Financial Intelligence Centre
Republic of Zambia

SUSPICIOUS TRANSACTIONS REPORTING GUIDELINES

Pensions and Insurance Sector

Contents

1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's financial institutions and other non-financial businesses and professions are not abused by persons involved in money laundering or the financing of terrorism, the Financial Intelligence Centre ('the Centre') was established to receive suspicious transaction reports from reporting entities, analyze and disseminate intelligence to law enforcement agencies (LEAs), pursuant to the Financial Intelligence Centre Act No 46 of 2010 ('the Act').

Prior to coming into effect of the Financial Intelligence Centre Act, 2010, Anti-Money Laundering/ Countering the Financing of Terrorism (AML/CFT) guidelines were issued pursuant to the Prohibition and Prevention of Money Laundering Act, No. 14 of 2001(PPMLA) which provided for the duties for the supervisory authorities such as the Pensions and Insurance Authority (PIA) to issue directives in 2011 to the regulated institutions under section 12(4) of the PPMLA.

It is the responsibility of the Centre to issue guidelines to reporting entities to ensure reporting entities comply accordingly with the provisions of the Financial Intelligence Centre Act, 2010. The purpose of these guidelines is to explain common reporting situations under the Financial Intelligence Centre Act, 2010 and assist the reporting entities (entities regulated by the Pensions and Insurance Authority i.e. pensions schemes and insurance businesses) to comply with the Financial Intelligence Centre Act, 2010.

These Suspicious Transaction Reports (STRs) Guidelines have been issued in accordance with section 56 and pursuant to section 29 of the Act. One of the cardinal responsibilities of reporting entities is to submit a suspicious

transaction report where there is suspicion that a transaction may arise from the commission of a crime or may be linked to the financing of terrorism. The directives that were issued by PIA in 2011 to the Industry will be revoked once the Centre issues the Financial Intelligence Centre General Regulations.

1.1 Overview of the Pensions and Insurance Sector

The Pensions and Insurance industry is composed of pension schemes, fund managers, fund administrators, reinsurance companies, long term insurance companies, general insurance companies, insurance brokers, insurance agents, claims agents, risk assessors, motor assessors and loss adjustors.

The Pensions and Insurance sector plays a fundamental role in the Zambian economy. A sound national 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 and pension sector to play fully its role in the economy.

The Pensions and 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 Pensions and 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 and TF in Zambia, the pension and insurance sector is subjected to the present Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime. The sector is regulated and supervised by the Pension and Insurance Authority (PIA).

The PIA's mission is to regulate the conduct of pension and insurance industry through prudential supervision in order to protect the interest of pension scheme members and insurance policyholders and to foster the industry's growth, development and stability.

1.2 Scope of the Guidelines

The Pensions Scheme and Insurance STR guidelines have incorporated essential elements of the Act, relevant FATF-Recommendations and other international best practices on AML/CFT regime. These guidelines cover among others the following key areas of AML/CFT policy; Customer due diligence, the AML/CFT Compliance programme; monitoring and responding to suspicious transactions. The STR Guidelines are provided as general information only and as such do not represent all the requirements under the law as the obligations imposed by the Supervisory Authority.

To this effect, the guidelines do not constitute legal advice and are not intended to replace the Act or any other guidelines, directives or regulations issued by Supervisory Authority for the Reporting Entities. Therefore, a Reporting Entity should also consult with its respective Supervisory Authority.

2.0 DEFINITION OF KEY TERMS

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 fee applicable to a certain transaction. 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.

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. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

Insurer: A company that carries on insurance business.

Insurance business: Means the business of issuing policies of insurance, and includes re-insurance business.

Insurance broker: Means a person who, not being an agent of the insurer and acting independently as to the choice of undertaking, in consideration for a commission or other compensation from the insurer:-

a) Brings together, with a view to the insurance or reinsurance of risks, persons seeking insurance or reinsurance undertaking;
b) Carry out work preparatory to the conclusion of contracts; and
c) Assists in the administration and performance of the contracts in particular in the event of collecting premiums and in the event of a claim.

Insurance agent: A person who, not being a salaried employee of an insurer:-

a) Initiates insurance business;
b) Does any act in relation to the receiving of proposals for insurance or the collection of premiums on behalf of the insurer.

Money Laundering: Under The Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious offence as defined in the Forfeiture of Proceeds of Crime Act, 2010. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation**.** A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

Pension Scheme: Scheme or arrangement other than a contract for life insurance, whether established by a written law for the time being in force or by any other instrument, under which persons are entitled to benefit in form payments, determined by age, length of service, amount of earnings or otherwise and payment primarily upon retirement, or upon death, termination of service, or upon the occurrence of such other event as maybe specified in such written law or other instrument.

Reporting Entity: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report under the Act. Examples of reporting entities include institutions supervised and regulated the Registrar of Pensions and Insurance appointed under Pension Scheme Regulations Act.

Supervisory Authority: For the purpose of these guidelines, a Supervisory Authority refers to the Pensions and Insurance Authority with mandate to supervise and regulate the pension schemes and insurance businesses sector in Zambia.

Terrorist Financing: Terrorist financing offences extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist. Under the Anti-Terrorism Act No. 21 of 2007, it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

3.0 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the reporting entity. Reporting Entities are not permitted to conduct any business transactions with an anonymous person whether natural of body corporate, or any institution whose identity is not ascertained.

Part III of the Act requires reporting entities to institute measures to ensure effective CDD at all times. Reporting Entities shall undertake measures when:

i. Establishing a business relationship with a customer

ii. Carrying out a transaction in an amount equal to, or above such amount as may be prescribed including where the transaction is carried out in a single operation or several operations that appear to be linked

iii. The Customer wishes to carry out a domestic or international wire transfer of monetary amounts in the amounts equal to, or above, the prescribed amount

iv. There is a suspicion of money laundering or terrorist financing

v. There are doubts about the veracity or adequacy of previously obtained customer identification data.

3.1 Customer Due Diligence Procedures

a. Reporting Entities shall 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, 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, reporting entities shall:

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. Reporting entities shall 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. Reporting entities shall 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 reporting entity shall take reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.

e. Reporting entities shall 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 customer; and

ii. Determine the natural persons that ultimately own or control the customer. For **trusts** – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries. Reporting entities should take appropriate measures to ascertain the source and control of funding of the trust.

f. Reporting entities shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

g. Reporting entities shall conduct ongoing due diligence on the business relationship as stated by the customers above.

h. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the financial institution/ customer relationship to ensure that the transactions being conducted are consistent with the reporting entities' knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

i. Reporting entities shall 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. All books and records with respect to its customers and transactions should be maintained for a period of at least 10 years;

3.2 High-Risk Categories of Customers

Section 19 of the Act requires reporting entities to have appropriate risk management systems to identify customers whose activities may pose a high risk of money laundering and financing terrorism. Reporting entities need to exercise enhanced identification, verification and ongoing due diligence procedures with respect to High Risk Customers. Reporting entities shall perform enhanced due diligence for high-risk categories of customers, business relationships or transactions. Examples of high-risk customer categories include:

a. Companies that have nominee-shareholders or shares in bearer form;

b. Non-resident customers;
c. Legal persons or legal arrangements such as trusts that are personal-assets holding vehicles;
d. Politically Exposed Persons (PEPs).

Reporting Entities shall, 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 PEP.

The risk management systems used by reporting entities to identify customers whose activities may pose a high risk of money laundering and financing of terrorism pursuant to section 19(a) of the Act shall require:-

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

   a. the nature and business of customers;
   b. customer activities, transaction patterns and operations;
   c. geographic location of the customer and/or transaction
   d. the magnitude of customer assets that a reporting entity handles;
   e. third parties that may be involved in the customer's activities;
   f. the beneficial ownership of an entity and their impact on risk;
   g. volume of cash used by customer in their transactions; and
   h. any other indicators that may be relevant.

II. **Verification and on-going Due Diligence**: Which includes:-

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

Reporting Entities shall obtain senior management approval before they establish a business relationship with PEP. Where a customer has been accepted or has an ongoing relationship with the reporting entity and the customer or beneficial-owner is subsequently found to be or becomes a PEP, the reporting entity shall obtain senior management approval in order to continue the business relationship.

Reporting entities shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PEPs and report all anomalies or unusual and abnormal transactions immediately to the Centre. Reporting Entities in business relationships with PEPs are required to conduct enhanced ongoing monitoring of that relationship.

4.0 THE ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT) COMPLIANCE PROGRAMME

An AML/CFT programme is an essential component of a reporting entity's compliance regime. The AML/CFT compliance programme should be risk-based, and should be designed to mitigate the Money Laundering and Terrorist Financing risks the reporting entity may encounter.

4.1 Elements of an AML/CFT Programme

4.1.1 A system of Internal Policies, Procedures and Controls

Reporting Entities shall adopt policies indicating its commitment to comply with AML/CFT obligations under the relevant Acts and regulations to prevent any transaction that facilitates ML/TF activities.

Every reporting entity shall formulate and implement internal rules procedures and other controls that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations under the relevant laws and regulations are always met. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

4.1.2 Compliance Officer

Reporting Entities should designate a Compliance Officer at in accordance with Section 23 (3) and such an officer shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. As it relates to the pensions business, the Compliance Officer will be expected to be at Fund Management of Fund Administration level. Each Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme. The Compliance Officer shall have ready access to all the books, records and employees of the reporting entity necessary to fulfil the responsibilities under the Act.

An employee of a reporting entity shall promptly report to a designated Compliance Officer all cases where:

a) the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that a customer has been or is involved in an illegal activity or crime; or
b) a customer in respect of whom the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that another customer has been engaging in illegal activities or crimes.

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

i. Developing an AML/CFT Compliance Programme;
ii. Receiving and vetting suspicious transaction reports from staff;
iii. Filing suspicious transaction reports with the Centre;
iv. Ensuring that the reporting entities' compliance programme is implemented;
v. Co-ordinating the training of staff in AML/CFT 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 money laundering and terrorist financing. Every reporting entity shall ensure that the Compliance Officer has access to other information that may be of assistance to the anti-money laundering reporting officer in consideration of a suspicious or unusual transaction.

A reporting entity shall cooperate with the Law enforcement Agencies to facilitate the exchange of information relating to money laundering and terrorist financing.

4.1.3 Training

The Act requires reporting entities to have formal, written AML/CFT Compliance programmes that include training. Ongoing employee training programs should be in place in all reporting entities to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting.

The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the reporting entity.

4.1.4 Independent Audit

Putting your AML/CFT Compliance programme in place is not enough. The programme must be monitored and evaluated. Therefore, reporting entities are supposed to have an independent audit performed by people not involved with the entity's AML/CFT Compliance staff to test compliance with the procedures, policies and controls. The individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors.

Monitoring of AML/CFT Compliance programme

The Financial Intelligence Centre will from time to time undertake on and off-site visits to reporting entities to monitor how the AML/CFT Compliance programmes are being implemented.

I. Obligation to Report Suspicious Transaction

Whenever a reporting entity processes a transaction to which there is reasonable grounds to suspect that any 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.

Further, a reporting entity is required to exercise caution when carrying out a transaction which it suspects to be related to money laundering or financing of terrorism. The Act also requires an STR to be submitted on attempted money laundering or financing of terrorism.

In exceptional cases (transactions that require immediate action), making a suspicious transaction report to the Centre does not prevent a reporting entity from reporting suspicions of money laundering or financing of terrorism directly to law enforcement agencies. The Centre encourages reporting entities to maintain established relationships with law enforcement agencies.

Failure to submit a suspicious transaction report to the Centre may lead to imprisonment upon conviction to a term of up to seven years or payment of a fine of seven hundred thousand penalty units or to both.

II. Prohibition against Tipping Off

A reporting entity is not allowed to disclose to any person the contents of the STR Form as well as that a report has been made or any other information from which the person whom the information is disclosed could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made. Any person who contravenes this requirement commits an offence and is liable to a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

III. Protection of identity of persons and information relating to STRs

A reporting entity 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. In light of the foregoing, the disclosure of identity of the above mentioned person is confidential. Section 47 of Act prohibits the disclosure of confidential information. Such disclosure is an offence which may result in a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

IV. Protection of entities/persons reporting

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

5.0 HOW TO IDENTIFY A SUSPICIOUS TRANSACTION

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

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 behavior.

5.1 ML/TF Indicators in the Pension and Insurance Sector

i. A customer who is reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information;
ii. Customer wants to use cash for a large transaction;
iii. Customer proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account;
iv. Customer requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;
v. Customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
vi. Customer conducts a transaction that results in a conspicuous increase in investment contributions;

vii. Scale of investment in insurance products is inconsistent with the Customer 's economic profile;

viii. Unanticipated and inconsistent modification of Customer 's contractual conditions, including significant or regular premium top-ups;

ix. Unforeseen deposit of funds or abrupt withdrawal of funds.

x. Involvement of one or more third parties in paying the premiums or in any other matters involving the policy;

xi. Overpayment of a policy premium with a subsequent request to refund the surplus to a third party;

xii. Funds used to pay policy premiums or deposits originate from different sources;

xiii. Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions;

xiv. Customer cancels investment or insurance soon after purchase;

xv. Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner;

xvi. Customer shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract;

xvii. The first (or single) premium is paid from a bank account outside the country;

xviii. Customer accepts very unfavourable conditions unrelated to his or her health or age;

xix. Unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual);

xx. The transfer of the benefit of a product to an apparently unrelated third party;

xxi. Transaction involves use and payment of a performance bond resulting in a cross-border payment;

xxii. Repeated and unexplained changes in beneficiary;

xxiii. Relationship between the policy holder and the beneficiary is not clearly established;

xxiv. The purchase of an insurance product inconsistent with the customer's needs;

xxv. A customer who shows little concern for the investment performance of a product/service but a great deal of concern about the early termination features of the product;

xxvi. Large cash sums deposited in Pension schemes by members of the scheme;

xxvii. Transfer of assets from unrelated third party into an investment portfolio;

xxviii. Insistence on depositing securities or other assets in an investment portfolio that would not normally be allowed by the scheme rules;

xxix. Unrelated third party paying contributions cash on behalf of a member of a pension scheme;

xxx. Unemployed persons paying contributions into an employee pension scheme;

xxxi. Customer who borrows the maximum amount available soon after purchasing the product;

6.0 HOW TO OBTAIN SUSPICIOUS TRANSACTION FORMS

You may obtain the STR forms by contacting the FIC office using the address provided under paragraph nine (9) of this document or emailing

fic@ficzambia.gov.zm. Further, an electronic copy of the STR form can be accessed on the FIC website (http/www.fic.gov.zm**)**.

7.0 HOW TO COMPLETE A SUSPICIOUS TRANSACTION REPORT

When completing an STR form, you MUST follow the instructions contained in the form and ensure that mandatory fields are duly completed.

8.0 HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO FIC

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

i. On the FIC e-system (applicable only to reporting institutions with electronic link with the FIC);
ii. Authenticated FIC email address provided for under six (6) of this document;
iii. Registered courier service providers using the address provided for in paragraph nine (9) below; and
iv. To be hand delivered to designated officials of the Monitoring and Analysis department of the Centre premises.

9.0 FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS

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

The Director
Financial Intelligence Centre
Plot 50L, Kudu Road, Kabulonga
P O Box 30481
Lusaka
ZAMBIA