



Financial Intelligence Centre
Republic of Zambia

Suspicious Transactions Reporting Guidelines

***Patents and Companies
Registration Agency
(PACRA)***

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.....	11
4.1	Elements of an AML/CFT Programme.....	12
4.1.1	A System of Internal Policies, Procedures and Controls	12
4.1.2	Compliance Officer	12
4.1.3	Training.....	13
4.1.4	Independent Audit.....	14
I.	Obligation to Report Suspicious Transactions.....	14
II.	Prohibition against Tipping Off.....	15
III.	Protection of identity of persons and information relating to STRs.....	15
IV.	Protection of entities/persons reporting.....	16
5.0	How to Identify a Suspicious Transaction.....	16
I.	Industry Specific Indicators.....	16
6.0	How to obtain Suspicious Transaction Forms.....	19
7.0	How to complete a Suspicious Transaction Report.....	19
8.0	How to send your Suspicious Transaction Report to Centre.....	19
9.0	Financial Intelligence Centre Contact Details.....	19

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 and supervisory authorities, 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 ensure that Patents and Companies Registration Agency (PACRA) comply accordingly with the provisions of the Act.

The purpose of these guidelines is to explain common reporting situations under the Financial Intelligence Centre Act and assist PACRA to comply with the Act. These Guidelines are provided as general information only and as such do not represent all the requirements under the law.

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 supervisory authorities is to disclose to the Centre 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 Patents and Companies Registration Agency (PACRA)

The Patents and Companies Registration Agency (PACRA) is an - autonomous statutory body under the Ministry of Commerce, Trade and

Industry in Zambia. Its principal functions are to operate a legal system for registration and protection of commercial and industrial property and to serve as a legal depository of the information tendered for registration.

One of the critical roles of PACRA is to promote the establishment and maintenance of a computerized information centre for the publicity of company transactions, financial positions and the dissemination of technical information contained in patent documents to potential and actual users.

In section 2 of the Act, PACRA is designated as a supervisory authority. One of the responsibilities of the supervisory authority is to disclose to the Centre information bordering on Money Laundering, Terrorist Financing and other serious crime as they conduct day to day activities.

1.2 Establishing the Beneficial Owners of Companies

PACRA should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information) that are registered in the country. PACRA will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors. In addition, among other checks PACRA should require companies to hold up-to-date information on the companies' beneficial ownership.

1.3 Scope of the PACRA STR Guidelines

The PACRA guidelines have incorporated essential elements of the Act, relevant FATF-Recommendations and other international best practices on AML/CFT regime. These guidelines cover among others the following key

areas of AML/CFT policy; Customer due diligence, the AML/CFT Compliance programme; monitoring and responding to suspicious transactions.

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

2.0 DEFINITION OF KEY TERMS

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

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

Money Laundering: Under The *Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010*, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious

offence as defined in the *Forfeiture of Proceeds of Crime Act, 2010*. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation.

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

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

Reporting Entity: “an institution regulated by a Supervisory Authority and required to make a suspicious transaction report under the Act.

Supervisory Authority: For the purpose of these guidelines, Supervisory Authority refers to the Registrar appointed under the PACRA Act, 2010.

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 business entities.

PACRA may undertake measures when:

- i. Establishing a business relationship with a customer or business entity
- ii. There is a suspicion of money laundering or terrorist financing
- iii. There are doubts about the veracity or adequacy of previously obtained customer identification data.

3.1 Customer Due Diligence Procedures

- a. PACRA shall identify its 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, PACRA 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. PACRA 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. PACRA 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, PACRA shall take reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.
- e. PACRA 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. PACRA shall obtain information on the purpose and intended nature of the business relationship of their customers.
 - g. PACRA 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 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. PACRA 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 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

PACRA need to exercise enhanced identification, verification and ongoing due diligence procedures with respect to high risk customers. 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. PACRA 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 PACRA to identify customers whose activities may pose a high risk of money laundering and financing of terrorism 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 or shares that a customer/business 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. 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 of a given transaction.

PACRA 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 PACRA and the customer or beneficial-owner is subsequently found to be or becomes a PEP, PACRA shall obtain senior management approval in order to continue the business relationship. PACRA 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.

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 PACRA'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 PACRA may encounter.

4.1. Elements of an AML/CFT Programme

4.1.1 A System of Internal Policies, Procedures and Controls

PACRA 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. PACRA should 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

PACRA should designate a Compliance Officer at Management who shall receive suspicious or unusual transaction reports from persons handling transactions within Agency. 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 records of the entities 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 PACRA's 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. PACRA 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

PACRA should have written AML/CFT Compliance programmes that include training. Ongoing employee training programs should be in place 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 PACRA

4.1.4 Independent Audit

Putting your AML/CFT Compliance programme in place is not enough. The programme must be monitored and evaluated. Therefore, PACRA is 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 PACRA to monitor how the AML/CFT Compliance programmes are being implemented.

I. Obligation to Report Suspicious Transactions

Whenever PACRA 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, PACRA 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 PACRA 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

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

Any person who contravenes this requirement commits an offence and is liable to a fine of up to 500,000 penalty units or to imprisonment for a period not exceeding five years, or to both.

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

A reporting entity is not allowed to disclose any information that identifies, or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction. In light of the foregoing, the disclosure of identity of the above mentioned person is

confidential. Section 47 of Act prohibits the disclosure of confidential information. Such disclosure is an offence which may result in a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

IV. Protection of Entities/Persons Reporting

No civil, criminal, administrative or disciplinary proceedings for breach of professional secrecy 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 Possible Money Laundering and Terrorist Financing Indicators under PACRA

- i. Customer admits or makes statements about involvement in criminal activities;

-
- ii. Customer insisting to register or incorporating a well-known company name not registered in Zambia without authorization from the country of origin;
 - iii. Customer insisting on registering or incorporating a similar or the same company name already registered in Zambia;
 - iv. Customer frequently changing directors or shareholders;
 - v. Customer frequently changing the registered office in an apparent attempt to avoid detection;
 - vi. Customer insisting that a transaction be done quickly in contravention of the period stipulated by laws e.g. for Company Closure – 3 Months or for registration of a trade mark – Minimum period 3 Months;
 - vii. Inconsistencies appearing in the customer's documents
 - viii. Customer obtaining the certificate by fraud;
 - ix. Customer deliberately or negligently submitting false information or statements;
 - x. Customer carrying on business that contravenes this Act or any other written law;
 - xi. Customer makes, signs or utters a false statement or declaration in support of an application or forges, defaces or alters a certificate;
 - xii. Customer knowingly or recklessly gives false or incomplete information for the purpose of obtaining a certificate;
 - xiii. A person who, not being a body corporate, trades or carries on business in Zambia under a name or title which includes the word "incorporation", "corporation" or "limited";
 - xiv. A Customer carrying on business under a business name which does not consist of the true surname of the individual without registering it with PACRA
 - xv. Customer offering money, gratuities or unusual favor for the provision of services that may appear unusual or suspicious;

-
- xvi. A new or prospective customer is known to you as having a questionable legal reputation or criminal background;
 - xvii. Customer attempts to convince an employee not to complete any documentation required for the transaction;
 - xviii. Customer attempts to convince an employee to destroy or hide records, files and documentation from the company registry;
 - xix. Customer attempts to convince an employee to back date the stamp;
 - xx. Customer attempting to register a company and operating a business under a false name, nationality, or NRC number;
 - xxi. Making payment to the agency by cheque on an account with insufficient fund;
 - xxii. Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;
 - xxiii. Third party purchases of shares in other names;
 - xxiv. Customer does not want to put his or her name on any document that would connect him or her with the company in question or uses different names
 - xxv. Transactions in which the parties show a strong interest in completing the transaction quickly, without there being a good cause;
 - xxvi. Customer wants to use foreign companies but does not seem to have a legitimate, legal or commercial reason for doing so;
 - xxvii. Customer wishes to form or purchase a company with a corporate objective that is irrelevant to the customer 's normal profession or activities without a reasonable explanation;
 - xxviii. Customer is uncertain about location of company records

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 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 50L, Kudu Road, Kabulonga
P O Box 30481
Lusaka
ZAMBIA

