




Financial Intelligence Centre

Republic of Zambia

**ANTI-MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM AND
PROLIFERATION (AML/CFTP) GUIDELINES FOR THE INSURANCE SECTOR**

This document is authorized by:

Name	Title	Date	Signature
Mrs. Liya Tembo	Acting Director General	18/08/2023	

Version Control:

Version	Date	Status	Author
1.0	2019	Initial development of document	Compliance & Prevention Department
2.0	August 2023	First Review	Compliance & Prevention Department

TABLE OF CONTENTS

1.0	INTRODUCTION.....	3
2.0	PURPOSE OF GUIDELINES	4
3.0	SCOPE OF GUIDELINES	4
4.0	OVERVIEW OF THE SECTOR	4
5.0	THE ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION COMPLIANCE PROGRAM	5
5.1.	INSTITUTIONAL RISK ASSESSMENT.....	5
5.2	RISK BASED APPROACH.....	6
5.3	INTERNAL POLICIES, PROCEDURES AND CONTROLS	6
5.4	COMPLIANCE OFFICER.....	7
5.5	TRAINING	8
5.6	INDEPENDENT AUDIT	8
6.0	CUSTOMER DUE DILIGENCE	9
6.1	CUSTOMER DUE DILIGENCE PROCEDURES	9
6.2	HIGH-RISK CATEGORIES OF CUSTOMERS.....	12
7.0	WIRE TRANSFERS	13
8.0	SANCTION SCREENING.....	14
9.0	RECORD KEEPING	14
10.0	REPORTING OBLIGATIONS	14
10.1	CURRENCY TRANSACTION REPORTS (CTRs).....	14
10.2	SUSPICIOUS TRANSACTION REPORTS (STRs)	15
(a)	Obligation to Report Suspicious Transactions.....	15
(b)	Prohibition against Tipping Off	15
(c)	Protection of Identity of Persons and Information Relating to STRs	16
(d)	Exemption from liability for good faith reporting of suspicious transactions	16
10.3	HOW TO IDENTIFY A SUSPICIOUS TRANSACTION IN THE SECTOR.....	16
10.4	HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO THE CENTRE.....	18
11.0	OFFENCES BY BODY CORPORATE OR UNINCORPORATE	19
12.0	MONITORING OF COMPLIANCE PROGRAM	19
13.0	FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS	19
ANNEXURE I	GLOSSARY OF TERMS	20

1.0 INTRODUCTION

Money laundering (ML), terrorist financing (TF) and proliferation financing (PF) and any other financial crimes are a global concern and as such the international community has come together to fight these crimes. People or groups laundering money or financing terrorists and proliferation activities take certain steps to conceal their true identities and sources of funds. As such, in keeping up with international obligations and ensuring that reporting entities such as insurance sector players are not abused by persons involved in ML/TF /PF, the Financial Intelligence Centre (the Centre) was established in 2010. The Centre is an autonomous corporate body established under the Financial Intelligence Centre Act No. 46 of 2010 as amended (the FIC Act) as amended. The Centre's core function is to receive, request, analyse suspicious transaction reports (STRs) and other disclosures for dissemination of financial intelligence reports to relevant competent authorities for investigation and prosecution where there are reasonable grounds to suspect that crimes have been committed.

ML /TF/PF involve activities that represent a threat to the stability and integrity of the financial system which in the long term weakens citizens' confidence in the democratic principles of a modern society, and leads to the increased necessity for supervising and monitoring of the financial system for the purpose of preventing and detecting activities linked with ML/ TF/PF.

The Zambian government recognizes the susceptibility of the insurance sector to ML/TF/PF. To this end the FIC Act has created certain obligations to reporting entities operating in the insurance sector in the fight against ML/TF/PF.

Combating ML/TF/PF requires all institutions identified under the FIC Act as reporting entities to effectively implement Anti Money Laundering (AML)/Countering the financing of terrorism and proliferation (CFTP) laws and measures outlined in these Guidelines in order to minimize the risk of the Zambian financial system being used to launder money or finance terrorism or proliferation activities. It is the responsibility of the Centre to issue guidelines to reporting entities to ensure that they comply accordingly with the provisions of the FIC Act.

2.0 PURPOSE OF GUIDELINES

The purpose of these Guidelines is to provide guidance for insurance sector players on their legal obligations to prevent and detect money laundering and financing of terrorism activities. In addition, the guidelines will assist the sector players to comply with the FIC Act.

The Guidelines are issued pursuant to Section 5 (2) (i) and Section 56 of the FIC Act and in consultation with the supervisory authorities for the purpose of ensuring a uniform application of AML/CFTP obligations by insurance sector players.

3.0 SCOPE OF GUIDELINES

The Guidelines have incorporated essential elements of the FIC Act, Insurance Act No. 38 of 2021, Financial Action Task Force (FATF) Recommendations and other international best practices on the AML/CFTP regime. They cover among others the following key areas of AML/CFTP policy; customer due diligence, the AML/CFTP compliance program; transaction monitoring and reporting obligations.

These Guidelines are provided as general information only and as such, do not cover all the AML/CFTP legal obligations of insurance sector players. The Guidelines do not constitute legal advice and are not intended to replace the FIC Act or any other guidelines, directives or regulations issued by the Centre or the sector regulator.

4.0 OVERVIEW OF THE SECTOR

The insurance sector plays a fundamental role in the Zambian economy. In Zambia the industry contributes to the economy by providing financial security, mobilising savings and promoting direct and indirect investments. A sound insurance sector represents an essential feature of a proper economic system, engendering economic growth and fostering high employment. However, an optimal regulatory environment is needed to allow the insurance sector to fully play its role in the economy.

Insurance business in Zambia is considered to be the business of undertaking liability by way of insurance, including re-insurance, in respect of any loss of life and personal injury and any loss or damage, including liability to pay damage or compensation, contingent upon the

happening of a specified event, and any business incidental to insurance business. Due to the nature of the products and services provided by the insurance industry and the increasing growth and sophistication of the insurance providers, insurance products are attractive to money launderers and terrorist financiers. Therefore, in order to protect the industry from criminal activities associated with ML/TF/PF in Zambia, the insurance sector is subjected to AML/CFTP requirements.

Thus, the creation of the Pension and Insurance Authority (PIA), a supervisory authority of the sector was part of the government's economic reform program aimed at developing the insurance and pension sector in order to support and enhance private sector initiatives. PIA's role is to regulate the conduct of insurance and pension industry players through supervision in order to protect the interest of insurance policyholders and members of pension schemes and to foster the industry's growth, development and stability.

5.0 THE ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION COMPLIANCE PROGRAM

An AML/CFTP compliance program is an essential component of a reporting entity's compliance regime. Reporting entities are obliged, according to Section 23 of the FIC Act, to develop and implement programs for the prevention of ML/TF/ PF or any other serious offence relating to ML/TF/PF. The programs should be risk based, and should be designed to mitigate the ML/TF/PF risks the reporting entity may encounter.

5.1. INSTITUTIONAL RISK ASSESSMENT

Insurance sector players are required to take appropriate steps to identify, assess and understand their ML/TF/PF risks relating to customers, services or products, geographical location and transaction or delivery channels (refer to the [*ML/TF/PF Institutional Risk Assessment Template*](#) on the FIC website). Insurance sector players are required to document their risk assessment and keep the risk assessments up to date. Further, insurance sector players are required to develop and implement mechanisms to manage or mitigate the risks identified.

5.2 RISK BASED APPROACH

The risk based approach (RBA) entails that the scope of applied measures for prevention and detection of ML/TF/PF should be proportional to the identified ML/TF/PF risks. The principle of the RBA therefore allows insurance sector players to focus resources where they are most needed to manage risks within the reporting entity's tolerance level.

In addition to risk assessment and risk mitigation activities, insurance sector players are expected to take measures to conduct on-going monitoring of financial transactions. The level of monitoring should be adapted according to the ML/TF/PF risks as outlined in the entity's risk assessment.

5.3 INTERNAL POLICIES, PROCEDURES AND CONTROLS

Insurance sector players should adopt policies indicating their commitment to comply with AML/CFTP obligations under the relevant Acts and regulations to prevent any transaction that facilitates ML/TF/PF activities. Every insurance sector player should formulate and implement internal policies, procedures and controls that will deter criminals from using its facilities for ML/TF/PF and to ensure that its obligations under the relevant laws and regulations are complied with. These internal policies, procedures and controls should cover Customer Due Diligence (CDD), record retention, the detection of unusual and suspicious transactions and the reporting obligations, among other things.

The AML/CFTP policies, procedures and controls should determine what kind of monitoring is done for particular high-risk activities, including how to detect suspicious transactions. The internal policies, procedures and controls should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

Section 44 (c) of the FIC Act provides for a penalty for failure to maintain internal controls. The provision states that a person who intentionally or negligently fails to maintain internal control programs commits an offence and is liable, upon conviction to a fine not exceeding five hundred thousand (500,000) penalty units or

to imprisonment for a period not exceeding five (5) years, or to both.

5.4 COMPLIANCE OFFICER

Insurance sector players should designate a Compliance Officer at management level within the organization, who will be responsible for managing the entity's AML/CFTP compliance program including filing of suspicious transaction reports (STRs) to the Centre. The designated Compliance Officer should be approved by the Centre and should be equipped with the relevant competence, authority and independence to implement the institution's AML/CFTP compliance program. The Compliance Officer should have ready access to all the books, records and employees of the reporting entity necessary to fulfil the responsibilities under the FIC Act.

An individual shall not be designated as a compliance officer unless that person—

- (a) Has two years' experience in the field of regulatory compliance;
- (b) Is not convicted of an offence under the FIC Act or any other written law and sentenced to a term of imprisonment of not less than six months without the option of a fine; and
- (c) Is certified and approved by the Centre.

The duties of the Compliance Officer include but are not limited to the following:

- i. Developing an AML/CFTP Compliance Program;
- ii. Receiving and vetting suspicious transaction reports from staff;
- iii. Filing suspicious transaction and currency transaction reports with the Centre;
- iv. Ensuring that the firm's compliance program is implemented;
- v. Coordinating the training of staff in AML/CFTP awareness, detection methods and reporting requirements; and
- vi. Serving both as a liaison officer with the Centre as well as a point-of-contact for all employees on issues relating to

AML/CFTP matters. The firm should ensure that the Compliance Officer has access to other information that may be of assistance in filing of suspicious or currency transaction reports.

The insurance sector player should ensure that the Compliance Officer has access to other information that may be of assistance in filing of suspicious or currency transaction reports.

It is important that the person designated as the Compliance Officer understands the operations of the insurance sector player to be able to develop effective internal controls that will mitigate the risks particular to that institution.

5.5 TRAINING

On-going employee training programs should be in place for all insurance sector players to ensure that:

- i. employees including management, board and committee members are kept informed of new developments, including information on current ML/TF/PF techniques, methods and trends; and
- ii. there is a clear explanation on the AML/CFTP laws and associated obligations.

The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the insurance sector player.

Insurance sector players should design, develop, implement and update the training program as appropriate to the nature and size of the business. An insurance sector player's training program must also be adapted to the ML/TF/PF risks it has identified. Further, the training should focus on the vulnerabilities and threats the entity is facing.

5.6 INDEPENDENT AUDIT

Putting the AML/CFTP compliance program in place is not enough. The program must be monitored and evaluated. The review can be conducted by an internal or external auditor.

Therefore, insurance sector players should have an independent audit performed by a person/people not involved with the entity's AML/CFTP compliance function to test compliance with the policies, procedures and controls. The individual(s) conducting the audit should report directly to the board of directors or to a designated committee. The audit should be documented and should include the specific areas reviewed by the auditor or the person conducting the review, and the recommendations that were put forth.

6.0 CUSTOMER DUE DILIGENCE

CDD is the identification and verification of both the customer and beneficial owner including but not limited to continuous monitoring of the business relationship with the reporting entity.

The FIC Act requires reporting entities to institute measures to ensure CDD at all times. Insurance sector players should conduct customer due diligence when:

- i. Establishing a business relationship with or conducting a business transaction for a customer;
- ii. Carrying out a cash transaction in an amount equal to, the kwacha equivalent of US\$10,000, whether denominated in Zambian kwacha or in foreign currency including where the transaction is carried out in a single transaction or several transactions that appear to be linked;
- iii. The Customer wishes to carry out a domestic or international wire transfer of monetary amounts in the amount equal to, or above, US\$1000 whether denominated in Zambian kwacha or in foreign currency;
- iv. There is a suspicion of ML/TF/PF;
- v. There are doubts about the veracity or adequacy of previously obtained customer identification data.

6.1 CUSTOMER DUE DILIGENCE PROCEDURES

(a) Insurance sector players should identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable,

independently sourced documents, such as a validly issued National Registration Card (NRC), Passport, Drivers' Licence, (which should not have expired at the time of conducting CDD), Certified Certificate of Incorporation or such other information as the Minister may prescribe;

(b) In respect of customers that are legal persons or legal arrangements, insurance sector players should:

- i. Verify any person purporting to have been authorised to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and
- ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from a recognised established body or similar evidence of establishment or existence and any other relevant information.

(c) Insurance sector players should, where applicable, identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is;

(d) Insurance sector players should in respect of all customers determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the sector player should take reasonable steps to obtain sufficient identification data and to verify the identity of that other person;

(e) Insurance sector players should take reasonable measures in respect of customers that are legal persons or legal arrangements to:

- i. Understand the ownership and control structure of such a client; and

- ii. Determine the natural persons that ultimately own or control the client. For trusts – the natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.
- (f) Insurance sector players should obtain information on the purpose and intended nature of the business relationship of their potential customers;
- (g) Insurance sector players should conduct ongoing due diligence on the business relationship with the customers. The ongoing due diligence includes scrutinizing the transactions undertaken by the customer throughout the course of the relationship to ensure that the transactions being conducted are consistent with the sector player's knowledge of the customer, its business and risk profiles, and the source of funds.
- (h) Insurance sector players should ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business relationships or customer categories.
- (i) In addition to the CDD requirements outlined above, insurance sector players are required to conduct CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated as provided under Section 16 (7) of the FIC Act and any other relevant written law.
- (j) Where insurance sector players are unable to comply with CDD requirements, they shall not open, commence business relations, perform transactions, and where appropriate, shall terminate the business relationship, and shall file a STR with the Centre in relation to the customer.

Section 44 (a) of the FIC Act provides for a penalty for failure to fulfil due diligence obligations. The provision states that a person who

intentionally or negligently fails to conduct due diligence with respect to customers, accounts and transactions commits an offence and is liable, upon conviction to a fine not exceeding five hundred thousand (500,000) penalty units or to imprisonment for a period not exceeding five (5) years, or to both.

6.2 HIGH-RISK CATEGORIES OF CUSTOMERS

Insurance sector players should have appropriate risk management systems to identify customers whose activities may pose a high risk of ML/TF/PF. In this regard, they are required to exercise enhanced identification, verification and ongoing due diligence procedures with respect to high risk customers. Insurance sector players should perform enhanced due diligence for high-risk categories of customers, business relationships or transactions.

Insurance sector players should, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a Prominent Influential Person (PIP).

Insurance sector players should obtain senior management approval before they establish a business relationship with a PIP. Where a customer has been accepted or has an ongoing relationship with the insurance sector player and the customer or beneficial-owner is subsequently found to be or becomes a PIP, an employee of a reporting entity is required to obtain senior management approval in order to continue the business relationship. The insurance sector player shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PIPs.

The risk management systems used by insurance sector players to identify customers whose activities may pose a high risk of ML/TF/PF should include:-

I. Enhanced identification which involves identifying clients or activities engaged in by clients who may pose high risk of money laundering or financing of terrorism by taking into account:

- a) the nature and business of customers;

- b) client activities, transaction patterns and operations;
- c) geographic location of the client and/or transaction
- d) the magnitude of client's assets that the insurance sector player handles;
- e) third parties that may be involved in the client's activities;
- f) where applicable, the beneficial ownership of an entity and their impact on risk;
- g) any other indicators that may be relevant.

II. Verification and on-going Due Diligence-should include:

- a. Seeking additional information beyond the minimum requirements under the law to substantiate the client's identity or the beneficial ownership of an entity and
- b. Obtaining additional information about the intended nature and value of a given transaction.

Where an insurance sector player determines that the risk of ML/TF/PF is low, the insurance sector player may apply simplified customer due diligence measures and take into consideration the risk factors outlined in the Second Schedule of the FIC (General) Regulations 2022. The insurance sector player, where it applies simplified customer due diligence measures, should prove the low risks to the satisfaction of the Centre or supervisory authority. Simplified measures should not be applied where there is a suspicion of ML/TF/PF.

7.0 WIRE TRANSFERS

Wire transfers are an important activity for reporting entities. Preventing and detecting ML/TF/PF requires reporting entities to know the originator and beneficiary of the transaction and where applicable, intermediary institutions.

With respect to wire transfers, the requirements set out under Regulations 6 (1) (6-30) of the Financial Intelligence (Prescribed Threshold) Regulations, Statutory Instrument No. 53 of 2022 apply to reporting entities.

8.0 SANCTION SCREENING

Sanctions screening is a control used in the detection, prevention and disruption of financial crimes. It is designed to identify targeted individuals or entities during on-boarding or the lifecycle of the customer relationship.

The Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 (as amended) and other domestic regulations prohibit reporting entities from entering in a business relationship or engaging in any transaction with a sanctioned person or entity on the United Nations Security Council (UNSC) sanctions list or local listing as established by the National Anti-Terrorism Centre (NATC). This therefore entails that insurance sector players should on a regular basis screen their customers (potential and existing) against these lists to ensure that they are not listed. Where there is a positive match, during screening of customers, insurance sector players should freeze the funds and other assets of the customer and should without delay report to the NATC and inform the supervisory authority and the Centre.

9.0 RECORD KEEPING

Reporting entities are required to keep adequate records as outlined in Section 22 of the FIC Act. Insurance sector players should maintain all books and records relating to their customers and transactions for a period of at least ten (10) years after the business relationship has ended or from the date of the transaction. The sector player should further ensure that the records and underlying information are available on a timely basis to the Centre, supervisory authority or other competent authority.

10.0 REPORTING OBLIGATIONS

10.1 CURRENCY TRANSACTION REPORTS (CTRs)

For cash transactions equal to or above USD 10,000.00, whether denominated in Zambian Kwacha or other currency, the insurance sector player is required to submit a Currency Transaction Report (CTR) to the Centre. This prescribed amount is a threshold and not a limit, which should trigger a report to the Centre within three (3) working days of the transaction, whether it is conducted as a single transaction or as several transactions that appear to be linked.

Insurance sector players are advised to submit subsequent CTRs on previously reported customers.

10.2 SUSPICIOUS TRANSACTION REPORTS (STRs)

(a) Obligation to Report Suspicious Transactions

Whenever an insurance sector player processes a transaction to which there are reasonable grounds to suspect that a property is the proceeds of crime, or is related to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism, it should take reasonable measures to ascertain the purpose of that transaction and submit a report to the Centre, setting out the suspicion, within three (3) working days of forming that suspicion. The STR should be submitted through the online reporting portal or physically delivered to the Centre. The designated Compliance Officer is responsible for the submission of STRs to the Centre.

Further, an insurance sector player is required to exercise caution when carrying out a transaction which it suspects to be related to ML/TF/PF. This may involve delaying the completion of the transaction while undertaking background checks on the customer. Where it is established that the transaction is linked to suspected ML/TF/PF this should trigger submitting of a STR to the Centre. The FIC Act also requires STRs to be submitted on attempted ML/TF/PF. Insurance sector players are advised to submit subsequent STRs on previously reported customers.

Section 45 of the FIC Act provides for a penalty for failure to submit a STR to the Centre. The provision states that a person who intentionally or negligently fails to submit a report to the Centre commits an offence and is liable, upon conviction to a fine not exceeding seven hundred thousand (700,000) penalty units or to imprisonment for a period not exceeding seven (7) years, or to both.

(b) Prohibition against Tipping Off

An insurance sector player or employee of an insurance sector player is not allowed to disclose to any person the contents of the

STR Form. Further, the disclosure of any other information from which a person could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made is prohibited.

Section 33 of the FIC Act provides for a penalty for tipping off. The provision states that a person who commits this offence is liable, upon conviction to a fine not exceeding five hundred thousand (500,000) penalty units or to imprisonment for a period not exceeding five (5) years, or to both.

(c) Protection of Identity of Persons and Information Relating to STRs

An insurance sector player is not allowed to disclose any information that identifies, or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction.

Section 47 of the FIC Act provides for a penalty for confidentiality violation. The provision states that a person who intentionally or negligently discloses such information to a customer or third party commits an offence and is liable, upon conviction to a fine not exceeding five hundred thousand (500,000) penalty units or to imprisonment for a period not exceeding five (5) years, or to both.

(d) Exemption from liability for good faith reporting of suspicious transactions

No civil, criminal, administrative or disciplinary proceedings for breach of banking or professional secrecy or contract shall be taken against an individual for submitting a completed STR form, in good faith, or in compliance with directions given by the FIC Act.

10.3 HOW TO IDENTIFY A SUSPICIOUS TRANSACTION IN THE SECTOR

Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with the customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about the customer and customer's business, to recognize that a transaction or series of transactions are unusual. In addition, the monitoring of

customer transactions helps to provide a clear picture of customer activity. Transaction monitoring involves manual or electronic scanning of transactions based on various parameters, including assessment of historical/current customer information and interactions. Transaction monitoring is a ML/TF prevention process and it helps to alert the reporting entity to any unusual business activities.

Reliance on what should be reported is largely on one's assessment, based on knowledge and experience, as well as specific circumstances of the transaction. The assessment should therefore be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour.

There are a number of indicators which may assist in the identification of potential ML/TF/PF activities. Although the existence of a single indicator does not necessarily indicate illicit activity, it should encourage further monitoring and examination.

In most cases, it is the existence of multiple indicators which raises a reporting entity's suspicion of potential criminal activity, and informs their response to the situation.

ML/TF/PF Indicators for Insurance Sector Players

The list below includes major indicators of ML/TF/PF in the sector and should be treated as a non-exhaustive guide:

- i. Unusually large single premiums or a series of large premium payments.
- ii. Unusual payment methods such as cash, cash equivalent or structured monetary instruments.
- iii. Customer uses an unknown intermediary to approach the insurance sector player
- iv. Customer performs activities that are irrelevant to his or her normal activities or profession and cannot provide a reasonable explanation;
- v. Customer repeatedly changes insurance sector providers within a short period of time without any reasonable explanation;

- vi. Customer is reluctant to discuss his or her financial affairs regarding behaviour that is inconsistent with his or her ordinary business practices;
- vii. Involve beneficiaries apparently unrelated to the client
- viii. Customer interested in a products early termination features than its investment performance
- ix. Customer who want to know how quickly and how much they can borrow or withdraw from permanent life insurance contracts
- x. Customers premiums are paid by a third party.
- xi. The transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- xii. The transaction involves designated persons;
- xiii. The transaction involves other financial institutions with known deficiencies in AML/CFTP controls or controls for combating proliferation financing;
- xiv. The transaction involves settlement instructions, including payment to apparently unconnected parties;
- xv. The transaction involves overpayment of premium with a request to refund the excess to a third party or an account held in a different country or jurisdiction;
- xvi. The transaction involves frequent taking out of policy loans that are repaid with large amounts of cash.

10.4 HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO THE CENTRE

The completed STR form by confidential cover, must be reported through the following means:

- i. On the Centre's e-system (applicable only to reporting entities with electronic link with the Centre);
- ii. Authenticated FIC email address (FICSTR@fic.gov.zm);
- iii. Hand delivered in two envelopes addressed to the Director General of the FIC and the inner envelop marked as STR.

11.0 OFFENCES BY BODY CORPORATE OR UNINCORPORATE

Section 52 of the FIC Act provides for an offence committed by a body corporate or unincorporated body. The Section states that where an offence under the FIC Act is committed by a body corporate or unincorporated body, every director or manager of the body corporate or unincorporated body shall be liable, upon conviction, as if the director or manager had personally committed the offence, unless the director or manager proves to the satisfaction of the court that the act constituting the offence was done without the knowledge, consent or connivance of the director or manager or that the director or manager took reasonable steps to prevent the commission of the offence.

12.0 MONITORING OF COMPLIANCE PROGRAM

The Centre will from time to time undertake on and off-site inspections of reporting entities to monitor how the AML/CFTP Compliance program is being implemented.

13.0 FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS

All the completed reports, correspondence or any queries should be sent to:

The Director General
Financial Intelligence Centre
P O Box 30481
Lusaka
ZAMBIA

ANNEXURE I GLOSSARY OF TERMS

Term	Definition
Attempted Transaction	Is one where a customer intended to conduct a transaction and took some form of action to do so. It is different from a simple request for information, such as an enquiry as to the price of a certain item. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.
Beneficial Owner	Means an individual- (a) who owns or effectively controls a client of a reporting entity, including the individual on whose behalf a transaction is conducted; or (b) who exercises effective control over a legal person or trust.
Control	<p>An individual is deemed to own or effectively control a client if the individual –</p> <ul style="list-style-type: none"> a) owns or controls, directly or indirectly , including through trusts or bearer shareholding for any legal person, twenty-five percent or more of the shares or voting rights of the entity; b) together with a connected person, owns or controls, directly or indirectly, including through trusts or bearer shareholding for any legal person, twenty-five percent or more of the shares or voting rights of the entity; c) despite a less than twenty-five percent shareholding or voting rights, receives a large percentage of the person's declared dividends; d) exercises control over the management of the person in that person's capacity as executive officer,

	non-executive director, independent non-executive director, director, manager or partner.
Competent Authority	For the purpose of these guidelines, a competent authority refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. This includes authorities that have Anti-Money Laundering)/Countering the Financing of Terrorism and Proliferation (AML/CFTP) supervisory or monitoring responsibilities aimed at ensuring compliance by accountable institutions with AML/CFTP requirements.
Financial Action Task Force (FATF)	Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
Funds or other assets	“funds or other assets” includes— (a) financial assets; (b) economic resources, oil and other natural resources; (c) property, whether tangible or intangible, or movable or immovable, however acquired; (d) legal documents or instruments in any form or manner evidencing title to, or interest in, the funds or other assets; (e) bank credits travelers cheques, bank cheques or money orders; (f) shares, securities or bonds; (g) drafts or letters of credit; (h) any interest, dividends or other

	<p>income accruing from, or generated by, the funds or other assets; and</p> <p>(i) any other assets which may potentially be used to obtain funds, goods or services.</p>
Money Laundering (ML)	<p>A money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of crime (e.g. money) knowing or believing that these were derived from the commission of a designated offence. Examples of designated offences include, drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation and tax crimes.</p>
Prominent Influential Person (PIP)	<p>An individual who is or has been entrusted with a prominent public function by a State or an international or local body or organization but is not of middle or junior ranking. Section 2 of the FIC Act No. 16 of 2020 provides detailed definition of a Prominent Influential Person.</p>
Proliferation Financing (PF)	<p>Section 2 of the Anti-Terrorism and Non Proliferation Act defines Proliferation Financing as an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including</p>

	technology, goods, software, services or expertise, in contravention of the Anti-Terrorism and Non-Proliferation Act or, where applicable, international obligations derived from relevant United Nations Security Council Resolutions.
Reporting Entity	An institution regulated by a Supervisory Authority and required to make a suspicious transaction report to the Centre on suspected Money Laundering, Terrorist Financing and other serious offences under the Act. They comprise financial service providers, designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs).
Supervisory Authority	For the purpose of these guidelines, Supervisory Authority refers to the PIA with the mandate to supervise and regulate the insurance sector players in Zambia.
Suspicious Transaction Report (STR)	Section 2 of the FIC Act defines a Suspicious Transaction Report as a report submitted on suspected or attempted money laundering, financing of terrorism or proliferation or any other serious offence whether in form of a data message or otherwise.
Terrorism Financing (TF)	Section 2 of the Anti-Terrorism and Non-Proliferation Act defines terrorism financing as an act by any person who, irrespective of whether a terrorist act occurs, by any means, directly or indirectly, willfully provides or collects funds or attempts to do so with the intention that the funds should be used or knowing that the funds are to be used in full or in part— (i) to carry out a terrorist act; (ii) by a terrorist; (iii) by a terrorist organisation; or (iv) for the travel of a

	<p>person to a State other than the person's State of residence or nationality for the purpose of perpetration, planning or preparation of, or participation in, terrorist act or the providing or receiving of terrorist training.</p>
<p>Wire transfer</p>	<p>Section 2 of the FIC Act defines a wire transfer as any transaction carried out on behalf of an originator, through a financial service provider or payment system including an institution that originates the wire transfer and an intermediary institution that participates in completion of the transfer, by electronic means, with a view to making an amount of money available to a beneficiary.</p>
<p>Without delay</p>	<p>Means within 24 hours</p>