Financial Intelligence Centre

Accounting and Audit *Sector*

Reporting Guidelines 2019

Contents

1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) 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 reports to law enforcement agencies and other competent authorities, pursuant to the Financial Intelligence Centre Act No. 46 of 2010 (as amended) ('the Act').

It is the responsibility of the Centre to issue guidelines to Accounting and Audit Firms (as reporting entities) to ensure Accounting and Audit Firms comply accordingly with the provisions of the Act. These Reporting Guidelines have been issued in accordance with section 56 and pursuant to section 29 and 30 of the Act. One of the responsibilities of reporting entities is to file suspicious transaction reports (STRs) and currency transaction reports (CTRs) to the Centre. These Reporting Guidelines replace the STR Guidelines which were issued by the Centre in 2016.

1.1 OVERVIEW OF THE ACCOUNTING AND AUDIT SECTOR

The importance of the role of professional accountants and auditors in ensuring prudent management for planning, controlling as well as decision making in the utilization of financial resources at both national and business level cannot be overly emphasized. It is with the aid of accounting/auditing information that the performance of a country can be evaluated.

Accountants and Auditors can be used to combat predicate offences to money laundering such as fraud and theft as well as to combat money

laundering and terrorist financing. Accountants/Auditors in practice may provide a very wide range of services, to a very diverse range of clients. For example, services may include but not limited to:

i. Audit and assurance services.
ii. ii. Book-keeping and the preparation of annual and periodic accounts.
iii. Tax compliance work, and advice on the legitimate minimisation of tax burdens.
iv. Internal audit and advice on internal control and risk minimisation
v. Insolvency/receiver-managers/bankruptcy related services
vi. Advice on the structuring of transactions, and succession advice
vii. Advice on investments and custody of client money
viii. Forensic accountancy.

On the other hand some of the functions performed by accountants and auditors can be abused by potential Money Launderers/ Financiers of Terrorism and some of those services include:

i. Financial and tax advice – Criminals with a large amount of money to invest may pose as individuals hoping to minimise their tax liabilities or desiring to place assets out of reach in order to avoid future liabilities;

ii. Creation of corporate vehicles or other complex legal arrangements (trusts, for example) – such structures may serve to confuse or disguise the links between the proceeds of a crime and the perpetrator;

iii. Buying or selling of property – Property transfers may serve as the cover for transfers of illegal funds; Performing financial transactions – Sometimes accountants may carry out various financial operations on behalf of the client (e.g. cash deposits or withdrawals on accounts, retail foreign exchange

operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers etc.)

Accountancy and auditing in Zambia are regulated professions and are subjected to regulatory or professional requirements which complement the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) domestic measures. According to the Accountants Act No. 13 of 2008, all accountants and auditors must be registered with the Zambia Institute of Chartered Accountants (ZICA) to practice accountancy in Zambia. ZICA is required to devise AML/CFT policies and procedures for accountants in a way that harmonises with other regulatory or professional requirements in accordance with the provisions under section 36 of the Financial Intelligence Centre Act, No. 46 of 2010.

1.1 Scope of the Guidelines

The purpose of these guidelines is to explain common reporting situations under the Act and assist the Accounting and Audit Firms (sole practitioners, partners/auditors or employed professionals within accounting /audit professional firms) to comply with the Act. The Reporting 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 ZICA for the reporting entities.

2.0 DEFINITION OF KEY TERMS

Accountant: A person qualified in the theory and practice of accountancy, an auditor, tax consultant and tax adviser and registered under then Accountants Act No 13 of 2008 and "accountancy" shall be construed accordingly.

Auditor: A person holding a practicing certificate, or a firm registered under the Accountants Act No. 13 of 2008 and appointed to perform any auditing functions.

Beneficial Owner: means an individual- (a) who owns or effectively controls a client of a reporting entity, including the individual on whose behalf a transaction is conducted; or (b) who exercises effective control over a legal person or trust.

Client: A customer of an accountant or firm of accountant(s) registered under the Accountants Act No 13 of 2008.

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) standards.

Money Laundering: Any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. This definition is in line with how ML has been defined under the Prohibition and Prevention of Money Laundering Act No. 14 of 2001, as amended by Act No.44 of 2010.

Politically Exposed Persons:

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, 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.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, 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.

Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Proliferation: Means an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services with the intention that the funds or financial services should be used or knowing that they are to be used in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, including both technologies and dual use of goods used for non-legitimate purpose.

Reporting Entity: An institution regulated by a supervisory authority and required to make a suspicious transaction report under the Act. Examples of Accounting and Audit Firms include institutions supervised by the Zambia Institute of Chartered Accountants established under the Accountants Act, 2008.

Supervisory Authority: For the purpose of these Guidelines, for the purpose of these guidelines, a Supervisory Authority refers to ZICA with mandate of providing accountability in the quality and service of the accounting profession in Zambia.

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

Terrorist Financing: Terrorist financing offences extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist.

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 always requires reporting entities to institute measures to ensure effective CDD. Reporting Entities shall undertake CDD 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. There is a suspicion of money laundering or terrorist financing
iv. 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 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's relationship with the customer 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 following the termination of the business relationship or after the date of the occasional transaction..

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). 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.

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: -

3.2.1 Enhanced CDD

Enhanced due diligence 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. Seeking additional information beyond the minimum requirements under the law to substantiate the customer's identity or the beneficial ownership of an entity and

i 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 non-face-to-face products, increasingly non-face-to-face transactions are being conducted by reporting entities without the need for the customer to visit the reporting entity's branch.

a. Due to possible false identities and impersonations that can arise with non-face-to face transactions, it is important to ensure that the customer 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 customer is requiring third party payments.

b. Procedures to identify and authenticate the customer must 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. Accounting and Audit firms 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. A risk-based Compliance Programme entails that a reporting entity should identify its ML/TF risks by conducting an institutional ML/TF risk assessment and treatment of the risks identified should be on a risk sensitive basis. This means that clients, business

transactions, products or activities that pose the highest risk should be given more attention in terms of monitoring and treatment in order to mitigate the highest risks.

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

Section 23 of the FIC Act, No. 46 of 2010 (as amended) requires a reporting entity to designate a Compliance Officer to be responsible for the implementation of the Act. The Compliance Officer should be at Management Level and should have more than two years experience in regulatory compliance.

The Compliance Officer shall be responsible for managing the AML/CFT matters including filing of STRs and CTRs to the Centre. The 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 not 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. Coordinating 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 him 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 TF techniques, Proliferation Financing 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 specific needs and functions of the reporting entity including targeted training. Upon the request of the reporting entity, the Centre can provide training to the employees of the reporting entity based on the training needs.

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.

The audit can be undertaken by internal audit or external audit as long as they are not part of the entity's AML/CFT day-to-day functions and they should have the necessary skills and competence to conduct the audit.

4.2 MONITORING OF AML/CFT COMPLIANCE PROGRAMME

The Financial Intelligence Centre will from time to time undertake on-site and off-site inspections of reporting entities to monitor Compliance with the FIC Act.

4.3 OBLIGATIONS FOR REPORTING ENTITIES

Reporting entities have a number of obligations under the FIC Act which among others include the following;

4.3.1. 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 transactions that have not been conducted but are suspected to be 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 cases 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 700,000penalty units or to both.

4.3.2 OBLIGATION TO REPORT CURRENCY TRANSACTIONS

As a reporting entity you are required to promptly but not later than 3 working days to submit a currency transaction report of an amount equal to or above the kwacha equivalent of 10,000 USD whether conducted as a single transaction or several transactions that appear to be linked. Please note that this report is not the same as a suspicious transaction report.

4.3.3. 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 or that a suspicious transaction report has been submitted to the Centre. 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.

4.3.4. 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. A person shall not be required to disclose a suspicious transaction report or any information contained in the report or provided in connection with it, or the identity of the person preparing or making such a report or handling the underlying transaction in any judicial proceeding unless the court is satisfied that the disclosure of the information is necessary in the interests of justice. This is provided for under section 34 of the Act.

4.3.5. CONFIDENTIALITY VIOLATIONS

A person who intentionally or negligently discloses to a customer or a third party information contrary to the FIC Act, commits an offence and is liable, upon conviction, to a fine not exceeding 500,000 penalty units or to imprisonment for a period not exceeding five years, or to both.

4.3.6. 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 anyone for submitting a completed STR Form, in good faith, or in compliance with directions given by the Act. This is provided for under section 35 of the FIC 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 clients business, financial history, background and behavior.

5.1. ML/TF indicators for Accounting/Audit Firms

i. Client appears to be living beyond his or her means;

ii. Client has cheques inconsistent with sales (i.e. unusual payments from unlikely sources);

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

iv. Client is uncertain about location of company records;

v. Company carries non-existent or satisfied debt that is continually shown as current on financial statements;

vi. Company has no employees, which is unusual for the type of business;

vii. Company is paying unusual consultant fees to offshore companies;

viii. Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues operating without reasonable explanation of the continued loss;

ix. Company shareholder loans are not consistent with business activity;

x. Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books;

xi. Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business;

xii. Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry; and

xiii. Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

xiv. Frequent change of external auditors (opinion shopping)

6.0 HOW TO OBTAIN STR AND CTR FORMS

In order for a reporting entity to report an STR or CTR to the FIC, the designated compliance officer should obtain login credentials from the FIC for the FIC online reporting portal.

In exceptional circumstances, reporting entities may obtain the STR forms by contacting the FIC office on the address provided under paragraph nine (9) or accessing soft copy of the STR form on the FIC website at **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. Complete as much information of the STR form as possible. Fields marked with an asterisk (*) are mandatory, except for attempted transactions. Complete form on the online reporting portal using the login credentials given and where not clear on how to complete certain fields please contact the FIC for assistance.

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. FIC online reporting portal

ii. **Only** in exceptional circumstances should the STR be reported via email to FICSTR@fic.gov.zm or hand delivered to designated officials of the Monitoring and Analysis department of the FIC to the address provided below:

9.0 FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS

All the completed reports or any queries should be sent to:

The Director General
Financial Intelligence Centre
Plot 50L, Kudu Road, Kabulonga
P O Box 30481
LUSAKA, ZAMBIA.