and the actions taken to mitigate identified risks.

18.6.4 Where enhanced due diligence is required in a non-face-to-face or digitally established relationship, additional measures may include corroboration through reliable independent databases, video or other live-interaction verification, certified or notarised documents where appropriate, electronic or biometric verification, device or IP-address information, corroboration of activity against the expected customer profile, and additional verification of source of funds or source of wealth.

18.6.5 Where enhanced due diligence is required in respect of a relationship or transaction involving a

higher-risk country or jurisdiction, registrants and licensees shall apply the measures prescribed in section 15, in addition to any other enhanced due diligence measures appropriate to the identified risks.

18.7 Monitoring of Higher-Risk Customer Relationships

- 18.7.1 Higher-risk customer relationships shall be subject to enhanced monitoring to ensure that activity remains consistent with the registrant's or licensee's understanding of the customer and the identified ML/TF/PF risks.
- 18.7.2 Registrants and licensees should consider whether the frequency, scope and intensity of monitoring remain sufficient to identify changes in customer behaviour, emerging risks or activity requiring further investigation.

18.8 Identification of Structuring and Other Unusual Activity

- 18.8.1 Registrants and licensees shall have appropriate systems and controls to identify activity that may indicate attempts to avoid AML/CFT/CPF obligations or internal controls, including structured transactions or activities.
- 18.8.2 In determining whether transactions or activities may be structured or otherwise unusual, registrants and licensees should consider relevant factors, including:
- the timing and frequency of transactions;
 - whether transactions are linked by common ownership, control or purpose;
 - whether transactions appear deliberately divided to avoid controls or scrutiny;
 - whether the activity is inconsistent with the customer's known profile or expected behaviour; and
 - other relevant ML/TF/PF risk indicators.
- 18.8.3 Where unusual activity or potential structuring is identified, registrants and licensees shall conduct appropriate review, consider whether enhanced due diligence is required and determine whether the circumstances give rise to a suspicious transaction report.

19. RELIANCE ON THIRD PARTIES FOR CUSTOMER DUE DILIGENCE MEASURES

19.1 General Principles

- 19.1.1 Registrants and licensees may, where permitted by law, rely on third parties to perform certain customer due diligence measures, including the identification and verification of customers, beneficial owners, beneficiaries or other relevant parties.
- 19.1.2 Reliance on a third party does not relieve the registrant or licensee of its ultimate responsibility for complying with applicable AML/CFT/CPF obligations and ensuring that customer due diligence measures are appropriately applied.
- 19.1.3 Before relying on a third party, the registrant or licensee shall satisfy itself that the third party:
- is subject to AML/CFT/CPF obligations that are consistent with applicable legal requirements;
 - is supervised or monitored for compliance with those obligations; and
 - has appropriate systems and controls to conduct customer due diligence.
- 19.1.4 For the avoidance of doubt, reliance on a third party under this section does not include arrangements where a registrant or licensee outsources or delegates the performance of customer due diligence activities to an agent, intermediary, or service provider. In such cases, the registrant or licensee remains responsible for ensuring that customer due diligence measures are performed in accordance with applicable AML/CFT/CPF requirements.

19.2 Conditions for Reliance on Third Parties

- 19.2.1 Where a registrant or licensee relies on a third party to conduct customer due diligence, it shall ensure that the third party has obtained sufficient information to identify and verify the customer and any relevant parties, including beneficial owners where applicable.
- 19.2.2 The registrant or licensee shall be able to obtain customer identification and verification information from the third party without delay upon request.
- 19.2.3 The information obtained from the third party shall be sufficient to enable the registrant or licensee to:
- understand the customer relationship;
 - assess ML/TF/PF risks;
 - determine whether enhanced due diligence is required; and
 - comply with applicable suspicious transaction reporting obligations.
- 19.2.4 Registrants and licensees shall maintain appropriate documentation evidencing the basis for reliance on the third party, including, where applicable:
- the identity and status of the third party;
 - confirmation of the third party's AML/CFT/CPF obligations and supervisory status;
 - the nature of the reliance arrangement; and
 - the information obtained from the third party.

19.3 Eligible Third Parties

- 19.3.1 Reliance may be placed on appropriate third parties that are subject to AML/CFT/CPF obligations and supervision, including, where applicable:
- banks and trust companies;
 - insurance companies;
 - securities firms, investment firms or other financial institutions;
 - regulated financial institutions in another jurisdiction that are subject to equivalent AML/CFT/CPF requirements; and
 - other persons or entities permitted under applicable legislation.
- 19.3.2 Registrants and licensees should take reasonable measures to verify the regulatory status of the third party, which may include:
- confirming the third party's status with the relevant supervisory authority;
 - obtaining evidence of licensing or authorization;
 - reviewing publicly available regulatory information; or
 - obtaining other reliable information confirming the third party's regulatory status.

19.4 Reliance Within Corporate Groups

- 19.4.1 A registrant or licensee may rely on customer due diligence measures conducted by another member of the same corporate group where:
- the group applies AML/CFT/CPF policies and procedures;
 - the policies and procedures are consistent with applicable Bahamian AML/CFT/CPF requirements;
 - the group member is subject to AML/CFT/CPF supervision; and
 - the registrant or licensee can obtain relevant customer information and documentation without delay.

- 19.4.2 Reliance on a group member does not remove the responsibility of the registrant or licensee to ensure that customer due diligence requirements are satisfied.

19.5 Written Confirmation and Evidence of Reliance

- 19.5.1 Where reliance is placed on a third party, registrants and licensees should obtain sufficient evidence to demonstrate that the third party has conducted the required customer due diligence measures.

- 19.5.2 Such evidence may include written confirmation from the third party that:

- customer identification and verification measures have been completed;
- relevant customer information and documentation are maintained; and
- such information and documentation will be provided to the registrant or licensee upon request and without delay.

- 19.5.3 The registrant or licensee shall retain evidence of reliance in accordance with applicable recordkeeping requirements.

19.6 Limitations on Reliance

- 19.6.1 Registrants and licensees shall not rely on third parties where:

- the third party is not subject to adequate AML/CFT/CPF obligations;
- the third party is not appropriately supervised;
- sufficient information cannot be obtained without delay;
- the information provided is incomplete, unreliable or inconsistent; or
- the registrant or licensee cannot adequately manage the associated ML/TF/PF risks.

- 19.6.2 Where reliance on a third party is not appropriate or does not provide sufficient assurance, the registrant or licensee shall conduct the required customer due diligence measures directly.

19.7 Reliance Does Not Transfer Responsibility

- 19.7.1 The ultimate responsibility for compliance with customer due diligence obligations remains with the registrant or licensee relying on the third party.

- 19.7.2 Registrants and licensees shall ensure that reliance arrangements are subject to appropriate oversight and are reviewed periodically to confirm that they remain effective and appropriate.

VII. RECORD KEEPING PROCEDURES

20. RECORD KEEPING REQUIREMENTS

20.1 Purpose and General Principles

- 20.1.1 Effective record keeping is a fundamental component of an effective AML/CFT/CPF framework. Registrants and licensees shall maintain records sufficient to demonstrate compliance with applicable AML/CFT/CPF obligations and to enable competent authorities, including the Commission and the Financial Intelligence Unit ("FIU"), to conduct supervisory reviews, investigations and other lawful inquiries.

- 20.1.2 Records maintained by registrants and licensees shall form an appropriate audit trail and should enable:

- the reconstruction of transactions and customer activity;
- identification of the parties involved in a transaction or business relationship;

- assessment of compliance with AML/CFT/CPF obligations; and
- timely provision of relevant information to competent authorities upon request.

20.1.3 Registrants and licensees shall ensure that records maintained are accurate, complete, reliable, accessible and capable of being retrieved within a reasonable timeframe.

20.2 Records to be Maintained

20.2.1 Registrants and licensees shall maintain records relating to their AML/CFT/CPF obligations, including, where applicable:

- customer identification and verification information;
- beneficial ownership and control information;
- information relating to beneficiaries of life insurance policies and investment-related insurance products;
- customer risk assessments and risk classifications;
- enhanced due diligence measures;
- simplified due diligence measures where applied;
- ongoing monitoring and review activities;
- suspicious transaction considerations, including internal assessments and decisions regarding whether to submit a suspicious transaction report;
- reliance on third parties to conduct customer due diligence;
- AML/CFT/CPF policies, procedures and internal controls;
- employee training;
- intermediaries training
- board of directors training
- compliance monitoring, independent testing and supervisory reviews; and
- transactions and business relationship records.

20.2.2 Records maintained should be sufficient to demonstrate the basis for decisions made by the registrant or licensee in managing ML/TF/PF risks.

20.3 Customer Identification and Verification Records

20.3.1 Registrants and licensees shall maintain records relating to customer identification and verification measures undertaken in accordance with these Guidelines and applicable legislation.

20.3.2 Such records should enable the registrant or licensee, where necessary, to demonstrate:

- a) the identity of the customer;
- b) the identity of persons acting on behalf of the customer;
- c) the ownership and control structure of legal persons and legal arrangements;
- d) the identity of beneficial owners;
- e) the identity of beneficiaries where applicable;
- f) the information relied upon to verify identity; and
- g) the basis for any risk-based decisions taken.

20.3.3 Where copies of documents are retained, registrants and licensees should ensure that such copies are accurate reproductions of the original documentation or information relied upon.

20.4 Records Relating to Transactions

20.4.1 Registrants and licensees shall maintain transaction records sufficient to enable transactions to be reconstructed and reviewed.

20.4.2 Transaction records should include, where applicable:

- a) the nature and date of the transaction;
- b) the amount and currency involved;
- c) the parties to the transaction;
- d) the customer, policyholder, beneficiary or other relevant party involved;
- e) the method of payment;
- f) the source of funds where obtained;
- g) the destination of funds where applicable; and
- h) supporting documentation and correspondence relating to the transaction.

20.4.3 For insurance business, transaction records may include, but are not limited to:

- premium payments;
- policy loans;
- policy assignments;
- surrender payments;
- claims payments;
- refunds;
- annuity transactions;
- beneficiary changes;
- changes in ownership; and
- ownership transfers.

20.5 Records Relating to Suspicious Activity

20.5.1 Registrants and licensees shall maintain records relating to suspicious transaction considerations, including where a suspicion has been raised internally but a suspicious transaction report has not been submitted.

20.5.2 Such records should include:

- details of the activity reviewed;
- the basis for the concern;
- internal analysis conducted;
- decisions made by the MLRO, Compliance Officer or Designated Reporting Officer; and
- supporting documentation considered.

20.5.3 Records relating to suspicious activity shall be retained regardless of whether a suspicious transaction report is ultimately submitted.

20.5.4 Where records relate to an ongoing investigation or inquiry by competent authorities, they shall be retained until the registrant or licensee has been advised that the matter has been concluded or otherwise in accordance with applicable law.

20.6 Records Maintained in Electronic Form

20.6.1 Records may be maintained in electronic or other forms, provided that such records:

- accurately reproduce the information originally obtained;
- are readily accessible and capable of retrieval;
- are protected against unauthorized alteration or destruction; and
- can be provided promptly to competent authorities upon request.

20.7 Reliance on Third Parties

20.7.1 Where a registrant or licensee relies on a third party to conduct customer due diligence measures, it shall maintain records demonstrating:

- the identity and status of the third party;
- the basis for reliance;
- the information obtained from the third party; and
- the arrangements in place to obtain customer information without delay.

20.8 Retention Period

20.8.1 Unless a longer period is required by law, registrants and licensees shall retain AML/CFT/CPF records for a minimum period of five (5) years.

20.8.2 The retention period shall commence:

- for transaction records, from the date the transaction is completed;
- for customer records, from the date the business relationship ends; and
- for other AML/CFT/CPF records, from the date the record is created.

20.8.3 Where records relate to an ongoing investigation, litigation, regulatory inquiry or other lawful request, registrants and licensees shall retain such records until permitted to dispose of them.

20.9 Destruction of Records

20.9.1 Records may be securely destroyed after expiry of the applicable retention period, unless retention is required by law, regulatory direction, legal proceedings, investigation or other legitimate business purposes.

20.9.2 Registrants and licensees shall ensure that the destruction of records is conducted in a manner that protects confidentiality and prevents unauthorized access.

20.10 Failure to Maintain Records

20.10.1 Failure to maintain required AML/CFT/CPF records, including beneficial ownership information where applicable, may constitute a breach of applicable AML/CFT/CPF obligations and may result in supervisory or enforcement action.

21. ELECTRONIC PAYMENT TRANSFERS

21.1 General Requirements

21.1.1 The Financial Transactions (Wire Transfers) Regulations, 2018 ("Wire Transfers Regulations"), as amended, establish requirements relating to the transparency and traceability of electronic payment transfers and implement the requirements of FATF Recommendation 16 concerning wire transfers.

21.1.2 Electronic payment transfers represent an important element of the insurance business model, including in relation to the payment of premiums, claims proceeds, policy benefits, refunds, surrenders and other insurance-related transactions. Registrants and licensees should implement appropriate measures to identify, assess and manage the ML/TF/PF risks associated with electronic payment transfers.

21.1.3 Where a registrant or licensee initiates, receives, processes or otherwise participates in electronic payment transfers that fall within the scope of the Wire Transfers Regulations, it shall comply with applicable requirements relating to the collection, verification, retention and transmission of required information.

21.1.4 Registrants and licensees should ensure that their policies, procedures and controls address risks associated with electronic payment transfers, including circumstances where:

- (a) payments are received from or made to persons other than the policyholder, beneficiary

or other relevant party;

- (b) payments originate from or are directed to jurisdictions presenting higher ML/TF/PF risks;
- (c) payment instructions are inconsistent with the registrant's or licensee's understanding of the customer, the purpose of the business relationship or expected activity; or
- (d) payment information is incomplete or cannot be satisfactorily verified.

21.2 Information Accompanying Electronic Payment Transfers

21.2.1 Where applicable, registrants and licensees shall ensure that electronic payment transfers contain sufficient information to enable the transfer to be traced and the parties involved to be identified.

21.2.2 Required information may include, as applicable:

- the name of the payer;
- the payer's account number or unique transaction identifier;
- the payer's address, date and place of birth, national identification number or customer identification number; and
- beneficiary information required under applicable legislation.

21.3 Cross-Border Electronic Payment Transfers

21.3.1 Where a registrant or licensee initiates, receives or otherwise participates in a cross-border electronic payment transfer that falls within the scope of the Wire Transfers Regulations, it shall ensure that the transfer is accompanied by the payer information required under applicable legislation.

21.4 Domestic Electronic Payment Transfers

21.4.1 Where both the originating and beneficiary financial institutions are located within The Bahamas, registrants and licensees shall comply with the applicable domestic information requirements prescribed under the Wire Transfers Regulations.

21.5 Monitoring and Record Retention

21.5.1 Registrants and licensees involved in electronic payment transfers shall maintain appropriate records of information obtained, verified and transmitted in accordance with applicable legislation and the record-keeping requirements set out in Section 19 of these Guidelines.

21.5.2 Registrants and licensees shall establish procedures to identify electronic payment transfers containing incomplete, missing or inconsistent information and shall apply appropriate risk-based measures where deficiencies are identified.

21.6 Compliance with Applicable Legislation

21.6.1 Registrants and licensees shall establish and maintain policies, procedures, systems and controls that address applicable obligations relating to electronic payment transfers and are appropriate to the nature, size and complexity of their business activities.

21.6.2 Registrants and licensees should ensure that employees responsible for processing or overseeing electronic payment transfers receive appropriate training to enable them to identify unusual or suspicious payment activity, understand the applicable legal requirements, and escalate concerns in accordance with the registrant's or licensee's AML/CFT/CPF policies and procedures.

VIII. PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

22. THE FINANCIAL INTELLIGENCE UNIT (FIU)

22.1 Role of the Financial Intelligence Unit

22.1.1 The Financial Intelligence Unit of The Bahamas (“FIU”) is the national agency responsible for receiving, analysing and disseminating suspicious transaction reports (“STRs”) and other financial intelligence in accordance with the Financial Intelligence Unit Act, 2023 (“FIU Act, 2023”) and applicable anti-money laundering, countering the financing of terrorism and proliferation financing (“AML/CFT/CPF”) legislation.

22.1.2 The FIU is empowered under the FIU Act, 2023 to obtain information necessary to fulfil its statutory functions, including information from registrants and licensees.

22.1.3 Registrants and licensees shall provide information requested by the FIU in accordance with applicable legislation and shall maintain appropriate systems and procedures to facilitate timely responses to such requests.

22.2 Obligation to Report Suspicious Transactions

22.2.1 Registrants and licensees shall establish and maintain effective procedures to identify, assess and report suspicious transactions and suspicious activity relating to money laundering, terrorist financing and proliferation financing.

22.2.2 Where a registrant or licensee knows, suspects or has reasonable grounds to suspect that a transaction or proposed transaction involves proceeds of criminal conduct, money laundering, terrorist financing or proliferation financing, it shall submit a suspicious transaction report to the FIU in accordance with applicable legislation.

22.2.3 The obligation to report applies regardless of the amount involved and whether the transaction has been completed, attempted or proposed.

22.2.4 Registrants and licensees should ensure that their suspicious transaction reporting procedures address relevant insurance activities, including, where applicable:

- premium payments;
- claims payments;
- policy surrenders;
- policy loans;
- refunds;
- beneficiary changes;
- payments involving third parties; and
- unusual transactions inconsistent with the customer profile or expected activity.

22.3 Recognition of Identification of Suspicious Activity

22.3.1 A suspicious transaction or activity may involve a transaction, series of transactions, attempted transaction, customer behaviour or other circumstances that are inconsistent with the registrant’s or licensee’s understanding of the customer, the purpose and intended nature of the relationship, or the expected activity associated with the customer.

22.3.2 Effective recognition of suspicious activity depends on a registrant’s or licensee’s understanding of its customers, products, services, delivery channels and geographic exposure.

22.3.3 Registrants and licensees should establish procedures to identify activity inconsistent with:

- (a) the known profile of the customer;
- (b) the customer's expected activity;
- (c) the purpose and nature of the business relationship; or
- (d) the registrant's or licensee's assessment of ML/TF/PF risk.

22.3.4 Registrants and licensees shall ensure that employees and relevant persons receive appropriate, risk-based AML/CFT/CPF training to enable them to understand the money laundering, terrorist financing and proliferation financing risks relevant to the insurance sector and to recognise indicators of suspicious activity requiring further review and potential reporting.

22.3.5 Examples of circumstances that may indicate suspicious activity include:

- transactions that are inconsistent with the customer's known financial profile, business activities, source of funds, expected behaviour or risk profile;
- unexplained payments from or to third parties, including premium payments, claims proceeds, refunds or other transactions involving persons unrelated to the insurance relationship;
- unusual premium payment arrangements, including payments from multiple sources, third-party payments without a clear explanation, or payment methods inconsistent with the customer's profile;
- requests for policy changes, cancellations, refunds, claims payments or other transactions that lack a clear legitimate purpose or are inconsistent with the customer's circumstances;
- transactions involving higher-risk jurisdictions, sanctioned jurisdictions, or persons connected to such jurisdictions without an apparent legitimate purpose;
- activity involving complex ownership, control or beneficiary structures where the purpose, ownership or source of funds cannot be satisfactorily explained;
- attempts to avoid or circumvent customer identification, verification, beneficial ownership, sanctions screening or ongoing monitoring requirements; and
- unusual activity involving insurance intermediaries, policyholders, beneficiaries or other relevant parties that cannot be reasonably explained or appears inconsistent with the nature and purpose of the insurance relationship.

22.4 Internal Reporting of Suspicious Transactions

22.4.1 Registrants and licensees shall establish procedures requiring employees, officers, agents and other relevant persons to promptly report suspicious activity internally to the MLRO or DRO.

22.4.2 Internal reporting procedures shall ensure that:

- (a) employees understand their reporting obligations;
- (b) reports are escalated without delay;
- (c) confidentiality is maintained; and
- (d) information relating to STRs is restricted to persons who require access.

22.4.3 Registrants and licensees shall ensure that the MLRO, DRO or other designated person has timely access to customer due diligence information, transaction records and other relevant information necessary to assess internal reports.

- 22.4.4 Employees who submit an internal suspicious activity report shall not conduct further investigation or disclose information concerning the report except in accordance with established procedures.

22.5 Appointment and Role of the Money Laundering Reporting Officer or Designated Reporting Officer

22.5.1 Appointment of Reporting Officer

- 22.5.1.1 Registrants and licensees shall designate an individual responsible for fulfilling their obligations relating to the recognition, assessment and reporting of suspicious transactions and suspicious activity.
- 22.5.1.2 Depending on the nature, size, complexity and risk profile of the business, this responsibility may be performed by:
- (a) a Money Laundering Reporting Officer (“MLRO”); or
 - (b) a Designated Reporting Officer (“DRO”).
- 22.5.1.3 Where applicable legislation requires a registrant or licensee to appoint an MLRO, the registrant or licensee shall ensure that the appointed MLRO performs the responsibilities set out in these Guidelines.
- 22.5.1.4 Where a registrant or licensee is not required to appoint an MLRO, including certain general insurers and insurance intermediaries, the registrant or licensee shall designate an individual to perform the suspicious transaction reporting function. Such individual shall be referred to as the Designated Reporting Officer (“DRO”).
- 22.5.1.5 The DRO shall perform the functions of the MLRO described in these Guidelines, including receiving internal reports, assessing suspicious activity and determining whether an STR should be submitted to the FIU.
- 22.5.1.6 The Commission recognises that governance arrangements may vary depending on the size, nature, complexity and risk profile of a registrant or licensee. A smaller registrant or licensee, including an insurance intermediary, may designate an appropriately qualified individual to perform the reporting function where the appointment of a dedicated MLRO is not proportionate to the nature and scale of its business activities.
- 22.5.1.7 Regardless of whether the individual is designated as an MLRO or DRO, the registrant or licensee remains responsible for ensuring that the suspicious transaction reporting function is effectively performed.
- 22.5.1.8 All life insurance companies engaged in insurance business are required by law 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.
- 22.5.1.9 The Commission must grant approval for an individual to perform the MLRO or DRO function, only if the candidate satisfies fit and proper criteria.³ 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.
- 22.5.1.10 The MLRO and DRO **must** be registered with the FIU. Registrants and licensees should ensure that any changes in this post are immediately notified to the FIU and the Commission.

22.5.2 Authority, Independence and Access

³ See The Insurance Commission’s Guidelines for Assessing the Fitness and Propriety of Money Laundering Reporting Officers (MLRO) in The Bahamas.

- 22.5.2.1 The MLRO or DRO shall possess sufficient authority, independence, seniority and resources to perform their responsibilities effectively and shall have timely and unrestricted access to customer due diligence information, transaction records, risk assessments, internal reports and any other information necessary to assess suspicious activity and discharge their statutory responsibilities.
- 22.5.2.2 The MLRO or DRO shall have direct and unrestricted access to the Board of Directors and any relevant committee of the Board and shall be permitted to communicate with the Commission, the Financial Intelligence Unit, external auditors and other competent authorities as required in the discharge of their statutory and regulatory responsibilities.
- 22.5.2.3 No director, officer, employee or business function shall improperly restrict, delay or influence the MLRO's or DRO's assessment of suspicious activity or decision whether to submit a suspicious transaction report. The registrant or licensee shall maintain governance arrangements that protect the independence and confidentiality of that decision-making process.

22.5.3 Responsibilities of the MLRO or DRO

- 22.5.3.1 The MLRO or DRO shall be responsible for:
- (a) receiving internal reports of suspicious activity;
 - (b) reviewing and assessing information received;
 - (c) determining whether the circumstances give rise to knowledge, suspicion or reasonable grounds for suspicion;
 - (d) submitting STRs to the FIU where required;
 - (e) maintaining appropriate records of internal reports, assessments and decisions;
 - (f) ensuring confidentiality of suspicious transaction reporting information; and
 - (g) providing guidance regarding suspicious transaction reporting obligations.

22.5.4 MLRO Assessment and Decision-Making

- 22.5.4.1 In determining whether an STR should be submitted, the MLRO or DRO should consider all relevant information available, including:
- (a) customer identification and beneficial ownership information;
 - (b) the nature and purpose of the business relationship;
 - (c) transaction history and patterns;
 - (d) source of funds and source of wealth information, where available;
 - (e) previous internal reports or concerns; and
 - (f) relevant risk information.
- 22.5.4.2 The MLRO or DRO shall document decisions made regarding suspicious activity reports, including the rationale for submitting or not submitting an STR.

22.6 Appointment and Role of the Compliance Officer (CO)⁴

⁴ To be read in conjunction with the Guidelines for Compliance Officer Functions, 2026.

- 22.6.1 Where required under applicable legislation, registrants and licensees shall appoint a Compliance Officer responsible for overseeing compliance with AML/CFT/CPF obligations.
- 22.6.2 The Compliance Officer should have sufficient authority and access to senior management to support the effective implementation and maintenance of AML/CFT/CPF policies, procedures and controls.
- 22.6.3 The Compliance Officer's responsibilities may include:
- overseeing the implementation of AML/CFT/CPF policies and procedures;
 - monitoring compliance with internal controls;
 - coordinating AML/CFT/CPF training;
 - supporting risk assessments; and
 - reporting significant compliance issues to senior management.
- 22.6.4 Depending on the size, nature and complexity of the business, the roles of Compliance Officer and MLRO/DRO may be performed by the same individual, provided that appropriate safeguards exist to ensure effective performance of both functions.
- 22.6.5 The Commission must grant approval for an individual to perform the CO function, only if the candidate satisfies fit and proper criteria. 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.

22.7 Submission of Suspicious Transaction Reports to the FIU

- 22.7.1 Where a registrant or licensee determines that there are reasonable grounds to suspect that a transaction or proposed transaction involves proceeds of criminal conduct, money laundering, terrorist financing or proliferation financing, the MLRO or Designated Reporting Officer (DRO), as applicable, shall ensure that a suspicious transaction report is submitted to the FIU in accordance with applicable legislation and FIU reporting procedures.
- 22.7.2 Suspicious transaction reports shall be submitted through the reporting mechanisms prescribed by the FIU from time to time. Registrants and licensees should ensure that reports are complete, accurate and submitted as soon as practicable after the suspicion has been formed.
- 22.7.3 An STR should contain sufficient information to enable the FIU to understand the basis for the suspicion and, where applicable, should include:
- (a) customer identification and relevant beneficial ownership information;
 - (b) details of the transaction or proposed transaction;
 - (c) the circumstances giving rise to the knowledge, suspicion or reasonable grounds for suspicion;
 - (d) any analysis or enquiries undertaken by the registrant or licensee;
 - (e) relevant supporting documentation or records, where available; and
 - (f) any other information required by the FIU or applicable legislation.
- 22.7.4 Where circumstances require urgent attention, registrants and licensees should communicate with the FIU through any reporting channels or procedures permitted by the FIU or applicable legislation. Any required formal STR shall be submitted as soon as practicable thereafter.
- 22.7.5 Registrants and licensees should maintain records of submitted suspicious transaction reports, including supporting documentation, internal analysis and the decision-making process leading

to the submission of the report, in accordance with the record-keeping requirements contained in Section 18 of these Guidelines.

22.8 Confidentiality and Tipping Off

22.8.1 Registrants and licensees shall ensure that information relating to suspicious transaction reports, including the existence of an STR, is treated as confidential.

22.8.2 Registrants and licensees, including their directors, officers, employees and agents, shall ensure that a customer or other person is **not** informed that:

- (a) an STR has been submitted or may be submitted;
- (b) information has been provided to the FIU; or
- (c) an investigation may be underway.

22.8.2 Registrants and licensees shall implement appropriate controls to prevent unauthorised disclosure of suspicious transaction reporting information. A registrant or licensee shall not disclose information to any person where such disclosure may constitute tipping off or otherwise prejudice an investigation, except where permitted by law.

22.8.3 The confidentiality obligations relating to STRs do not prevent a registrant or licensee from communicating information required by law or responding to lawful requests from competent authorities.

22.9 Feedback from the FIU and Communication with Competent Authorities

22.9.1 The FIU may provide feedback, guidance, trends or other information to reporting entities to support the effectiveness and quality of suspicious transaction reporting.

22.9.2 Registrants and licensees should consider relevant feedback provided by the FIU and use such information to strengthen their AML/CFT/CPF policies, procedures, controls and training programmes.

22.9.3 Registrants and licensees should ensure that relevant communications with the FIU, law enforcement agencies or other competent authorities are appropriately escalated internally to the MLRO, DRO, Compliance Officer or senior management, where applicable.

22.9.4 The submission of an STR to the FIU does not require routine notification to the Commission. However, registrants and licensees shall communicate with the Commission regarding material AML/CFT/CPF deficiencies, governance concerns, significant compliance failures or other matters relevant to the Commission's supervisory responsibilities.

IX. STAFF RECRUITMENT, EMPLOYEE SCREENING, EDUCATION AND TRAINING

23. KNOW YOUR EMPLOYEE (KYE) PROCEDURES

23.1 General Principles

23.1.1 An effective AML/CFT/CPF programme extends beyond customer due diligence and transaction monitoring to include appropriate measures for identifying, assessing and managing risks associated with employees, officers, directors, agents and other persons acting on behalf of a registrant or licensee.

23.1.2 Registrants and licensees should establish and maintain appropriate "Know Your Employee" (KYE) procedures designed to promote high standards of integrity and professionalism and to reduce the risk of employees or other relevant persons facilitating or becoming involved in money laundering, terrorist financing, proliferation financing, fraud or other financial crime.

22.1.3 Employee screening procedures should be risk-based, proportionate to the size, nature and complexity of the registrant's or licensee's business, and applied consistently throughout the employment lifecycle.

23.2 Employee Screening

23.2.1 Before appointing employees, directors, agents or other relevant persons whose duties may expose the registrant or licensee to ML/TF/PF risks, appropriate screening procedures should be undertaken.

23.2.2 Depending on the nature of the position and the level of risk involved, screening measures may include:

- (a) verification of identity;
- (b) confirmation of employment history;
- (c) verification of professional qualifications, licences or certifications, where applicable;
- (d) reference checks;
- (e) police certificates of character or equivalent background checks where appropriate;
- (f) confirmation that the individual satisfies applicable fit and proper requirements; and
- (g) any other screening measures appropriate to the risks associated with the position.

23.2.3 Registrants and licensees should document their employee screening procedures and retain appropriate records demonstrating that the required screening has been completed.

23.3 Ongoing Employee Integrity

23.3.1 Employee screening should not be limited to the recruitment process. Registrants and licensees should establish procedures to identify circumstances that may affect the continued suitability or integrity of employees performing functions relevant to AML/CFT/CPF compliance.

23.3.2 Registrants and licensees should take appropriate action where information becomes available that may affect an individual's fitness, integrity or ability to perform their responsibilities.

23.3.3 Appropriate internal controls should also enable the registrant or licensee to identify and investigate unusual employee conduct that may indicate increased ML/TF/PF, fraud or other financial crime risks.

Examples may include:

- unusual transaction activity involving customers handled by the employee;
- unexplained changes in business patterns or customer activity;
- repeated attempts to override internal controls;
- unauthorized access to customer information or records;
- unexplained lifestyle changes inconsistent with known income; or
- known associations with persons engaged in criminal activity or other circumstances giving rise to integrity concerns.

23.4 Responsibility of Senior Management

- 23.4.1 Senior management should ensure that appropriate employee screening procedures form part of the registrant's or licensee's overall AML/CFT/CPF compliance framework.
- 23.4.2 The effectiveness of employee screening procedures should be reviewed periodically and updated where necessary to address changes in the registrant's or licensee's business activities or ML/TF/PF risks.

24. AML/CFT/CPF EDUCATION, TRAINING AND AWARENESS

24.1 General Requirements

- 24.1.1 Registrants and licensees shall establish and maintain ongoing AML/CFT/CPF education and training programmes designed to ensure that employees, directors, officers, agents and other relevant persons understand their legal obligations and are capable of effectively implementing the registrant's or licensee's AML/CFT/CPF programme.
- 24.1.2 Registrants and licensees should undergo AML/CFT/CPF training at least once per year.
- 24.1.3 Training programmes shall be appropriate to the size, nature and complexity of the business and tailored to the responsibilities of the individuals receiving the training.
- 24.1.4 New employees and other relevant persons should receive AML/CFT/CPF training as soon as practicable following their appointment and before undertaking duties that may expose the registrant or licensee to ML/TF/PF risks.

24.2 Training Content

- 24.2.1 Training programmes should, where applicable, include, but are not limited to, the following:
- (a) applicable AML/CFT/CPF legislation and regulatory requirements;
 - (b) the registrant's or licensee's AML/CFT/CPF policies, procedures and internal controls;
 - (c) customer due diligence and ongoing monitoring requirements;
 - (d) beneficial ownership requirements;
 - (e) targeted financial sanctions and proliferation financing obligations;
 - (f) recognising and reporting suspicious transactions;
 - (g) internal reporting procedures and the roles of the MLRO, Designated Reporting Officer (DRO) and Compliance Officer, where applicable;
 - (h) record-keeping obligations;
 - (i) tipping-off prohibitions and confidentiality requirements;
 - (j) emerging ML/TF/PF risks, trends and typologies relevant to the insurance sector; and
 - (k) the consequences of non-compliance for both the individual and the registrant or licensee.

24.3 Role-Specific Training

- 24.3.1 Training should be appropriate to the functions performed by the individual and should take into account the nature of the ML/TF/PF risks associated with those responsibilities.
- 24.3.2 Additional or specialised training should be provided, where appropriate, to persons with specific AML/CFT/CPF responsibilities, including:
- members of the Board;
 - senior management;
 - Compliance Officers;
 - MLROs and Designated Reporting Officers;
 - underwriting personnel;
 - claims personnel;
 - employees responsible for customer onboarding and customer due diligence;
 - agents, brokers and intermediaries; and
 - any other employees performing higher-risk functions.

24.4 Ongoing Awareness

- 24.4.1 Registrants and licensees shall provide ongoing education and awareness programmes to ensure that employees remain informed of developments in AML/CFT/CPF legislation, regulatory expectations, emerging risks, sanctions obligations and evolving money laundering, terrorist financing and proliferation financing typologies.
- 24.4.2 Training should be provided regularly and whenever significant changes occur to applicable legislation, regulatory requirements, internal policies or the registrant's or licensee's risk profile.

24.5 Training Records and Effectiveness

- 24.5.1 Registrants and licensees shall maintain appropriate records of AML/CFT/CPF training conducted, including, where applicable:
- (a) the dates of training;
 - (b) the content delivered;
 - (c) the names or positions of attendees;
 - (d) attendance records; and
 - (e) any assessments or other measures used to evaluate understanding.
- 24.5.2 Registrants and licensees should periodically assess the effectiveness of their AML/CFT/CPF training programmes and take appropriate steps to address any identified deficiencies.

APPENDIX A

OVERVIEW OF THE BAHAMIAN AML/CFT/CPF LEGISLATIVE FRAMEWORK

The Proceeds of Crime Act, 2018 (POCA), as amended

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 (FTRA), as amended

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 (FTRR), as amended

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, 2023 (FIUA)

The Financial Intelligence Unit Act, 2023 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 (FI(TR)R

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 (ATA), and Regulations, 2018 as amended

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.

International Obligations (Economic and Ancillary Measures) Act, 1993 and Related Orders

This legislation provides the framework for implementing international sanctions and other obligations arising from decisions of international organisations, including measures relating to targeted financial sanctions.

DRAFT

APPENDIX B

AML/CFT/CPF EXAMINATION PROCESS AND SUPERVISORY ASSESSMENT

Overview of AML/CFT/CPF Examination Process and Supervisory Assessments

The Commission conducts AML/CFT/CPF supervisory assessments using a risk-based approach. The nature, scope, and frequency of supervisory reviews may vary depending on the type of registrant or licensee, its risk profile, the nature and complexity of its business activities, and the Commission's supervisory priorities.

AML/CFT/CPF assessments may be conducted through various supervisory processes, including the review of completed AML/CFT/CPF examination forms and onsite examinations conducted by the Commission's Examination Unit.

Routine AML/CFT/CPF Examination Form Reviews

Where applicable, the AML/CFT/CPF examination form shall be completed and submitted to the Commission by the Compliance Officer (CO) or external auditor, as applicable.

The Commission reviews the information submitted and evaluates the effectiveness of the registrant's or licensee's AML/CFT/CPF framework, including its compliance with applicable AML/CFT/CPF obligations.

Following the review, the Commission issues a feedback letter to the registrant or licensee outlining the results of the assessment, including any identified deficiencies and required corrective actions, where applicable.

Onsite AML/CFT/CPF Examinations

The Commission may conduct onsite AML/CFT/CPF examinations as part of its supervisory process. Onsite examinations are conducted by the Commission's Examination Unit and involve an assessment of the registrant's or licensee's AML/CFT/CPF framework, policies, procedures, systems, controls, and overall compliance with applicable requirements.

The results of onsite examinations, including identified deficiencies and required corrective actions, are communicated to the registrant or licensee by the Examination Unit.

The findings arising from onsite examinations assist the Commission in determining the appropriate supervisory response and whether further monitoring, remediation, or supervisory action is required.

Supervisory Assessment Outcome

The Commission assigns an assessment outcome based on its evaluation of the information obtained through the applicable supervisory process.

The assessment outcome provides an indication of the effectiveness of the registrant's or licensee's AML/CFT/CPF framework and its ability to identify, assess, manage, and mitigate ML/TF/PF risks.

Table 2

Supervisory Activity	Process	Commission Assessment and Feedback
Routine AML/CFT/CPF Examination	The completed examination form is submitted to the Commission by the Compliance Officer (CO) or external auditor, as applicable.	The Commission reviews and evaluates the information provided, assigns an assessment outcome, and issues a feedback letter to the registrant or licensee outlining the results of the assessment, including deficiencies and required corrective actions, where applicable.
Onsite AML/CFT/CPF Examination	The Commission's Examination Unit conducts an onsite review of the registrant's or licensee's AML/CFT/CPF framework, policies, procedures, systems, and controls.	The Commission evaluates the results of the examination, assigns an assessment outcome, and issues communication to the registrant or licensee outlining the results, including deficiencies and required corrective actions, where applicable.

The Commission's supervisory assessment outcome is based on its evaluation of information obtained through the applicable examination process and other relevant supervisory information. The assessment outcome provides an indication of the effectiveness of the registrant's or licensee's AML/CFT/CPF framework and the extent to which ML/TF/PF risks are being effectively identified, assessed, managed, and mitigated.

APPENDIX C

MINIMUM INFORMATION TO SUPPORT THE SUBMISSION OF A SUSPICIOUS TRANSACTION REPORT (STR)

This Appendix is intended to provide guidance on the minimum information that registrants and licensees should consider compiling when preparing a Suspicious Transaction Report (STR). It does not replace or modify the reporting requirements or prescribed reporting procedures established by the Financial Intelligence Unit (FIU). Registrants and licensees should submit STRs using the FIU's prescribed reporting mechanism and in accordance with applicable AML/CFT/CPF legislation.

When a registrant or licensee determines that a Suspicious Transaction Report (STR) should be submitted to the Financial Intelligence Unit (FIU), sufficient information should be obtained and documented to enable the FIU to understand the circumstances giving rise to the suspicion and to support any subsequent investigation. As appropriate, the following information should be compiled and retained:

1. Reporting Institution Information

- Name of the registrant or licensee.
- Name and position of the MLRO or Designated Reporting Officer (DRO).
- Internal reference number (if applicable).
- Date the suspicion was identified.
- Date the STR was submitted.

2. Customer Information

- Full name of the customer.
- Residential and mailing address.
- Date of birth (where applicable).
- Nationality.
- Occupation or nature of business.
- Customer identification number or policyholder reference.
- Risk classification (where applicable).

3. Beneficial Owner and Other Relevant Parties

Where applicable:

- Beneficial owner(s).
- Policy owner.
- Beneficiary or beneficiaries.
- Trustee, settlor, protector or nominee.
- Authorised representative.
- Intermediary or broker.

- Any other connected person.

4. Policy Information

- Policy number.
- Type of insurance product.
- Date issued.
- Sum insured.
- Premium amount and payment frequency.
- Policy status.
- Beneficiary details.
- Any assignments or ownership changes (where applicable).

5. Transaction Information

Where relevant:

- Date(s) of the transaction.
- Amount(s).
- Currency.
- Method of payment.
- Source of funds (if known).
- Destination of funds.
- Premium payments.
- Refunds.
- Surrenders.
- Policy loans.
- Claims payments.
- Any attempted transaction.

6. Description of the Suspicious Activity

A clear narrative explaining:

- The activity that gave rise to the suspicion.
- The reasons why the activity is considered suspicious.
- Relevant dates and chronology.
- Any unusual or inconsistent behaviour.
- Any identified ML, TF or PF indicators or red flags.
- Whether the transaction was completed, refused or attempted.

7. Supporting Documentation

Where available:

- Customer due diligence records.
- Identification documents.
- Policy documentation.
- Transaction records.
- Payment instructions.
- Internal investigation notes.
- Correspondence.
- Any other relevant records.

8. Action Taken by the Registrant or Licensee

Where applicable:

- Enhanced due diligence undertaken.
- Additional information requested.
- Transaction delayed or declined.
- Business relationship terminated.
- Internal escalation to the MLRO.
- Other mitigating measures implemented.

9. Recordkeeping

Registrants and licensees should maintain copies of the STR and all supporting documentation in accordance with applicable legislative and regulatory recordkeeping requirements. Appropriate safeguards should be implemented to preserve the confidentiality of the report and to prevent unauthorised disclosure or tipping-off.

APPENDIX D

EXAMPLES OF AML/CFT/CPF TYPOLOGIES, RISKS AND RED FLAGS IN THE INSURANCE SECTOR

This Appendix provides examples of money laundering (ML), terrorist financing (TF), and proliferation financing (PF) typologies and indicators that may be encountered in the insurance sector. It is intended to assist registrants and licensees in recognising potentially suspicious activities and transactions and should be read in conjunction with these Guidelines, the registrant's or licensee's AML/CFT/CPF policies, procedures and controls, and its institutional risk assessment.

The examples are illustrative only and are not exhaustive. The presence of one or more indicators does not necessarily mean that ML, TF, or PF is occurring. Registrants and licensees should consider the facts and circumstances of each case and apply a risk-based approach when determining whether further enquiries, enhanced due diligence, or the submission of a Suspicious Transaction Report (STR) is warranted.

1. Customer, Beneficial Ownership and Due Diligence Risks

Insurance products may be vulnerable to misuse where registrants and licensees do not have a clear understanding of the customer, beneficial owner, beneficiary, source of funds, and purpose of the insurance business relationship.

Examples include:

- Customers who are reluctant, unwilling, or unable to provide required identification, beneficial ownership, or source of funds information.
- Difficulty identifying or verifying the ultimate beneficial owner of a customer, policyholder, beneficiary, or other relevant party.
- Use of complex ownership structures, trusts, nominees, or intermediaries without a clear legitimate purpose.
- Information provided by the customer that is inconsistent, incomplete, or difficult to verify.
- Frequent changes to ownership, beneficiaries, authorised persons, or other relevant parties without a reasonable explanation.

2. Insurance Product and Policy Risks

Certain insurance products and policy features present increased ML/TF/PF risks, particularly where they permit the movement, accumulation, or recovery of funds.

Examples include:

- Purchase of single premium life insurance policies or investment-related insurance products inconsistent with the customer's known financial profile.
- Early surrender, cancellation, or termination of policies shortly after inception without a reasonable economic explanation.
- Requests for policy loans, withdrawals, or surrender proceeds without a clear legitimate purpose.
- Use of insurance products to move funds between individuals, entities, or jurisdictions.

- Assignment of policies or changes to beneficiaries shortly after policy issuance without an apparent legitimate reason.

3. Premium Payment and Transaction Risks

Premium payments and related transactions may present elevated risk where the source, purpose, or destination of funds is unclear.

Examples include:

- Premium payments made by third parties with no apparent relationship to the policyholder.
- Large or unusual premium payments inconsistent with the customer's financial circumstances.
- Requests for refunds or payments to persons other than the policyholder or original source of funds.
- Frequent overpayments followed by requests for reimbursement.
- Unusual payment methods or transactions involving jurisdictions with increased ML/TF/PF risks.

4. Claims and Benefit Payment Risks

Insurance claims and benefit payments may be misused to introduce illicit funds into the financial system or create the appearance of legitimate proceeds.

Examples include:

- Claims involving suspicious, incomplete, altered, or inconsistent supporting documentation.
- Requests for claim payments to unrelated third parties.
- Claims activity inconsistent with the nature of the policy or customer profile.
- Attempts to use insurance proceeds as a means of transferring or legitimising illicit funds.

5. General Insurance Sector Indicators

General insurers may face ML/TF/PF risks arising from underwriting, claims activity, premium payments, and the involvement of intermediaries.

Examples include:

- Multiple insurance policies purchased without an apparent legitimate insurance purpose.
- Unusual premium payments for the nature of the insured activity or customer's business.
- Transactions involving fictitious, inflated, or questionable claims.
- Customers using insurance products primarily as a means of moving funds rather than obtaining insurance protection.
- Unusual activity involving brokers, agents, or intermediaries.
- Adverse-media-driven declination/rescission.
- Applicant misrepresentation leading to preventive refusal.
- High-risk ownership with unknown source of funds.

6. Intermediary-Related Risks

Intermediaries may introduce additional risk where customer information is incomplete or where due diligence responsibilities are not effectively performed.

Examples include:

- Intermediaries failing to provide sufficient customer information.
- Customers introduced through intermediaries who seek to avoid direct engagement with the insurer.
- Intermediaries discouraging completion of customer due diligence requirements.
- Unusual reliance on intermediaries for customer information or verification.
- Transactions involving intermediaries connected to higher-risk jurisdictions or activities.

7. Geographic and Sanctions-Related Risks

Insurance products may be vulnerable to misuse through cross-border transactions or relationships involving higher-risk jurisdictions or sanctioned persons.

Examples include:

- Customers, beneficiaries, counterparties, or transactions connected to jurisdictions presenting increased ML/TF/PF risks.
- Transactions involving sanctioned persons, entities, or jurisdictions.
- Payments to or from countries unrelated to the customer's residence, business activities, or insurance relationship.
- Unexplained cross-border movements of funds.

8. Behavioural Indicators

Customer behaviour may provide important indicators of potential misuse of insurance products.

Examples include:

- Customers attempting to avoid reporting thresholds or internal controls.
- Customers demonstrating unusual knowledge of AML/CFT/CPF processes.
- Customers providing conflicting explanations regarding the purpose of the insurance relationship.
- Requests to circumvent established procedures or requirements.

Illustrative Case Examples from the Bahamian Insurance Sector

Case 1: Potential Misuse of Life Insurance Products by a Politically Exposed Person

Description

A politically exposed person (PEP) sought to obtain life insurance coverage while using an adopted son as the life insured. During the customer due diligence and enhanced due diligence process, the insurer identified inconsistencies relating to the customer's source of wealth, a lack of cooperation in providing requested information, and a previously undisclosed change to the life insured. The combination of these factors raised concerns that the policy structure may have been used to conceal beneficial ownership or facilitate the placement or integration of proceeds derived from corruption or other criminal activity.

Key Typologies

- Use of life insurance products to facilitate the placement or integration of proceeds of corruption or other illicit activity.
- Use of a third-party nominee or related person as the life insured to obscure the true ownership, control, or purpose of the insurance policy.
- Use of complex or unusual policy structures involving family members or associates to distance the customer from the underlying assets or benefits.

Red Flags

- Customer is a PEP or closely associated with a PEP, particularly where higher-risk jurisdictions or corruption risks are present.
- Customer is unable or unwilling to provide satisfactory evidence of source of wealth or source of funds.
- Failure or refusal to provide requested CDD or EDD information.
- Repeated delays, evasiveness, or non-cooperation during the due diligence process.
- Undisclosed, unexplained, or late changes to the life insured, beneficiary, ownership structure, or other relevant parties.
- Use of family members, associates, or other third parties without a clear and legitimate rationale.
- Insurance arrangement appears inconsistent with the customer's known financial profile, circumstances, or stated purpose.

Key Compliance Lessons

- Registrants and licensees should apply enhanced due diligence measures to PEPs and their close associates in accordance with their risk-based approach.
- The purpose and rationale for involving third parties in an insurance relationship should be clearly understood, documented, and supported by appropriate evidence.
- Source of wealth and source of funds should be independently verified where required, particularly for higher-risk customers and transactions.
- Unexplained changes involving policy ownership, beneficiaries, insured persons, or other relevant parties should be subject to appropriate review and escalation.
- Where concerns remain unresolved, the matter should be escalated to the MLRO or

designated officer for consideration of whether further action, including the filing of an STR, is warranted.

Case 2: Potential Use of Life Insurance Products to Conceal Proceeds of Fraud

Description

An individual established a life insurance policy and transferred assets into the policy using funds purportedly derived from a legitimate business activity. Subsequent information raised concerns that the stated source of funds may have been connected to proceeds derived from fraudulent activity. Additional concerns included transfers involving an associated entity and the movement of multiple asset types into the policy.

The circumstances raised concerns that the insurance product may have been used to place, layer, or conceal proceeds of crime and create the appearance of legitimate wealth.

Key Typologies

- Use of life insurance products to place or hold suspected proceeds of crime.
- Movement of funds through associated entities or third parties to create distance from the underlying criminal activity.
- Misrepresentation or concealment of the true source of funds or source of wealth.
- Use of insurance products to facilitate the eventual integration of illicit proceeds.

Red Flags

- Source of funds or source of wealth is inconsistent with information obtained through customer due diligence.
- Customer's declared source of funds is connected to allegations of fraud, financial crime, or other criminal activity.
- Significant assets introduced into an insurance policy without a clear legitimate rationale.
- Transfers received from associated entities or third parties without a clear economic purpose.
- Customer unable to satisfactorily explain the origin or movement of funds used to establish or maintain the policy.
- Use of a life insurance product primarily as an asset-holding vehicle rather than for a genuine insurance purpose.

Key Compliance Lessons

- Source of funds and source of wealth should be appropriately verified, particularly where significant assets are introduced into an insurance relationship.
- Registrants and licensees should consider the purpose, timing, and rationale for significant transactions or asset transfers.
- Information indicating possible links to fraud or other criminal activity should be assessed as part of the institution's ongoing monitoring and risk assessment processes.

Case Example 3: Potential Misuse of Insurance Processes Through Document Fraud

and Internal Control Circumvention

Description

During a post-contractual file review and remediation exercise conducted following the expiry of an insurance management arrangement, several insurance policy files were identified as lacking formal approval documentation. A further review of selected policies identified documents bearing the signature of a designated approving Director who confirmed that the signature had not been provided by him and that he had not authorized any person to sign on his behalf.

The circumstances raised concerns that policy approval processes may have been circumvented and that falsified documentation may have been used to create the appearance of appropriate authorization, governance oversight, and compliance with internal procedures.

Such practices may expose insurers to increased financial crime risks by weakening governance controls, undermining the reliability of customer and policy records, and creating opportunities for unauthorized transactions or concealment of irregular activity.

Key Typologies

- **Document fraud and falsification of records:** Use of fraudulent signatures or altered documentation to create the appearance of legitimate approval or authorization.
- **Internal control circumvention:** Deliberate bypassing of established governance, underwriting, approval, or oversight processes.
- **Unauthorized policy issuance or processing:** Issuance or administration of policies without appropriate authorization or review.
- **Exploitation of periods of organizational change:** Use of management transitions, contractual changes, or reduced oversight periods to conceal irregular activities.

Red Flags

- Policy files lacking required approval documentation or evidence of appropriate authorization.
- Documents containing signatures or approvals that cannot be independently verified.
- Approval processes that are inconsistent with established governance procedures.
- Policies issued or amended without a clear audit trail.
- Significant documentation gaps identified during file reviews, remediation exercises, or management transitions.
- Employees, representatives, or service providers bypassing established controls or approval requirements.
- Unusual activity occurring during periods of organizational change, outsourcing transitions, management changes, or reduced oversight.
- Inconsistencies between policy records, approval documentation, and information provided by responsible officers.

Key Compliance Lessons

- Registrants and licensees should maintain effective governance frameworks and internal controls to ensure that policies are issued and administered only through authorized processes.
- Approval documentation and records should be maintained in a manner that allows for independent verification and audit review.
- Periods of transition, including changes in management arrangements, outsourcing relationships, or operational responsibilities, should be subject to appropriate oversight and monitoring.
- Suspected fraud, document falsification, or intentional circumvention of controls should be escalated promptly in accordance with internal procedures and assessed for potential financial crime implications.
- Weaknesses in governance and record integrity may increase exposure to ML, fraud, and other financial crime risks and should be addressed through appropriate remediation.

APPENDIX E

AML/CFT/CPF INFORMATION RESOURCES

The following websites provide access to legislation, guidance, advisories, sanctions information, typologies, and other resources relevant to AML/CFT/CPF compliance. Registrants and licensees should consult these resources regularly to remain informed of developments affecting their AML/CFT/CPF obligations.

Organisation	Purpose
Insurance Commission of The Bahamas	AML/CFT/CPF Guidelines, supervisory notices, circulars, legislation, and regulatory guidance applicable to the insurance sector.
Financial Intelligence Unit of The Bahamas (FIU)	Suspicious Transaction Reports (STRs), guidance, advisories, and reporting information.
Financial Transactions Reporting Act (Government of The Bahamas) https://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2018/2018-0005/2018-0005_1.pdf	AML/CFT/CPF legislation and related statutory instruments.
Financial Action Task Force (FATF)	FATF Recommendations, guidance, High-Risk Jurisdictions, and Calls for Action.
Caribbean Financial Action Task Force (CFATF)	Regional AML/CFT/CPF guidance, mutual evaluation reports, and typologies.
International Association of Insurance Supervisors (IAIS)	Insurance supervisory standards and AML/CFT application papers relevant to insurers.
United Nations Security Council Sanctions	United Nations sanctions regimes and designated persons and entities.
United Nations Consolidated Sanctions List	Consolidated list of individuals and entities subject to UN Security Council sanctions.
Office of Financial Sanctions Implementation (OFSI)	UK financial sanctions guidance and Consolidated List.
Office of Foreign Assets Control (OFAC)	U.S. sanctions programs, SDN List, and sanctions guidance.
Egmont Group of Financial Intelligence Units	Information on international cooperation among Financial Intelligence Units.