




**Financial Intelligence Centre**

**Republic of Zambia**

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

**This document is authorized by:**

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

**Version Control:**

<b>Version</b>	<b>Date</b>	<b>Status</b>	<b>Author</b>
1.0	2019	Initial development of document	Compliance & Prevention Department
2.0	August 2023	First review	Compliance & Prevention Department

## Sector Guidelines for Law Firms – 2023

### 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 ANT-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION COMPLIANCE PROGRAM .....	5
5.1.	INSTITUTIONAL RISK ASSESSMENT .....	6
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 .....	9
6.0	CUSTOMER DUE DILIGENCE .....	9
6.1	CUSTOMER DUE DILIGENCE PROCEDURES .....	10
6.2	HIGH-RISK CATEGORIES OF CLIENTS .....	11
7.0	WIRE TRANSFERS .....	13
8.0	SANCTION SCREENING.....	13
9.0	RECORD KEEPING .....	14
10.0	REPORTING OBLIGATIONS .....	14
10.1	CURRENCY TRANSACTION REPORTS (CTRs).....	14
10.2	SUSPICIOUS TRANSACTION REPORTS (STRs) .....	14
(a)	Obligation to Report Suspicious Transactions.....	14
(b)	Prohibition against Tipping Off .....	16
(c)	Protection of Identity of Persons and Information Relating to STRs .....	17
(d)	Exemption from Liability for Good Faith Reporting of Suspicious Transactions .....	17
10.3	HOW TO IDENTIFY A SUSPICIOUS TRANSACTION IN THE SECTOR.....	17
10.4	HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO THE CENTRE.....	19
11.0	OFFENCES BY BODY CORPORATE OR UNINCORPORATE.....	19
12.0	MONITORING OF AML/CFTP COMPLIANCE PROGRAM.....	20
13.0	FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS.....	20
ANNEXURE I	GLOSSARY OF TERMS .....	21

## 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 law firms 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). 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 law firms to ML/TF/PF. To this end the FIC Act has created certain obligations for reporting entities operating in the legal practitioners' 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 the Anti-Money Laundering/ Countering the Financing of Terrorism and Proliferation (AML/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 law firms 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. These Guidelines are issued in consultation with the Law Association of Zambia (LAZ) for the purpose of ensuring a uniform application of AML/CFTP obligations by law firms.

## **3.0 SCOPE OF GUIDELINES**

The Guidelines have incorporated essential elements of the FIC Act, 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; client 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 represent all the requirements under the law. 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**

Under Section 2 of the FIC Act, law firms are included under DNFBPs, which are a category of reporting entities. The law recognizes legal practitioners, notaries and other independent legal professionals as reporting entities when they prepare for or carry out transactions relating to the following activities:

- a) Buying and selling of real estate;
- b) Managing of client money, securities or other assets;
- c) Management of bank, savings or securities accounts on behalf of clients;
- d) Organization of contributions for the creation, operation or management of companies;

- e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

The FIC Act further recognizes the LAZ as a supervisory authority for AML/CFTP purposes and legal practitioners in Zambia are regulated by the LAZ in as far as they are registered with the supervisory body. LAZ is established by the Law Association of Zambia Act, Chapter 31 of the Laws of Zambia. The role of LAZ in regulating legal practitioners is provided for in the Legal Practitioners Act, Chapter 30 of the Laws of Zambia and in summary includes:

- (i) to promote and regulate the practice and business of legal practitioners;
- (ii) to promote and maintain best standards and practices in the business of legal practitioners;
- (iii) to register members of the institute and persons qualified to be registered as legal practitioners and to maintain a register for both;
- (iv) to provide continuing education for its members; and
- (v) to regulate the professional conduct and discipline of legal practitioners.

Law firms are highly attractive to individuals seeking to launder criminal proceeds through various means such as the development and acquisition of real estate. Further, studies and ML/TF typologies indicate that the sector is vulnerable to potential ML through the abuse of client accounts. Law firms may accept large cash amounts from their clients which are later deposited into their client accounts at commercial banks.

## **5.0 THE ANT-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. These programs should be risk-based, and should be designed to mitigate the money laundering and terrorist financing risks the reporting entity may encounter.

### **5.1. INSTITUTIONAL RISK ASSESSMENT**

Law firms are required to take appropriate steps to identify, assess and understand their ML/TF/PF risks for clients, services or products, geographical location, transaction or delivery channels (refer to the [\*\*ML/TF/PF Institutional Risk Assessment Template\*\*](#) on the FIC website). Law firms are required to document the risk assessment and keep the risk assessment up to date. Further, law firms 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 law firms to focus resources where they are most needed to manage risks within the law firm's tolerance level.

In addition to risk assessment and risk mitigation activities, law firms 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**

Law firms 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. Law firms should formulate and implement policies, procedures and other controls that will deter criminals from using their facilities for ML/TF/PF and to ensure that their obligations under the relevant laws and regulations are complied with. These 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 law firm's policies, procedures and controls should determine what kind of monitoring is done for particular high-risk situations, including how to detect suspicious transactions. The 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**

Law firms should designate a Compliance Officer at management level within the organization, who will be responsible for managing the firm's AML/CFTP compliance program including filing of suspicious transaction reports (STRs) to the Centre. Where the lawyer is a sole practitioner, he or she shall designate himself/herself as the Compliance Officer. 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 law 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 law 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.

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

## **5.5 TRAINING**

Ongoing employee training programs should be in place in all law firms to ensure that:

- (i) employees including partners or sole practitioners 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 law firm.

The law firm should design, develop, implement and update its training program as appropriate to the nature and size of its business. A law firm's training program must also be adapted to the ML/TF/PF risks it has identified. Further the training should focus on the particular vulnerabilities and threats the firm 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, law firms should have an independent audit performed by a person/people not involved with the firm'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 partners or sole practitioner. The review should be documented and should include the specific areas reviewed by the expert or the person conducting the audit, and the recommendations that were put forth.

## 6.0 CUSTOMER DUE DILIGENCE

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 effective CDD at all times. Law firms should conduct customer due diligence when:

- i. Establishing a business relationship with or conducting a business transaction for a client;
- ii. Carrying out a cash transaction in an amount equal to, or above 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 client wishes to carry out a domestic or international wire transfer of monetary amounts equal to, or above, US\$1,000 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 client identification data.

## 6.1 CUSTOMER DUE DILIGENCE PROCEDURES

- a) Law firms should 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 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 clients that are legal persons or legal arrangements, law firms should :
  - i. verify any person purporting to have been authorized 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 a recognized established body or similar evidence of establishment or existence and any other relevant information.
- c) A law firm 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) A law firm should 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 law firm should take reasonable steps to obtain sufficient identification data and to verify the identity of that other person;
- e) Law firms should 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.

- f) A law firm should obtain information on the purpose and intended nature of the business relationship of their potential clients;
- g) A law firm should conduct ongoing due diligence on the business relationship with the clients. The ongoing due diligence includes scrutinizing the transactions undertaken by the client throughout the course of the relationship to ensure that the transactions being conducted are consistent with the law firm's knowledge of the client, its business and risk profiles, and the source of funds.
- h) Law firms 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 client categories.
- i) Where law firms 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 client.

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 CLIENTS**

Law firms should have appropriate risk management systems to identify clients 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 clients. Law firms should perform enhanced due diligence for high-risk categories of clients, business relationships or transactions.

Law firms should, 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 Prominent Influential Person (PIP).

Employees of law firms should obtain senior management approval before they establish a business relationship with a PIP. Where a client has been accepted or has an ongoing relationship with the law firm and the client or beneficial-owner is subsequently found to be or becomes a PIP, an employee of a law firm is required to obtain senior management approval in order to continue the business relationship. The law firm shall take reasonable measures to establish the source of wealth and the sources of funds of clients and beneficial-owners identified as PIPs.

The risk management systems used by law firms to identify clients whose activities may pose a high risk of ML/TF/PF 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 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 law firm 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 the law firm determines that the risk of ML/TF/PF is low, the firm may apply simplified CDD measures and take into consideration the risk factors outlined in the Second Schedule of the FIC (General) Regulations 2022. The law firm, where it applies simplified CDD 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 Centre (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 client 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 law firms should on a regular basis screen their clients (potential and existing) against these lists to ensure that

they are not listed. Where there is a positive match, during screening of clients, law firms should freeze the funds and other assets of the client 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. A law firm should maintain all books and records relating to its clients 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 law firm 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 law firm 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. Law firms are advised to submit subsequent CTRs on previously reported customers.

### **10.2 SUSPICIOUS TRANSACTION REPORTS (STRs)**

#### **(a) Obligation to Report Suspicious Transactions**

Whenever a law firm 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, a law firm 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 client. 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. Law firms are advised to submit subsequent STRs on previously reported customers.

Section 29 (1) of the FIC Act requires law firms to submit STRs when there are reasonable grounds to suspect that any property-

- a. is the proceeds of crime; or
- b. is related or linked to, or is to be used for, terrorism and proliferation or any other serious offence, relating to money laundering, financing of terrorism or proliferation terrorist acts or by terrorist organisations or persons who finance terrorism or proliferation or any other serious offence relating to money laundering, financing of terrorism or proliferation.

### **Exemptions for law firms from filing STRs**

Section 29 (3) of the FIC Act removes the requirement to file a STR, if that information is subject to legal privilege. Information is privileged if it is communicated or given to a law firm:

- i. By a client or representative of a client in connection to giving legal advice to a client;
- ii. By a person, or by a representative of a person seeking legal advice from a law firm;
- iii. By a person in contemplation of, or in connection of, legal proceedings; and for the purpose of those legal proceedings.

However, this exemption is overridden and does not apply if the information is communicated or given with a view to furthering any criminal purpose.



According to Section 29(3) of the FIC Act, a legal practitioner, a notary public or an accountant shall submit a report under Section 29(1) if—

- a. the legal practitioner, notary public or accountant engages, on behalf of or for a client, in a financial transaction associated with an activity specified in relation to such professionals under this Act; and
- b. the relevant information upon which the suspicion is based was not received from, or obtained on, a client—
  - i. in the course of ascertaining the legal position of the client; or
  - ii. in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

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**

A law firm or any, partner, or employee of the law firm is not allowed to disclose to any person the contents of the STR. 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**

A law firm 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 client 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 directives 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 client's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about the client and client's business, to recognize that a transaction or series of transactions are unusual. In addition, the monitoring of client transactions helps to provide a clear picture of client's activity. Transaction monitoring involves manual or electronic scanning of transactions based on various parameters, including assessment of historical/current client 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 client's business, financial history, background and behavior.

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 Law firms**

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

- i. Client uses an unknown intermediary to approach the law firm;
- 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 law firms 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 is uncertain about location of company records;
- ix. Client is invoiced by organizations located in a country that does not have adequate money laundering laws and is known for highly secretive banking and as a corporate tax haven;
- x. Third party is present for all transactions but does not participate in the actual transaction;

- xi. 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;
- xii. Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference under the table;
- xiii. The transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- xiv. The transaction involves designated persons<sup>1</sup>;
- xv. The transaction involves financial institutions with known deficiencies in AML/CFTP controls or controls for combating proliferation financing.

#### **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 Centre with 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

---

<sup>1</sup> A person or entity that is subject to targeted financial sanctions pursuant to the applicable United Nations Security Council Resolutions (UNSCRs) and listed on the UN sanctions list.

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 AML/CFTP COMPLIANCE PROGRAM**

The FIC will from time to time undertake on and off-site visits to 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
<b>Attempted Transaction</b>	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 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 client.
<b>Beneficial Owner</b>	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.
<b>Control</b>	<p>An individual is deemed to own or effectively control a client if the individual –</p> <p>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;</p> <p>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;</p> <p>c) despite a less than twenty-five percent shareholding or voting rights, receives a large percentage of the person's declared dividends;</p>

	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.
<b>Customer</b>	For the purpose of these guidelines customer includes clients
<b>Financial Action Task Force (FATF)</b>	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.
<b>Funds or other assets</b>	<p>"funds or other assets" includes—</p> <ul style="list-style-type: none"> <li>(a) financial assets;</li> <li>(b) economic resources, oil and other natural resources;</li> <li>(c) property, whether tangible or intangible, or movable or immovable, however acquired;</li> <li>(d) legal documents or instruments in any form or manner evidencing title to, or interest in, the funds or other assets;</li> <li>(e) bank credits travelers cheques, bank cheques or money orders;</li> <li>(f) shares, securities or bonds;</li> <li>(g) drafts or letters of credit;</li> <li>(h) any interest, dividends or other income accruing from, or generated by, the funds or other assets; and</li> <li>(i) any other assets which may potentially be used to obtain funds,</li> </ul>

	goods or services.
<b>Law Firms</b>	For the purpose of these guidelines 'law firms' refer to legal practitioners, notaries and other independent legal professionals
<b>Money Laundering (ML)</b>	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.
<b>Prominent Influential Person (PIP)</b>	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.
<b>Proliferation Financing (PF)</b>	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



	<p>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 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.</p>
<b>Reporting Entity</b>	<p>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).</p>
<b>Supervisory Authority</b>	<p>For the purpose of these guidelines, a Supervisory Authority refers to the Law Association of Zambia with the mandate to supervise and regulate the legal profession in Zambia.</p>
<b>Suspicious Transaction Report (STR)</b>	<p>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.</p>
<b>Terrorism Financing (TF)</b>	<p>Section 2 of the Anti-Terrorism and Non-Proliferation Act defines</p>

	<p>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 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>
<b>Wire transfer</b>	<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>
<b>Without delay</b>	<p>Means within 24 hours</p>