



Financial Intelligence Centre
Republic of Zambia

Suspicious Transactions Reporting Guidelines

Banking Sector

Contents

1.0	Introduction.....	3
2.0	Definition of Key Terms.....	5
3.0	Customer Due Diligence	7
4.0	Anti-Money Laundering/Countering Financing of Terrorism Compliance Programme.....	20
4.1	Elements of an AML/CFT Programme.....	20
4.1.1	A System of Internal Policies, Procedures and Controls	20
4.1.2	Compliance Officer	21
4.1.3	Training.....	22
4.1.4	Independent Audit.....	22
I.	Obligation to Report Suspicious Transactions.....	23
II.	Prohibition against Tipping Off.....	24
III.	Protection of identity of persons and information relating to STRs.....	24
IV.	Protection of entities/persons reporting.....	24
5.0	How to Identify a Suspicious Transaction.....	25
I.	Industry Specific Indicators.....	26
6.0	How to obtain Suspicious Transaction Forms.....	35
7.0	How to complete a Suspicious Transaction Report.....	36
8.0	How to send your Suspicious Transaction Report to Centre.....	36
9.0	Financial Intelligence Centre Contact Details.....	36

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 (LEAs), 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 (Banks) 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 The Banking Sector

The banking sector is supervised by the Bank of Zambia (BOZ) whose mission is to formulate and implement monetary and supervisory policies that achieve and maintain price stability and promotes financial system stability. BOZ is charged with the responsibility of regulating and supervising commercial banks as per provisions under the Banking and Financial Services Act Cap 387 of the Laws of Zambia (BFSa). Furthermore, BOZ is

responsible for executing and implementing the Government's monetary policy and licensing of commercial banks which makes it a supervisory authority for all authorised and licensed financial institutions in Zambia. Commercial banking is provided by local and international banks which offer a wide range of financial services.

The increasing integration of financial systems means that money launderers can now make use of the financial system to hide the proceeds of the illegal activities easily. Launderers are now able to quickly move illicit money between national jurisdictions via the use of the well-established banking sector in Zambia, therefore complicating the task of tracing and confiscating these assets.

Banks in this regard have been identified as the primary focus of money launderers and provide an entry point for laundered money into the financial system. Efforts to combat this scourge are therefore mostly targeted towards banks.

1.2 Scope of the Banking Sector Guidelines

The Banking sector STR guidelines have incorporated essential elements of the Act, relevant FATF-Recommendations, the sound practices of the Basle Committee on Banking Supervision and other international best practices on Anti-Money Laundering and the Combating of the Financing of Terrorism (AML/CFT). 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.

It should be noted however that these 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 the Bank of Zambia. Therefore, banks should also consult with BOZ on any regulatory issues related to the foregoing.

2.0 DEFINITION OF KEY TERMS

Act: Refers to the Financial Intelligence Centre Act No. 46 of 2010.

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.

Bank: The Banking and Financial Services Act No. 25 of 2005 defines a Bank as a company conducting **banking business**

Banking business means any of the following;

- a. the business of receiving deposits from the public including chequing account and current account deposits and the use of such deposits, either in whole or in part, for the account of and at the risk of the person carrying on the business, to make loans, advances or investments;
- b. Providing financial services; and
- c. Any custom, practice or activity prescribed by the bank of Zambia as banking business.

Designated Offence: Means a serious offence as defined in the *Forfeiture of Proceeds of Crime Act, 2010*. The *Forfeiture of Proceeds of Crime Act, 2010* defines a serious offence as an offence for which the maximum penalty prescribed by law is death, or imprisonment for not less than 12 months (the definition is the same as it has been defined in the Act).

Legal Arrangement: As defined in the Act means to express trusts or other similar arrangements.

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. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

Reporting Entity: An institution regulated by a supervisory authority and required to make a suspicious transaction report under the Act. For the purpose of these guidelines, all commercial banks are reporting entities.

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 financing offence or related to all criminal acts that would constitute a predicate offence for money laundering. 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 and other serious offences.

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.

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 Centre 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 and person exercising effective control over the trust and the beneficiaries.
 - f. Reporting entities shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

-
- g. Reporting entities shall conduct ongoing due diligence on the business relationship as stated by the customers above.
 - h. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the financial institution/ customer relationship to ensure that the transactions being conducted are consistent with the reporting entities' knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).
 - i. Reporting entities may rely on an intermediary or other third party to perform the customer identification required pursuant to Section 17 of the Act. Reporting entities relying on third parties have the ultimate responsibility of ensuring that the due diligence and reporting requirements are met in accordance with the Act.
 - j. 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;

Note: in addition to the listed requirements above, reporting entities are further advised to do all other things that may be deemed necessary to verify the documentation submitted by the applicant.

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

Banks are an important mechanism for the disposal of criminal proceeds. The following are some special services and products that provide potential money launderers and terrorist financiers the platform to achieve their objectives:

i. Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank).

Large international banks typically act as correspondents for several other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international transfers of funds, cheque clearing and foreign exchange services.

Correspondent banking is vulnerable to money laundering for two main reasons;

- a. Transactions performed in a correspondent relationship create a situation which permits a financial institution conduct transactions on behalf of other institutions, thereby failing to verify the identities and customer details of the parties involved.
- b. The nature of the large volumes of customer transactions processed making it very difficult to identify suspicious transactions

as the processing financial institution does not have information on the actual parties involved.

ii. Payable Through Accounts (PTAs)

Payable Through Accounts (PTAs) are arrangements available in some correspondent banking relationships permitting the respondents bank customers to conduct their own transactions through the respondents banks correspondent account without needing to clear the transactions through the respondent bank. The transactions services offered also include sending wire transfers, making and withdrawing deposits. With PTAs, customers have the ability to directly control funds at the correspondent bank.

Elements that pose a threat to PTAs money laundering defences include:

- a. PTAs with foreign institutions licensed in offshore financial services sectors with weak or absent bank supervision and weak licensing laws;
- b. PTA arrangements where the corresponded bank regards a respondent bank as its sole customer and fails to apply its CDD policies and procedures to customers of the respondent bank;
- c. PTA arrangements in which sub-account holders have currency deposit and withdrawal privileges;
- d. PTAs used in conjunction with subsidiary, representative or other office of the respondent bank, which may enable a respondent bank to offer the same service as a branch without being subject to supervision.

iii. Concentration (Suspense) Accounts

Internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the

bank, usually on the same day are known as concentration accounts. They can also be referred to settlement, suspense, intraday, sweep or collection accounts. These accounts are usually used to facilitate transactions for private banking, trusts and custody accounts and funds transfers.

Money laundering risks can arise in concentration accounts if the customer-identifying information, such as, transaction and amount and account number, is separated from the financial transaction thereby subjecting the accounts to misuse or being administered improperly.

iv. Private Banking

Private banking provides highly personalised and confidential products and services to exclusive and wealthy clients at fees that are often based on “assets under management”. In most cases, private banking customers are “non-resident aliens” meaning that they are mostly conducting their banking outside the country they originate or reside. Private banking offers a customer the possibility of moving their assets overseas in the names of different corporations established in secrecy havens.

Factors that may contribute to the vulnerability of private banking with regards to money laundering include;

- a. Perceived high profitability;
- b. Intense competition;
- c. Powerful clientele;
- d. The high level of confidentiality associated with private banking;
- e. The close relationship of trust developed between the relationship manager and their clients;

-
- f. Commission based compensation for relationship managers which is at times translated into annual bonuses
 - g. A culture of secrecy and discretion developed by the relationship manager; and
 - h. The relationship managers becoming client advocates to protect their clients.

v. Structuring

Structuring is the designing of transactions to evade triggering a reporting or recordkeeping requirement. It is one of the most common methods of money laundering. In Zambia, it is a crime and maybe reported to the Centre by filling a suspicious transaction report (STR). Usually, individuals engaged in structuring are runners hired by launderers, go from bank to bank depositing cash and purchasing monetary instruments in amounts under the reporting threshold.

In relation to the above mentioned products and services offered by most commercial banks, reporting entities of this nature shall, in addition to performing the normal CDD procedures, take the following measures:

- a. Gather sufficient information about a respondent bank to understand fully the nature of its business and to determine from publicly available information the reputation of the bank and the quality of supervision, including whether or not it has been subject of a money laundering or terrorist financing investigation or regulatory action
- b. Assess the respondent bank's AML/CFT controls and ascertain that the latter are in compliance with FATF standards.

-
- c. Obtain approval from senior management before establishing correspondent relationships.
 - d. Document the respective AML/CFT responsibilities of such a bank.
 - e. Prohibiting direct customer access to concentration accounts
 - f. Prohibiting customers' knowledge of concentration accounts or their ability to direct employees to conduct transactions through concentration accounts

Where a correspondent relationship involves the maintenance of payable through accounts, the financial institution should be satisfied that:

- a. Its customer (the respondent bank or financial institution) has performed the normal CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution; and
- b. The respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

3.4 Non Face-to-Face Identification

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. Banks shall conduct regular monitoring of internet-based business/clients. 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.

3.5 Reliance on Identification by Intermediaries and Third Parties

Banks relying on intermediaries or other third parties which have no outsourcing or agency relationships, business relationships, accounts or transactions between banks for their customers are required to perform some of the elements of the CDD process on the introduced business. The following criteria should also be met:

- i. Immediately obtain from the third party the necessary information concerning certain elements of the CDD process;
- ii. Take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
- iii. Satisfy themselves that the third party is regulated and supervised in accordance with core principles of AML/CFT and has measures in place to comply with the CDD requirements set out in the Guideline; and
- iv. Make sure that adequate CDD provisions are applied to the third party in order to get account information for competent authorities.

The ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

3.6 Large and unusual transactions

Banks shall pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions relative to a relationship; transactions that exceed

prescribe limits, very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity.

Banks are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the Centre.

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 at Management level in accordance with Section 23 (3) of the Act such an officer shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. Each Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme. The Compliance Officer shall have ready access to all the books, records and employees of the reporting entity necessary to fulfil the responsibilities under the Act.

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

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

4.1.3 Training

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

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

4.1.4 Independent Audit

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

Monitoring of AML/CFT Compliance Programme

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

I. Obligation to Report Suspicious Transaction

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

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

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

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

II. Prohibition against Tipping Off

A reporting entity or any director, partner, officer, principal or employee of the reporting entity is not allowed to disclose to any person the contents of the STR Form. Further, the disclosure of any other information from which a person could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made is prohibited.

Any person who contravenes this requirement commits an offence and is liable to a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

III. Protection of Identity of Persons and Information Relating to STRs

A reporting entity is not allowed to disclose any information that identifies, or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction. In light of the foregoing, the disclosure of identity of the above mentioned person is confidential. Section 47 of Act prohibits the disclosure of confidential information. Such disclosure is an offence which may result in a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

IV. Protection of Entities/Persons Reporting

No civil, criminal, administrative or disciplinary proceedings for breach of 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.

5.1. Freezing Orders Issued by the Centre

Pursuant to Section 10(2) of the Act, the Director of the Centre may direct a reporting entity to freeze an account for a period not exceeding ten (10) days in the event that there are reasonable grounds suspecting that a transaction maybe related to money laundering, terrorist financing or any other serious offence. For more details on how to deal with such an order, these are provided for in the Regulations to the Act.

I. Common Predicate Offences

Below are some common predicate offences related to the Banking Sector:

- i. Corruption;
- ii. Tax evasion;
- iii. Fraud
- iv. Counterfeiting,

-
-
- v. Organised crime,

II. The Common Indicators of Money Laundering

The common methods used to launder money through the Banking Sector include the following:

a) General

- 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 traveller'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).

b) Knowledge of reporting or record keeping requirements

- i. customer attempts to convince an employee not to complete any documentation required for the transaction;
- ii. customer makes inquiries that would indicate a desire to avoid reporting;
- iii. customer has unusual knowledge of the law in relation to suspicious transaction reporting;
- iv. customer seems very conversant with money laundering or terrorist financing activity issues;
- v. customer is quick to volunteer that funds are “clean” or “not being laundered”;
- vi. customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds; and
- vii. customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds.

c) Cash Transactions

- i. Customers who frequently seek to exchange large quantities of low denomination notes for those of higher denomination;
- ii. Customer who uses notes in denominations that are unusual for the customer, when the norm in that business is different;
- iii. 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;
- iv. Customer makes cash transactions of consistently rounded off large amounts;
- v. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer ;
- vi. Unusually large cash deposits made by an individual or company whose normal business activities would normally be generated by cheques and other instruments;
- vii. Customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers draft, etc.;

-
- viii. 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;
 - ix. Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer;
 - x. 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);
 - xi. Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area); and
 - xii. Customer has no account but deposits huge cash amounts in exchange for a bank cheque.

d) Bank Accounts

- i. Paying in large third party cheques endorsed in favour of the customer;
- ii. Large cash withdraws from a previously dormant/inactive account or from an account which has just received an unexpected large credit from abroad;
- iii. Customers who decline to provide information that in normal circumstances would make the customer eligible

-
- for credit or for other banking services that would be regarded as valuable;
- iv. Unexplained transfers between multiple accounts with no rationale;
 - v. Customers who wish to maintain a number of trustee accounts which do not appear consistent with the type of business;
 - vi. Activity in accounts inconsistent with what would be expected from declared business;
 - vii. Unusual activity in accounts compared to past transactions;
 - viii. Opening accounts when the customer's address is outside the local service area;
 - ix. Opening accounts with names very close to other established business entities;
 - x. Attempting to open or operating accounts under a false name;
 - xi. Funds being deposited into several accounts, consolidated into one and transferred outside the country;
 - xii. Customer frequently uses many deposit locations outside of the home branch location;
 - xiii. Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers;
 - xiv. Establishment of multiple accounts, some of which appear to remain dormant for extended periods;
 - xv. opening accounts in other people's names;
 - xvi. account with a large number of small cash deposits and a small number of large cash withdrawals;

-
- xvii. activity far exceeds activity projected at the time of opening of the account;
 - xviii. account that was reactivated from inactive or dormant status suddenly sees significant activity;
 - xix. reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed;
 - xx. unexplained transfers between the customer's products and accounts;
 - xxi. multiple deposits are made to a customer's account by third parties;
 - xxii. deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered;
 - xxiii. frequent deposits of bearer instruments (for example, cheques, money orders) in amounts just below a determined threshold;
 - xxiv. unusually large cash deposits by a customer with personal or business links to an area associated with drug trafficking;
 - xxv. regular return of cheques for insufficient funds;
 - xxvi. correspondent accounts being used as "pass-through" points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction; and
 - xxvii. Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.

e) Identity Documents

- i. Customer provides doubtful or vague information;
- ii. Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate;
- iii. Customer refuses to produce personal identification documents;
- iv. Customer only submits copies of personal identification documents;
- v. Customer wants to establish identity using something other than his or her personal identification documents;
- vi. Customer ordinarily delays presenting corporate documents;
- vii. All identification presented is foreign or cannot be checked for some reason;
- viii. All identification documents presented appear new or have recent issue dates; and
- ix. Customer presents different identification document each time a transaction is conducted.

f) Offshore International Activity

- i. Customers introduced by an overseas affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent;

-
- ii. 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;
 - iii. Building up large balances, not consistent with the known turnover of the customers business and subsequent transfer to account(s) held overseas;
 - iv. Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account;
 - v. Frequent requests for travelers cheques, Foreign currency drafts or other negotiable instruments to be issued; and
 - vi. Large sums being transferred from overseas for making payments.

g) Reporting Entities' Employees and Agents

- i. Changes in employees characteristics (e.g. lavish lifestyles);
- ii. Corporate crime against the interest of shareholders and of the public at large;
- iii. 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;
- iv. Any dealing with an agent where the identity of the ultimate beneficiary is undisclosed, contrary to normal procedure for the type of business concerned;
- v. Changes in employee or agent performance (e.g. salesman selling products for cash has remarkable or unexpected increase in performance); and

-
- vi. Admissions or statements by directors, officers or employees to legal practitioners, auditors or accountants of their or their company's involvement in criminal activities.

h) Secured and Unsecured Lending

- i. Customers who repay problem loan unexpectedly; and
- ii. 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.

i) Other Areas

- i. An investor introduced by an overseas affiliate or other investor both of which are based in countries where production of drug trafficking may be prevalent;
- ii. Any transaction in which the counterparty to the transaction is unknown;
- iii. A customer with no acceptable reason for using the firms distant services who could find the same service nearer their home base;
- iv. Any apparent unnecessary use of an intermediary in the transaction; and
- v. Sales invoice totals exceeding the known value of goods.

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 seven (7) 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 50 L, Kudu Road, Kabulonga
P. O. Box 30841
Lusaka
ZAMBIA