




**Financial Intelligence Centre**

**Republic of Zambia**

**ANTI-MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM AND  
PROLIFERATION (AML/CFTP) GUIDELINES FOR THE NON-BANK FINANCIAL  
INSTITUTIONS (NBFIs) SECTOR**

**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

## TABLE OF CONTENTS

1.0	INTRODUCTION.....	3
2.0	PURPOSE OF GUIDELINES .....	4
3.0	SCOPE OF GUIDELINES.....	4
4.0	OVERVIEW OF THE SECTOR .....	4
5.0	THE ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION COMPLIANCE PROGRAM .....	5
5.1.	INSTITUTIONAL RISK ASSESSMENT.....	5
5.2	RISK BASED APPROACH .....	5
5.3	INTERNAL POLICIES, PROCEDURES AND CONTROLS .....	6
5.4	COMPLIANCE OFFICER.....	6
5.5	TRAINING .....	7
5.6	INDEPENDENT AUDIT .....	8
6.0	CUSTOMER DUE DILIGENCE .....	8
6.1	CUSTOMER DUE DILIGENCE PROCEDURES .....	9
6.2	HIGH-RISK CATEGORIES OF CUSTOMERS.....	11
7.0	WIRE TRANSFERS .....	12
8.0	SANCTION SCREENING.....	13
9.0	RECORD KEEPING .....	13
10.0	REPORTING OBLIGATIONS .....	13
10.1	CURRENCY TRANSACTION REPORTS (CTRs).....	13
10.2	SUSPICIOUS TRANSACTION REPORTS (STRs) .....	14
(a)	Obligation to Report Suspicious Transactions.....	14
(b)	Prohibition against Tipping Off .....	14
(c)	Protection of Identity of Persons and Information Relating to STRs .....	15
(d)	Exemption from Liability for Good Faith Reporting of Suspicious Transactions .....	15
10.3	HOW TO IDENTIFY A SUSPICIOUS TRANSACTION IN THE SECTOR.....	15
10.4	HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO THE CENTRE .....	22
11.0	OFFENCES BY BODY CORPORATE OR UNINCORPORATE .....	23
12.0	MONITORING OF AML/CFTP COMPLIANCE PROGRAM.....	23
13.0	FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS .....	23
	ANNEXURE I GLOSSARY OF TERMS .....	24

## 1.0 INTRODUCTION

Money laundering (ML), terrorist financing (TF) and proliferation financing (PF) and 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 non-bank financial institutions (NBFIs<sup>1</sup>) 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 (the FIC Act) as amended. The Centre's core function is to receive, request, analyse suspicious transaction reports (STRs) and other disclosures for dissemination of financial intelligence reports to relevant competent authorities for investigation and prosecution where there are reasonable grounds to suspect that crimes have been committed.

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

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

---

<sup>1</sup> For the purpose of these Guidelines, NBFIs refer to financial institutions and financial businesses (except bureaux de change) licensed and supervised by the BoZ.

## **2.0 PURPOSE OF GUIDELINES**

The purpose of these Guidelines is to provide guidance for NBFIs regulated by the Bank of Zambia (BoZ) on their legal obligations to prevent and detect ML/TF/PF activities. In addition, the Guidelines will assist NBFIs to comply with the FIC Act.

The Guidelines are issued pursuant to Section 5(2)(i) and Section 56 of the FIC Act. The process of developing the Guidelines involved consultations with the BoZ for the purpose of ensuring a uniform application of AML/CFTP obligations by NBFIs.

## **3.0 SCOPE OF GUIDELINES**

The Guidelines have incorporated essential elements of the FIC Act, Banking and Financial Services Act No.7 of 2017 (BFSA), Financial Action Task Force (FATF) Recommendations and other international best practices on the AML/CFTP regime. They cover among others the following key areas of AML/CFTP policy; customer due diligence, the AML/CFTP compliance program, transaction monitoring and reporting obligations.

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

## **4.0 OVERVIEW OF THE SECTOR**

The BoZ has a statutory mandate to regulate and supervise NBFIs so as to promote the safe, sound and efficient operation and development of the financial sector. NBFIs are licensed and regulated in accordance with the provisions of the Banking and Financial Services Act (BFSA). In this regard, NBFIs are subject to prudential regulatory requirements so that they contribute to the overall soundness and stability of the financial system. NBFIs are also subject to non-prudential requirements that contribute to creating an environment of fairness, transparency and financial integrity.

Due to the increasing growth and sophistication of the financial products and services that NBFIs provide, they are susceptible to ML/TF/PF abuse.

Therefore, in order to protect NBFIs from criminal activities associated with ML/TF/PF, the sector is subjected to AML/CFTP requirements.

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

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

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

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

In addition to the risk assessment and risk mitigation activities, NBFIs 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**

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

The AML/CFTP policies, procedures and controls should determine what kind of monitoring is done for high-risk activities, 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 control programs. 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**

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

A NBFIs should not designate a person 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 STRs from staff;
- iii. Filing suspicious transaction and currency transaction reports with the Centre;
- iv. Ensuring that the NBFIs's compliance program is implemented;
- v. Co-ordinating 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 NBFIs 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 NBFIs to be able to develop effective internal controls that will mitigate the risks particular to that institution.

## **5.5 TRAINING**

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

- i. employees including management, board and committee members are kept informed of new developments, including



- information on current ML/TF/PF techniques, methods and trends; and
- ii. there is a clear explanation on the AML/CFTP laws and associated obligations.

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

A NBF should design, develop, implement and update its training program as appropriate to the nature and size of its business. The training program should also be adapted to the ML/TF/PF risks the NBF has identified. Further, the training should focus on the vulnerabilities and threats the institution 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, NBFs should have an independent audit performed by a person/people not involved with the entity's AML/CFTP compliance function to test compliance with the policies, procedures, and controls. The individuals conducting the audit should report directly to the board of directors or to a designated committee. The audit should be documented and should include the specific areas reviewed by the auditor or the person conducting the review, and the recommendations that were put forth.

## **6.0 CUSTOMER DUE DILIGENCE**

Customer Due Diligence 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 NBFs to institute measures to ensure CDD at all times. NBFs should conduct customer due diligence when:

- i. Establishing a business relationship with or conducting a business transaction for a customer;

- ii. Carrying out a cash transaction in an amount equal to 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 customer wishes to carry out a domestic or international wire transfer of monetary amounts in the amount equal to, or above, US\$1000 whether denominated in Zambian kwacha or in foreign currency;
- iv. There is a suspicion of ML/TF/PF;
- v. There are doubts about the veracity or adequacy of previously obtained customer identification data.

#### **6.1 CUSTOMER DUE DILIGENCE PROCEDURES**

- a) NBFIs should identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, such as a validly issued National Registration Card (NRC), Passport, Drivers' Licence, (which should not have expired at the time of conducting CDD), Certified Certificate of Incorporation or such other information as the Minister may prescribe;
- b) In respect of customers that are legal persons or legal arrangements, NBFIs should:
  - i. Verify any person purporting to have been authorised to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and
  - ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from a recognised established body or similar evidence of establishment or existence and any other relevant information.
- c) NBFIs 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) NBFIs should in respect of all customers, determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the institution should take reasonable steps to obtain sufficient identification data and to verify the identity of that other person;
- e) NBFIs should take reasonable measures in respect of customers that are legal persons or legal arrangements to:
  - i. Understand the ownership and control structure of such a 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) NBFIs should obtain information on the purpose and intended nature of the business relationship of their potential customers;
- g) NBFIs should conduct ongoing due diligence on the business relationship with the customers. The ongoing due diligence includes scrutinizing the transactions undertaken by the customer throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, its business and risk profiles, and the source of funds.
- h) NBFIs should ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business relationships or customer categories.
- i) Where NBFIs are unable to comply with CDD requirements, they shall not open, commence business relations, perform transactions, and where appropriate, shall terminate the business relationship, and shall file a STR with the Centre in relation to the customer.

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

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

## **6.2 HIGH-RISK CATEGORIES OF CUSTOMERS**

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

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

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

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

- 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's assets that the institution handles;
  - e. third parties that may be involved in the customer'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 – which should include:
- 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.

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

## **7.0 WIRE TRANSFERS**

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

With respect to wire transfers, the requirements set out under Regulations 6 (1) (6-30) of the Financial Intelligence 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 customer relationship.

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

## **9.0 RECORD KEEPING**

Reporting entities are required to keep adequate records as outlined in Section 22 of the FIC Act. NBFIs should maintain all books and records relating to their customers and transactions for a period of at least ten (10) years after the business relationship has ended or from the date of the transaction. The NBFIs 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 US\$10,000.00, whether denominated in Zambian Kwacha or other currency, the NBFIs are 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. NBFIs are advised to submit subsequent CTRs on previously reported customers.

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

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

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

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

### **(b) Prohibition against Tipping Off**

A NBFi or employee of a NBFi 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 NBFII is not allowed to disclose any information that identifies or is likely to identify the person who prepared or made a STR, or handled the underlying transaction.

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

**(d) Exemption from Liability for Good Faith Reporting of Suspicious Transactions**

No civil, criminal, administrative or disciplinary proceedings for breach of banking or professional secrecy or contract shall be taken against an individual for submitting a completed STR form, in good faith, or in compliance with 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 customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about the customer and customer's business, to recognize that a transaction or series of transactions are unusual. In addition, the monitoring of customer transactions helps to provide a clear picture of customer activity. Transaction monitoring involves manual or electronic scanning of transactions based on various parameters, including assessment of historical/current customer information and interactions. Transaction monitoring is a ML/TF prevention process



and it helps to alert the reporting entity to any unusual business activities.

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

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

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

#### **ML/TF/PF indicators for NBFIs**

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

- i. Customer conducts transactions at different physical locations in an apparent attempt to avoid detection;
- ii. Customer repeatedly uses one particular address but frequently changes the names involved;
- iii. Customer is accompanied and watched;
- iv. Customer shows uncommon curiosity about internal systems, controls and policies;
- v. Customer has only vague knowledge about the amount of a deposit;
- vi. Customer presents confusing details about the transaction or knows few details about its purpose;
- vii. Customer over justifies or explains the transaction;
- viii. Customer is secretive and reluctant to meet in person;
- ix. Customer is nervous when conducting the transaction;
- x. Normal attempts to verify the background of a new or prospective customer are difficult;

- xi. Customer appears to be acting on behalf of a third party, but does not tell you;
- xii. Customer insists that a transaction be done quickly;
- xiii. Inconsistencies appear in the customer's presentation of the transaction;
- xiv. The transaction does not appear to make sense or is out of the usual or expected activity for the customer;
- xv. Customer appears to have recently established a series of new relationships with different financial entities;
- xvi. Customer attempts to develop close rapport with staff;
- xvii. Customer uses aliases and a variety of similar but different addresses;
- xviii. Customer spells his or her name differently from one transaction to another;
- xix. Customer provided false information or information that you believe is unreliable;
- xx. Customer offers money, gratuities, or unusual favour for the provision of services that may appear unusual or suspicious;
- xxi. Customer pays for services or products using financial instruments, such as money orders or traveller's cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes;
- xxii. You are aware that a customer is the subject of a money laundering or terrorist financing investigation;
- xxiii. A new or prospective customer is known to you as having a questionable legal reputation or criminal background;
- xxiv. Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations, or other reasons to exist);
- xxv. Customer attempts to convince an employee not to complete any documentation required for the transaction;
- xxvi. Customer is quick to volunteer that funds are "clean" or "not being laundered";
- xxvii. Customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds;
- xxviii. Customers who frequently seek to exchange large quantities of low denomination notes for those of higher denomination;

- xxix. Customer who uses notes in denominations that are unusual for the customer, when the norm in that business is different;
- xxx. The use of multiple accounts to collect and then channel funds to a small number of foreign beneficiaries, particularly when these are in locations of specific concern;
- xxxi. Customer consistently makes cash transactions that are just under the reporting threshold amount in an attempt to avoid the reporting threshold or in an attempt to avoid triggering the identification and reporting requirements;
- xxxii. Customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers draft, etc;
- xxxiii. Shared address or phone numbers for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc);
- xxxiv. Stated occupation of the customer is not in line with the level of or type of activity;
- xxxv. Attempting to open or operating accounts under a false name;
- xxxvi. Funds being deposited into several accounts, consolidated into one and transferred outside the country;
- xxxvii. Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers;
- xxxviii. Customer provides doubtful or vague information;
- xxxix. Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate;
- xl. Customer refuses to produce personal identification documents;
- xli. Customer only submits copies of personal identification documents;
- xlii. Customer wants to establish identity using something other than his or her personal identification documents;
- xliii. All identification presented is foreign or cannot be checked for some reason;

- xliv. All identification documents presented appear new or have recent issue dates;
- xlvi. Any dealing with an agent where the identity of the ultimate beneficiary is undisclosed, contrary to normal procedure for the type of business concerned;
- xlvi. Customers who repay problem loan unexpectedly;
- xlvi. Customer gives power of attorney to a non-relative to conduct large transactions;
- xlvi. Customer acquires significant assets and liquidates them quickly with no explanation;
- xlix. Customer acquires significant assets and encumbers them with security interests that do not make economic sense;

In addition to the foregoing indicators, reporting entities involved in the business of electronic funds transfers (EFTs) or the remittance or transmission of funds or wire transfers, should consider the following indicators:

- i. Customer is reluctant to give an explanation for the remittance;
- ii. Customer orders wire/electronic transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements;
- iii. Customer transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash;
- iv. Customer receives large sums of money from an overseas location and the transfers include instructions for payment in cash;
- v. Customer makes frequent or large funds transfers for individuals or entities that have no account relationship with the customer's institution;
- vi. Customer receives frequent funds transfers from individuals or entities who have no account relationship with the customer's institution;
- vii. Customer instructs you to transfer funds abroad and to expect an equal incoming transfer. Immediately after transferred funds have cleared, the customer moves the funds to another account or to another individual or entity;

- viii. Customer shows unusual interest in funds transfer systems and questions the limit of what amount can be transferred;
- ix. Large incoming wire/electronic transfers from foreign jurisdictions are withdrawn immediately by company principals;
- x. Customer sends frequent wire/electronic transfers to foreign countries, but does not seem to have connection to such countries;
- xi. Wire/electronic transfers are received from entities having no apparent business connection with customer;
- xii. Several customer s requesting transfers share common identifiers, such as family name, address or telephone number;
- xiii. Several different customer's send transfers that are similar in amounts, sender names, test questions, free message text and destination country;
- xiv. Stated occupation of the customer or the customer's financial standing is not in line with the level or type of activity (for example a student or an unemployed individual who receives or sends large amounts of wire/electronic transfers);
- xv. Migrant remittances made outside the usual remittance corridors;
- xvi. Customer requests transfers to a large number of recipients outside Zambia who do not appear to be family members;
- xvii. Customer does not appear to know the recipient to whom he or she is sending the transfer;
- xviii. Customer does not appear to know the sender of the transfer received;
- xix. Beneficiaries of wire/electronic transfers involve a large group of nationals of countries associated with terrorist activity;
- xx. Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices;
- xxi. Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then channel

funds immediately or after a short time to a small number of foreign beneficiaries.

Reporting entities involved in the business of providing loans (including mortgages) or extending credit to individuals or corporations, should consider the following indicators:

- i. Customer suddenly repays a problem loan unexpectedly;
- ii. Customer makes a large, unexpected loan payment with unknown source of funds, or a source of funds that does not match what you know about the customer;
- iii. Customer repays a long-term loan, such as a mortgage, within a relatively short time period;
- iv. Source of down payment is inconsistent with borrower's background and income;
- v. Down payment appears to be from an unrelated third party;
- vi. Customer offers you large deposits or some other form of incentive in return for favourable treatment of loan request;
- vii. Customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known;
- viii. The loan transaction does not make economic sense (for example, the customer has significant assets, and there does not appear to be a sound business reason for the transaction);
- ix. Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction;
- x. Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the customer ; and
- xi. Down payment or other loan payments are made by a party who is not a relative of the customer.

Reporting entities involved in Money Services Businesses should consider the following in addition to the other indicators outlined in the other previous paragraphs:

- i. Customer requests a transaction at a foreign exchange rate that exceeds the posted rate;
- ii. Customer wants to pay transaction fees that exceed the posted fees;
- iii. Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument;
- iv. Customer wants cash converted to a cheque and you are not normally involved in issuing cheques;
- v. Customer instructs that funds are to be picked up by a third party on behalf of the payee;
- vi. Customer requests numerous cheques in small amounts and various names, which total the amount of the exchange;
- vii. The transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- viii. The transaction involves designated persons;

#### **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); or
- iii. Hand delivered in two envelopes addressed to the Director General of the Centre and the inner envelop marked as STR.

## **11.0 OFFENCES BY BODY CORPORATE OR UNINCORPORATE**

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

Other supervisory sanctions may apply where NBFIs are found to be non-compliant with specific requirements in other applicable laws.

## **12.0 MONITORING OF AML/CFTP COMPLIANCE PROGRAM**

The Centre and the BoZ will, from time to time, undertake on and off-site inspections of NBFIs to monitor how their 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 customer intended to conduct a transaction and took some form of action to do so. It is different from a simple request for information, such as an enquiry as to the price of a certain item. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.
<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> <p>d) exercises control over the management of the person in that</p>

	<p>person's capacity as executive officer, non-executive director, independent non-executive director, director, manager or partner.</p>
<b>Competent Authority</b>	<p>For the purpose of these guidelines, a competent authority refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. This includes authorities that have Anti-Money Laundering)/Countering the Financing of Terrorism and Proliferation (AML/CFTP) supervisory or monitoring responsibilities aimed at ensuring compliance by accountable institutions with AML/CFTP requirements.</p>
<b>Financial Action Task Force (FATF)</b>	<p>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.</p>
<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 travellers cheques, bank cheques or money orders;</li> <li>(f) shares, securities or bonds;</li> <li>(g) drafts or letters of credit;</li> </ul>

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

	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.
<b>Reporting Entity</b>	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).
<b>Supervisory Authority</b>	For the purpose of these guidelines, Supervisory Authority refers to the BoZ that has the mandate to supervise and regulate NBFIs in Zambia.
<b>Suspicious Transaction Report (STR)</b>	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.
<b>Terrorism Financing (TF)</b>	Section 2 of the Anti-Terrorism and Non-Proliferation Act defines terrorism financing as an act by any person who, irrespective of whether a terrorist act occurs, by any means, directly or indirectly, wilfully 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

	<p>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>
<p><b>Wire transfer</b></p>	<p>Section 2 of the FIC Act defines a wire transfer as any transaction carried out on behalf of an originator, through a financial service provider or payment system including an institution that originates the wire transfer and an intermediary institution that participates in completion of the transfer, by electronic means, with a view to making an amount of money available to a beneficiary.</p>
<p><b>Without delay</b></p>	<p>Means within 24 hours.</p>