Financial Intelligence Centre

Republic of Zambia

Suspicious Transactions Reporting Guidelines

Non-Bank Financial Institutions

Contents

1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's financial institutions and other non-financial businesses and professions are not abused by persons involved in money laundering or the financing of terrorism, the Financial Intelligence Centre ('the Centre') was established to receive suspicious transaction reports from reporting entities, analyze and disseminate intelligence to law enforcement agencies, 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 (Non-Bank Financial Institutions and Businesses) 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 Non-Bank Financial Institutions and Businesses (NBFIs)

For the purpose of these STR guidelines, Non-Bank Financial Institutions and Businesses (NBFIs) refer to financial institutions which provide financial services including but not limited to: mortgage financing; consumer financing; cheque cashing; micro-credit financing; money services business; financial leasing or finance leasing; money or value transfer services. e.g. mobile money providers; the issuance and administration of

credit cards, debit cards, travelers' cheques or bankers' drafts and merchant banking services.

1.2 Vulnerability of NBFIs to Money Laundering/Terrorist Financing (ML/TF)

Due to the nature of the products and services provided by NBFIs and increasing growth and sophistication of the products this sector is attractive to money launderers and terrorist financiers. Transactions performed by other NBFIs such as money or value transfer services can involve one or more intermediaries and a third party final payment. Therefore, in order to protect the financial sector from criminal activities associated with ML and TF, the sector is subjected to the present Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime. The sector is regulated and supervised by the Bank of Zambia.

1.3 Scope of the STR Guidelines

The Non-Bank Financial Institutions and Businesses (NBFIs) STR guidelines have incorporated essential elements of the Act, relevant FATF Recommendations and other international best practices on AML/CFT regime. These guidelines cover among others the following key areas of AML/CFT policy; Customer due diligence, the AML/CFT Compliance programme; monitoring and responding to suspicious transactions.

The STR Guidelines are provided as general information only and as such do not represent all the requirements under the law as the obligations imposed by the Supervisory Authority. To this effect, the guidelines do not constitute legal advice and are not intended to replace the Act or any other guidelines, directives or regulations issued by BoZ for the Reporting Entities.

Therefore, Reporting Entities should also consult with BoZ on any regulatory or professional requirements.

2.0 DEFINITION OF KEY TERMS

Attempted Transaction: is one where a customer intended to conduct a transaction and took some form of action to do so. It is different from a simple request for information, such as an enquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.

Financial Action Task Force (FATF): Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

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, No. 19 of 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: 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 all institutions supervised and regulated by the Bank of Zambia (BOZ).

Supervisory Authority: For the purpose of these Guidelines, supervisory authority means the Bank of Zambia established under the Bank of Zambia Act, No. 43 of 1996.

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

Terrorist Financing: Terrorist financing offences extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist. Under the Anti-Terrorism Act No. 21 of

2007, it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

3.0 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the reporting entity. Reporting Entities are not permitted to operate anonymous accounts or accounts in fictitious names.

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

i. Opening an account for, or otherwise establishing a business relationship with a customer

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

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

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

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

3.1 Customer Due Diligence Procedures

a. Reporting Entities shall identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, such as a validly issued National Registration Card, Passport, Drivers' Licence, (which should not have expired at the time of conducting CDD) Certified Certificate of Incorporation or such other information as the Minister may prescribe.

b. In respect of customers that are legal persons or legal arrangements, reporting entities shall:

   i. verify any person purporting to have been authorised to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and

   ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from a recognised established body or similar evidence of establishment or existence and any other relevant information.

c. Reporting entities shall identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is.

d. Reporting entities shall in respect of all customers determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the reporting entity shall take reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.

e. Reporting entities shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:

   i. Understand the ownership and control structure of such a customer; and

   ii. Determine the natural persons that ultimately own or control the customer. For **trusts** – The natural persons are the settlor, the trustee, the beneficiary and other person exercising effective control over the trust and the beneficiaries.

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

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

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

i. Reporting entities shall ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of high-risk business relationships or customer categories. All books and records with respect to its customers and transactions should be maintained for a period of at least 10 years;

3.2 High-Risk Categories of Customers

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

a. Companies that have nominee-shareholders or shares in bearer form;
b. Non-resident customers;
c. Legal persons or legal arrangements such as trusts that are personal-assets holding vehicles;
d. Politically Exposed Persons (PEPs)
e. Reporting Entities shall, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a PEP.
f. The risk management systems used by reporting entities to identify customers whose activities may pose a high risk of money laundering

and financing of terrorism pursuant to section 19(a) of the Act shall require:-

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

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

ii. **Verification and on-going Due Diligence**-which includes:

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

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

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

3.3 Non Face-to-Face Identification

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch.

a. Due to possible false identities and impersonations that can arise with non-face-to face customers, it is important to ensure that the applicant is who he/she claims to be. Accordingly, at least one additional measure or check should be undertaken to supplement the documentary or electronic evidence. These additional measures will apply whether the applicant is resident in Zambia or elsewhere and must be particularly robust where the applicant is requiring a bank account or other product/ service that offers money transmission or third party payments.

b. Procedures to identify and authenticate the customer have to ensure that there is sufficient evidence either documentary or electronic to confirm his address and personal identity and to undertake at least one additional check to guard against impersonation or fraud.

c. The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk. However, care must be taken to ensure that

the same level of information is obtained for internet customers and other postal/telephone customers.

d. If reliance is being placed on intermediaries to undertake the processing of applications on the customer's behalf, checks should be undertaken to ensure that the intermediaries are regulated for anti-money laundering prevention and that the relevant identification procedures are applied. In all cases, evidence as to how identity has been verified should be obtained and retained with the account opening records.

e. NBFIs shall conduct regular monitoring of internet-based business/customers. If a significant proportion of the business is operated electronically, computerized monitoring systems/solutions that are designed to recognize unusual transactions and related patterns of transactions should be put in place to recognize suspicious transactions.

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

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

4.1 Elements of an AML/CFT Programme

4.1.1 A System of Internal Policies, Procedures and Controls

Reporting Entities shall adopt policies indicating its commitment to comply with AML/CFT obligations under the relevant Acts and regulations to

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

4.1.2 Compliance Officer

Reporting Entities should designate a Compliance Officer who shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. Each Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme. The Compliance Officer shall have ready access to all the books, records and employees of the reporting entity necessary to fulfil the responsibilities under the Act.

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

(a) the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that a customer has been or is involved in an illegal activity or crime; or

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

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

i. Developing an AML/CFT Compliance Programme;
ii. Receiving and vetting suspicious transaction reports from staff;
iii. Filing suspicious transaction reports with the Centre;
iv. Ensuring that the reporting entities' compliance programme is implemented;
v. Co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements; and
vi. Serving both as a liaison officer with the Centre a point-of-contact for all employees on issues relating to money laundering and terrorist financing. Every reporting entity shall ensure that the Compliance Officer has access to other information that may be of assistance to the anti-money laundering reporting officer in consideration of a suspicious or unusual transaction.

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

4.1.3 Training

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

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

4.1.4 Independent Audit

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

Monitoring of AML/CFT Compliance programme

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

I. Obligation to Report Suspicious Transaction

Whenever a reporting entity processes a transaction to which there is reasonable grounds to suspect that any property is the proceeds of crime, or is related to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism, it should take reasonable measures to ascertain the purpose of that transaction and submit a report to the Centre, setting out the suspicion, within three (3) working days of forming that suspicion.

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

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

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

II. Prohibition against Tipping Off

A reporting entity or any director, partner, officer, principal or employee of the reporting entity is not allowed to disclose to any person the contents of the STR Form. Further, the disclosure of any other information from which a person could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made is prohibited.
Any person who contravenes this requirement commits an offence and is liable to a fine of up to 500,000 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 your customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about your customer and customer's business, to recognize that a transaction or series of transactions are unusual.

Reliance on what should be reported is largely on one's assessment, based on knowledge and experience, as well as specific circumstances of the transaction. The assessment should therefore be based on a reasonable

evaluation of relevant factors, including the knowledge of the customers business, financial history, background and behavior.

Money Laundering/Terrorist Financing Indicators for NBFIs

i. Customer admits or makes statements about involvement in criminal activities;
ii. Customer appears to have accounts with several financial institutions in one area for no apparent reason;
iii. Customer conducts transactions at different physical locations in an apparent attempt to avoid detection;
iv. Customer repeatedly uses an address but frequently changes the names involved;
v. Customer is accompanied and watched;
vi. Customer shows uncommon curiosity about internal systems, controls and policies;
vii. Customer has only vague knowledge of the amount of a deposit;
viii. Customer presents confusing details about the transaction or knows few details about its purpose;
ix. Customer over justifies or explains the transaction;
x. Customer is secretive and reluctant to meet in person;
xi. Customer is nervous, not in keeping with the transaction;
xii. Customer is involved in transactions that are suspicious but seems blind being involved on money laundering activities;
xiii. Normal attempts to verify the background of a new or prospective customer are difficult;
xiv. Customer appears to be acting on behalf of a third party, but does not tell you;

xv. Customer is involved in activity unusual for that individual or business;

xvi. Customer insists that a transaction be done quickly;

xvii. Inconsistencies appear in the customer's presentation of the transaction;

xviii. The transaction does not appear to make sense or is out of keeping with usual or expected activity for the customer;

xix. Customer appears to have recently established a series of new relationships with different financial entities;

xx. Customer attempts to develop close rapport with staff;

xxi. Customer uses aliases and a variety of similar but different addresses;

xxii. Customer spells his or her name differently from one transaction to another;

xxiii. Customer provided false information or information that you believe is unreliable;

xxiv. Customer offers money, gratuities or unusual favor for the provision of services that may appear unusual or suspicious;

xxv. Customer pays for services or products using financial instruments, such as money orders or traveler's cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes;

xxvi. You are aware that a customer is the subject of a money laundering or terrorist financing investigation;

xxvii. A new or prospective customer is known to you as having a questionable legal reputation or criminal background; and

xxviii. Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reasons to exist).

xxix. customer attempts to convince an employee not to complete any documentation required for the transaction;

xxx. customer makes inquiries that would indicate a desire to avoid reporting;

xxxi. customer has unusual knowledge of the law in relation to suspicious transaction reporting;

xxxii. customer seems very conversant with money laundering or terrorist financing activity issues;

xxxiii. customer is quick to volunteer that funds are "clean" or "not being laundered;

xxxiv. customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds;

xxxv. customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds;

xxxvi. Customers who frequently seek to exchange large quantities of low denomination notes for those of higher denomination;

xxxvii. Customer who uses notes in denominations that are unusual for the customer , when the norm in that business is different;

xxxviii. Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g. countries designated by national authorities or FATF as non-cooperative countries);

xxxix. The opening of accounts of financial institutions for persons from locations of specific concern;

xl. Sending and receiving funds by international transfers from and or to locations of specific concern;

xli. 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;

xlii. 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;

xliii. Customer makes cash transactions of consistently rounded off large amounts;

xliv. Customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers draft, etc

xlv. Customer frequently purchases traveler's cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity of the customer;

xlvi. Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer;

xlvii. 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);

xlviii. Stated occupation of the customer is not in keeping with the level or type of activity;

xlix. Unexplained transfers between multiple accounts with no rationale;

l. Customers who wish to maintain a number of trustee accounts which do not appear consistent with the type of business;

li. Activity in accounts inconsistent with what would be expected from declared business;

lii. Unusual activity in accounts compared to past transactions;

liii. Opening accounts when the customer's address is outside the local service area;

liv. Opening accounts with names very close to other established business entities;

lv. Attempting to open or operating accounts under a false name;

lvi. Funds being deposited into several accounts, consolidated into one and transferred outside the country;

lvii. Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers;

lviii. unexplained transfers between the customer 's products and accounts;

lix. Customer provides doubtful or vague information;

lx. Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate;

lxi. Customer refuses to produce personal identification documents;

lxii. Customer only submits copies of personal identification documents;

lxiii. Customer wants to establish identity using something other than his or her personal identification documents;

lxiv. All identification presented is foreign or cannot be checked for some reason;

lxv. All identification documents presented appear new or have recent issue dates;

lxvi. Customer presents different identification document each time a transaction is conducted;

lxvii. Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customers usual business;

lxviii. Building up large balances, not consistent with the known turnover of the customers' business and subsequent transfer to account(s) held overseas;

lxix. Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account;

lxx. Frequent requests for travelers cheques Foreign currency drafts or other negotiable instruments to be issued;

lxxi. Large sums being transferred from overseas for making payments;

lxxii. Overpricing Schemes, for instance materials ordered for a purchase are of a poorer quality and lower price than what was specified, but this is not reflected in the negotiated contract;

lxxiii. Any dealing with an agent where the identity of the ultimate beneficiary is undisclosed, contrary to normal procedure for the type of business concerned;

lxxiv. Changes in employee or agent performance (e.g. salesman selling products for cash has remarkable or unexpected increase in performance);

lxxv. Customers who repay problem loan unexpectedly;

lxxvi. Request by a customer for an institution to arrange financing where the source of the customers financial contribution to a deal is unclear particularly where property is involved;

lxxvii. Customer gives power of attorney to a non-relative to conduct large transactions;

lxxviii. Any transaction in which the counterparty to the transaction is unknown;

lxxix. A customer with no acceptable reason for using the firms distant services who could find the same service nearer their home base;

lxxx. Any apparent unnecessary use of an intermediary in the transaction;

lxxxi. Sales invoice totals exceeding the known value of goods;

lxxxii. customer makes frequent or large payments to online payment services;

lxxxiii. customer runs large positive credit card balances;

lxxxiv. customer uses cash advances from a credit card account to purchase money orders or to wire/electronically transfer funds to foreign destinations;

lxxxv. large cash payments for outstanding credit card balances;

lxxxvi. customer makes credit card overpayment and then requests a cash advance;

lxxxvii. customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address;

lxxxviii. customer deposits large endorsed cheques in the name of a third-party;

lxxxix. customer frequently exchanges currencies;

xc. customer acquires significant assets and liquidates them quickly with no explanation;

xci. customer acquires significant assets and encumbers them with security interests that do not make economic sense;

xcii. customer requests movement of funds that are uneconomical; and

xciii. High volume of wire/electronic transfers are made or received through the account

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 receives funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the customer ;
viii. customer requests payment in cash immediately upon receipt of a large funds transfer;

ix. Customer instructs you to transfer funds abroad and to expect an equal incoming transfer.

x. immediately after transferred funds have cleared, the customer moves the funds to another account or to another individual or entity;

xi. customer shows unusual interest in funds transfer systems and questions the limit of what amount can be transferred;

xii. customer transfers funds to another country without changing the currency;

xiii. large incoming wire/electronic transfers from foreign jurisdictions are withdrawn immediately by company principals;

xiv. customer sends frequent wire/electronic transfers to foreign countries, but does not seem to have connection to such countries;

xv. wire/electronic transfers are received from entities having no apparent business connection with customer ;

xvi. size of funds transfers is inconsistent with normal business transactions for that customer ;

xvii. rising volume of remittances exceeds what was expected from the customer when the relationship was established;

xviii. several customer s request transfers either on the same day or over a period of two to three days to the same recipient;

xix. different customer s request transfers that are all paid for by the same customer ;

xx. several customer s requesting transfers share common identifiers, such as family name, address or telephone number;

xxi. several different customer s send transfers that are similar in amounts, sender names, test questions, free message text and destination country;

xxii. a customer sends or receives multiple transfers to or from the same individual;

xxiii. Stated occupation of the customer or the customer 's financial standing is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire/electronic transfers);

xxiv. migrant remittances made outside the usual remittance corridors;

xxv. personal funds sent at a time not associated with salary payments;

xxvi. customer requests transfers to a large number of recipients outside Zambia who do not appear to be family members;

xxvii. customer does not appear to know the recipient to whom he or she is sending the transfer;

xxviii. customer does not appear to know the sender of the transfer from whom the transfer was received;

xxix. beneficiaries of wire/electronic transfers involve a large group of nationals of countries associated with terrorist activity;

xxx. customer makes funds transfers to free trade zones that are not in line with the customer 's business; and

xxxi. 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;

xxxii. Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification;

xxxiii. Foreign exchange transactions that are performed on behalf of a customer by a third party followed by transfers of funds to a location having no apparent business connection with the customer; and

xxxiv. Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel 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. down payment uses a series of money orders or bank drafts from different financial institutions;
vii. customer shows income from "foreign sources" on loan application without providing further details;
viii. customer 's employment documentation lacks important details that would make it difficult for you to contact or locate the employer;

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

x. customer has loans with offshore institutions or companies that are outside the ordinary course of business of the customer ;

xi. customer offers you large deposits or some other form of incentive in return for favourable treatment of loan request;

xii. customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known;

xiii. 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);

xiv. customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction;

xv. 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

xvi. 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 a cheque issued in the same currency to replace the one being cashed;
v. Customer wants cash converted to a cheque and you are not normally involved in issuing cheques;
vi. Customer wants to exchange cash for numerous postal money orders in small amounts for numerous other parties;
vii. Customer enters into transactions with counter parties in locations that are unusual for the customer ;
viii. Customer instructs that funds are to be picked up by a third party on behalf of the payee;
ix. Customer makes large purchases of traveller's cheques not consistent with known travel plans;
x. Customer makes purchases of money orders in large volumes;
xi. Customer requests numerous cheques in small amounts and various names, which total the amount of the exchange;
xii. Customer requests that a cheque or money order be made out to the bearer; and
xiii. Customer requests that a large amount of foreign currency be exchanged to another foreign currency.

It should be noted that none of the above indicators on their own necessarily mean that a customer or any third party is involved in money

laundering. However, in most circumstances a combination of some of the factors above should arouse suspicion.

6.0 HOW TO OBTAIN SUSPICIOUS TRANSACTION FORMS

You may obtain the STR forms by contacting the FIC office using the address provided under paragraph nine (9) of this document or emailing fic@ficzambia.gov.zm. Further, an electronic copy of the STR form can be accessed on the FIC website (www.fic.gov.zm**)**.

7.0 HOW TO COMPLETE A SUSPICIOUS TRANSACTION REPORT

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

8.0 HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO FIC

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

i. On the FIC e-system (applicable only to reporting institutions with electronic link with the FIC);
ii. Authenticated FIC email address provided for under 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.

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