Financial Intelligence Centre
Republic of Zambia

Suspicious Transactions Reporting Guidelines

Real estate sector

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 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 Zambia's Real Estate Sector

Zambia's real estate sector has experienced tremendous expansion in the recent years. It has been reported that increased investments from major economies such as China and South Africa, coupled with sustained investment in the mining and agriculture sectors are ensuring that the demand for residential and commercial property which includes industrial property, is on the increase. The capital city of Lusaka for instance has seen steady investment in both the retail and office sector in the last five years.

However, this growth in the real estate sector is not restricted to the capital city. There is likely to be increased interest in the commercial sector on the Copperbelt and North-Western provinces due to the existing absence of structured retail property and as a result of the economic growth registered in other parts of the country. Areas such as the Copperbelt and North-Western provinces still have not been heavily invested into when it comes to retail and office property and Zambia is seeing these as two key growth areas.

The demand for real estate is being driven by individuals, commercial entities and government. This makes the real estate sector vulnerable to a number of criminal activities such as fraud, forgery, tax evasion, embezzlement, terrorist financing and other serious offences which are predicate offences to Money Laundering (ML).

According to section 5 of the Estate Agents Act No. 21 of 2000, estate agents are regulated by the *Zambia Institute of Estate Agents whose functions are: -*

a) to promote and regulate the practice and business of estate agents;
b) to promote and maintain best standards and practices in the business of estate agents;
c) to register members of the Institute and persons qualified to be registered as estate agents and to maintain a register for both;
d) to provide continuing education for its members;
e) to regulate the professional conduct and discipline of estate agents; and
f) to promote the general interests of estate agents.

1.2 Scope of the Real Estate Sector STR Guidelines

The STRs 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.

These Guidelines are provided as general information only and as such do not represent all the requirements under the law. 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 Supervisory Authorities for the Reporting Entities. Therefore, a Reporting Entity should also consult with its respective Supervisory Authority.

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 a reporting entity 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, 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 (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.

Supervisory Authority: Includes the Registrar of Estate Agents appointed under the Estate Agents Act, 2000.

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.

Real Estate: real estate is defined as ownership and rights to land, purchasing and selling of immovable property (residential, commercial, and agricultural), leasing and management and valuation of immovable property.

Estate Agent: A person who is registered as an estate Agent under section (12) (3) or section (13) of the Estate Agents Act No. 21 of 2000.

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 conduct business transaction with an anonymous person whether natural of body corporate, or any institution whose identity is not ascertained.

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. 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 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 applicable.

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).

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:-

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.

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

An AML/CFT compliance 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 FIC 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 programme 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.

I. Obligation to Report Suspicious Transaction

Whenever you process 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, you 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 of up to seven years or seven hundred penalty points or to both.

II. Prohibition against Tipping Off

A reporting entity is not allowed to disclose to any person the contents of the STR Form as well as that a report has been made or any other information from which the person whom the information is disclosed could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made. 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 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. 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 a jail sentence upon conviction or to both.

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.

I. Common Predicate Offences

Below are some common predicate offences related to the Real Estate Sector:

i. Forgery – manipulation of records;
ii. Fraud;
iii. Tax evasion;
iv. Embezzlement; and

v. Other offences relating to the governing law of the sector.

II. The Common methods used to launder money

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

i. Purchase of real estate using large cash amounts;

ii. Use of third parties, gate keepers (lawyers/real estate agents)/fronts to purchase and lease immovable property;

iii. Buying of building material which can be purchased in cash or through successive deposits in the accounts of the suppliers of construction materials;

iv. Acquiring of mortgage bonds and settlement of the bonds using large cash amounts;

v. Purposefully defaulting payment of mortgage instalments and later settling them off using lump sum amounts (cash, wire transfers, using other property, series of transactions);

vi. Foreign PEPs and nationals, investing in real estate;

vii. Foreign nationals using locals to acquire real estate;

viii. The use of corporate structures through buying and/or owning companies or corporations which own real estate;

ix. Use of third parties (minors, spouses, other family members, companies, trusts etc.) to register real estate, mainly for tax evasion; and

x. The use of unregistered real estate agents, who are not accountable to the regulators.

III. Industry-Specific Indicators

The indicators for detecting suspicious transactions in the Real Estate sector can be categorized as follows:

Unusual Possession

i. Customer purchases property in someone else's name such as an associate or a relative (other than a spouse);
ii. Customer does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts;
iii. Customer inadequately explains the last minute substitution of the purchasing party's name;

Unusual Financing

iv. Customer arrives at a real estate closing with a significant amount of cash;
v. Customer negotiates a purchase for the market value or above the asked price, but requests that a lower value be recorded on documents, paying the difference "under the table";
vi. Customer pays initial deposit with a cheque from a third party, other than a spouse or a parent;
vii. Customer pays substantial down payment in cash and balance is financed by an unusual source (for example a third party or private lender) or offshore bank;
viii. Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction;
ix. Transactions in which the party asks for the payment to be divided into smaller parts with a short interval between them;

x. Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments;

Unusual Transactions

xi. Customer purchases personal use property through his or her company when this type of transaction is inconsistent with the ordinary business practice of the Customer;

xii. Customer purchases multiple properties in a short time period, and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property;

xiii. Customer insists on providing signature on documents by fax only;

xiv. Customer over justifies or over explains the purchase;

xv. Customer's home or business telephone or mobile number has been disconnected or there is no such number;

xvi. Customer wants to build a luxury house in non-prime locations;

xvii. Customer exhibits unusual concerns regarding the firm's compliance with government reporting requirements and the firm's anti-money laundering policies;

xviii. Customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;

xix. Customer persists in representing his financial situation in a way that is unrealistic or that could not be supported by documents;

xx. Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases;

xxi. A transaction involving legal entities, when there does not seem to be any relationship between the transaction and the

activity carried out by the buying company, or when the company has no business activity;

xxii. Transactions in which the parties show a strong interest in completing the transaction quickly, without there being good cause;

xxiii. Transactions in which the parties are foreign or non-resident for tax purposes and their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying);

xxiv. Transactions which are not completed in seeming disregard of a contract clause penalizing the buyer with loss of the deposit if the sale does not go ahead;

xxv. Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics; and

xxvi. Transaction is completely anonymous–transaction conducted by lawyer–all deposit cheques drawn on lawyer's trust account. The party is reluctant to produce power of attorney when acting for non-resident person.

xxvii. Customer sells property below market value with an additional "under the table" payment;

xxviii. Customer purchases property without inspecting it;

xxix. Customer is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided;

xxx. Customer buys back a property that he or she recently sold;

xxxi. Frequent change of ownership of same property, particularly between related or acquainted parties; and

xxxii. Property is re-sold shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.

6.0 HOW TO OBTAIN SUSPICIOUS TRANSACTION FORMS

You may obtain the STR forms by contacting the FIC office using the address provided under 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 paragraph 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 premises.

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 30481
Lusaka
ZAMBIA