Financial Intelligence Centre
Republic of Zambia

Suspicious Transactions Reporting Guidelines

Capital Markets Sector

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, pursuant to the Financial Intelligence Centre Act No. 46 of 2010 ('the Act').

It is the responsibility of the Centre to issue guidelines to reporting entities to ensure reporting entities comply accordingly with the provisions of the Act.

The purpose of these guidelines is to explain common reporting situations under the Financial Intelligence Centre Act and assist reporting entities under the supervision of SEC to comply with the Act. These Guidelines are provided as general information only and as such do not represent all the requirements under the law.

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.

1.1 Capital Markets Sector

The formation of the Securities and Exchange Commission (SEC) is part of the government's economic reform programme aimed at developing the financial and capital market in order to support and enhance private

sector initiatives. SEC is also an initiative to attract foreign portfolio investment through recognition of Zambia and the region as an emerging capital market with potentially high investment returns.

The Regulator of the Capital Markets in Zambia, SEC, is responsible for the supervision and development of the Zambian Capital Markets, as well as licensing, registration and authorization for financial intermediaries, issuers of debt and equity instruments and collective investment schemes. It aims to promote and maintain a strong and facilitative regulatory framework that ensures the orderly development of an innovative and competitive capital market for the secure, fair, efficient and transparent issuance and trading of securities in Zambia.

The capital market is an integral part of the financial markets where long-term financial instruments are traded. The importance of a well-functioning capital market cannot be overemphasized as it improves financial market efficiency and is the missing link in Zambia's long quest and search for economic development, sustainable economic growth and poverty reduction.

1.2 Establishing the Beneficial Owners of Companies

SEC should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information) that are investing in the country. SEC will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors. In addition, among other

checks, SEC should require registered entities to hold up-to-date information on the companies' beneficial owners.

1.3 Scope of the SEC STR Guidelines

SEC 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 SEC.

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.

Beneficial Owner: means *(a)* a natural person who ultimately owns or controls the rights to or benefits from property, including the person on whose behalf a transaction is conducted; or
(b) a person who exercises ultimate effective control over a legal person or legal arrangement;

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.

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.

Politically Exposed Persons (PEPs): Are individuals who are or have been entrusted with prominent public functions both in Zambia and foreign countries and those associated with them. For example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Middle ranking or more junior individuals are not categorised as PEPs.

Reporting Entity: "means an institution regulated by a Supervisory Authority and required to make a suspicious transaction report under the Act.

Supervisory Authority: For the purpose of these guidelines, Supervisory Authority refers to the the Securities and Exchange Commission, established

under the Securities Act. No. 354 of 1993.

Suspicious Transactions: Suspicious transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offence or commission of a terrorist activity financing offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering or terrorist activity financing offence.

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 operate an anonymous business relationship with customers.

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

iii. 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 the National Registration Card, Valid Passport, Valid Drivers' Licence, 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 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.

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 of 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).

e. 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.

f. 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.
c. 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 ML/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 Management level in accordance with Section 23 (3) and such an officer shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. 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.

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 and 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.

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 of completely or outside directors.

Monitoring of AML/CFT Compliance programme

The Financial Intelligence Centre in collaboration with the Supervisory Authority 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 or any director, partner, officer, principal or employee of the reporting entity 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.

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 of 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 a customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is having enough knowledge about your customer, and customers' business, and recognising 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 customers' business, financial history, background and behavior.

I. Specific ML/TF indicators for the Capital markets Sector

i. Acquiring of bonds and settlement of the bonds using large cash amounts;
ii. Foreign and national PEPs, investing in securities;
iii. Foreign nationals using locals to acquire securities;
iv. The use of unregistered or unlicensed securities businesses those are not accountable to the regulators.
v. Customer admits or makes statements about involvement in criminal activities;
vi. Customer uses aliases and a variety of similar but different addresses;
vii. Customer provided false information or information that you believe is unreliable;
viii. Customer offers money, gratuities or unusual favour for the provision of services that may appear unusual or suspicious;
ix. You are aware that a customer is the subject of a money laundering or terrorist financing investigation;
x. A new or prospective customer is known to you as having a questionable legal reputation or criminal background;
xi. Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reasons to exist).
xii. Changing share ownership in order to transfer wealth across borders;

xiii. Redeeming a long-term investment within a short period;

xiv. Opening multiple accounts or nominee accounts

xv. Using brokerage accounts as long term depository accounts for funds;

xvi. Effecting transactions involving nominees or third parties;

xvii. Engaging in market manipulation, e.g. "pump & dump" schemes; and

xviii. Engaging in 'boiler room' operations.

II. Unusual Financing Characteristics

i. Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or their financial ability;

ii. Customer attempts to purchase investments with cash;

iii. Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed;

iv. Customer wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments where the transaction is inconsistent with the normal investment practice of the customer or their financial ability;

v. Customer wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the customer;

vi. Customer frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the customer;

vii. Customer makes large or unusual settlements of securities in cash;

viii. The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading;

ix. Several customers open accounts within a short period of time to trade the same stock;

x. Customer is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party;

xi. Unrelated customers redirect funds toward the same account;

xii. Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;

xiii. Customer is willing to deposit or invest at rates that are not advantageous or competitive;

xiv. All principals of customer are located outside Zambia;

xv. Customer attempts to purchase investments with instruments in the name of a third party;

xvi. Payments made by way of third party cheques are payable to, or endorsed over to, the customer;

xvii. Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties;

xviii. Third-party purchases of shares in other names (i.e., nominee accounts);

xix. Transactions in which customers make settlements with cheques drawn by, or remittances from, third parties;

xx. Customer maintains bank accounts and custodian or brokerage accounts at offshore banking centres with no

explanation by customer as to the purpose for such relationships;

xxi. Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system; and

xxii. Customer uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the customer or their financial ability;

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 (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 paragraph six (6) of this document; and

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