Financial Intelligence Centre
Republic of Zambia

Suspicious Transactions Reporting Guidelines

Legal Professional 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 Act and assist the reporting entities (legal practitioners and notary publics) to comply with the Act.

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 Overview of the Legal Professionals Sector

For the purposes of these STR guidelines, legal professional refers to legal practitioners and notary public whether partners of firms or employed within law firms. Legal professionals provide a range of services and activities that differ vastly, such as in their methods of delivery and in the depth and duration of the relationships formed with Clients. Services provided to Clients may include but are not limited to:

i. Buying and selling of real estate.

ii. Managing of Client money, securities or other assets.

iii. Management of bank, savings or securities accounts.

iv. Organization of contributions for the creation, operation or management of companies.

v. Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

Services and activities undertaken by legal professionals are susceptible (both generally and particularly) to money laundering and terrorist financing due to issues of confidentiality and the principle of lawyer/Client privilege. In undertaking the services or activities, if legal professionals have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, they should report promptly to the Centre.

LAZ as a supervisory authority is expected to assist in the enforcement of the Act, through among other measures, the promulgation, in consultation with the Centre, directives to guide the legal profession in ensuring compliance with the Act.

1.2 Client Identification Requirements

Section 16 of the Act requires legal professionals including notary publics to identify Clients and verify the Client's identities by means of reliable and independent source documents or information. Under this section a lawyer is required to identify and verify the identity of each Client, and obtain other information before establishing a business relationship, or before carrying on further business, if the lawyer suspects money laundering,

financing of terrorism or any other serious offence or doubts the veracity or adequacy of previously obtained identification information. The requirement under this section creates an added obligation for identification of a potential Client, even where a referral has been made by another lawyer in good faith.

1.3 An STR and Legal Professional Privilege

Section 29(3) (a) of the Act obliges lawyers, notary publics to make suspicious transaction reports in relation to their Clients' transactions. This is by far the most important section that touches on legal professional privilege under the Act. The section further creates a specific exception to the requirement to make suspicious transaction reports. In particular section 29(3)(b) recognises the duties that lawyers have to their Clients by excluding information covered by legal professional privilege or professional secrecy from the obligation to file an STR.

1.4 Inapplicability of Confidentiality Provisions

Section 32 of the Act provides for the non-application of provisions in legislation relating to secrecy and confidentiality. Lawyers and notary publics are not bound by general secrecy provisions under the Act and any reports rendered to the Centre accordingly enjoy immunity from prosecution for breach of confidentiality. This provision is however different from the requirement to preserve lawyer and Client privilege. Please note that legal practitioners and notary publics who divulge information in accordance with the Act are not liable to any sanction as long as such disclosure is made in good faith and does not relate to privileged information.

1.5 Scope of the STR Guidelines

The STRs guidelines have incorporated essential elements of the Act, relevant FATF-Recommendations and other international best practices on AML/CFT regime. The FATF, the body which sets standards internationally for money laundering and financing of terrorism, in evaluating risks and vulnerable activities has found that lawyers are susceptible to being used not only in the layering and integration stages, as has been the case historically, but also as a means to disguise the origin of funds before placing them into the financial system. Lawyers are often the first professionals consulted for general business advice and on a wide range of regulatory and compliance issues.

These guidelines cover among others the following key areas of AML/CFT policy; Client 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 and 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, code of ethics issued by LAZ for the legal professionals. Therefore, Reporting Entities should also consult with LAZ on any regulatory or professional requirements.

2.0 DEFINITION OF KEY TERMS

Attempted Transaction: Is one where a Client 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 a reporting entity or the Client.

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.

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: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report under the Act. Examples of reporting entities include legal practitioners supervised by the Law Association of Zambia (LAZ).

Supervisory Authority: For the purpose of these guidelines, Supervisory Authority refers to LAZ with mandate to supervise and regulate the legal profession in Zambia.

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 CLIENT DUE DILIGENCE

Client Due Diligence (CDD) is the identification and verification of both the Client and beneficiary including but not limited to continuous monitoring of the business relationship with the reporting entity. Legal Practitioners are not permitted to conduct business transaction 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 (legal practitioners) to institute measures to ensure effective CDD at all times. Legal Practitioners shall undertake measures when:

i. Establishing a business relationship with a Client;

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 Client 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 Client identification data.

3.1 Client Due Diligence (CDD) Procedures

a. Reporting Entities shall identify their Clients (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the Clients' 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 Clients 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 Client 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 Clients determine whether or not a Client is acting on behalf of another person. Where the

Client 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 Clients 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. 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 Clients.

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

h. The ongoing due diligence above includes scrutinizing the transactions undertaken by the Client throughout the course of the financial institution/ Client relationship to ensure that the transactions being conducted are consistent with the reporting entities' knowledge of the Client, 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 Client categories. All books and records with respect to its Clients and transactions should be maintained for a period of at least 10 years;

3.2 High-Risk Categories of Clients

Section 19 of the Act requires reporting entities to have appropriate risk management systems to identify Clients 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 Clients. Reporting entities shall perform enhanced due diligence for high-risk categories of Clients, business relationships or transactions. Examples of high-risk Client categories include:

a. Companies that have nominee-shareholders or shares in bearer form;
b. Non-resident Clients;
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 Client or existing Client or the beneficial-owner is a PEP.

The risk management systems used by reporting entities to identify Clients 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 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 Clients;
b. Client activities, transaction patterns and operations;
c. geographic location of the Client and/or transaction
d. the magnitude of Client assets that a reporting entity handles;
e. third parties that may be involved in the Client's activities;
f. the beneficial ownership of an entity and their impact on risk;
g. volume of cash used by Client 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 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.

A reporting entity shall obtain senior management approval before they establish a business relationship with a PEP. Where a Client has been accepted or has an ongoing relationship with the reporting entity and the

Client 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 Clients 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 compliance 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

Legal Practitioners should designate a Compliance Officer (preferably a Managing Partner) who shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. The Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the entity'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 Client has been or is involved in an illegal activity or crime; or
b) a Client in respect of whom the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that another Client 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 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 TF 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 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 of banking or 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 Client's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is having enough knowledge about your Client, and Clients' 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 Clients' business, financial history, background and behavior.

5.1 Specific ML/TF Indicators for Legal Professionals Sector

i. Client uses an unknown intermediary to approach legal practitioner;
ii. Client wants to use foreign companies but does not seem to have a legitimate, legal or commercial reason for doing so;

iii. Client wishes to form or purchase a company with a corporate objective that is irrelevant to the Client's normal profession or activities without a reasonable explanation;

iv. Client performs activities that are irrelevant to his or her normal activities or profession and cannot provide a reasonable explanation;

v. Client repeatedly changes legal practitioners within a short period of time without any reasonable explanation;

vi. Client often transfers funds or securities to a third party;

vii. Client is reluctant to discuss his or her financial affairs regarding behaviour that is inconsistent with his or her ordinary business practices;

viii. Client has a history of changing bookkeepers or accountants yearly;

ix. Client is uncertain about location of company records;

x. Client is invoiced by organizations located in a country that does not have adequate money laundering laws and is known for high secretive banking and as a corporate tax haven;

xi. Third party is present for all transactions but does not participate in the actual transaction;

xii. Client uses gatekeepers (legal practitioners) to structure deposits and purchase real estate;

xiii. Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts;

xiv. Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table";

xv. Client purchases personal use property under corporate veil when this type of transaction is inconsistent with the ordinary business practice of the Client;

xvi. Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse);

xvii. Client purchases multiple properties in a short time period and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property;

xviii. Client insists on providing signature on documents by fax only;

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

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

xxi. Client is willing to deposit or invest at rates that are not advantageous or competitive;

xxii. Client's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved;

xxiii. Client seems unconcerned with terms of credit or costs associated with completion of a loan transaction; and

xxiv. Client frequently uses trust accounts for transactions where it may not make business sense to do so.

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 THE CENTRE

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;
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