Financial Intelligence Centre
Republic of Zambia

SUSPICIOUS TRANSACTIONS REPORTING GUIDELINES

Casino 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 (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 (Casinos and Gaming) to comply with the Act.

These Suspicious Transaction Reports (STRs) Guidelines have been issued in accordance with section 56 and pursuant to section 29 of the Act. One of the cardinal responsibilities of reporting entities is to submit a suspicious transaction report where there is suspicion that a transaction may arise from the commission of a crime or may be linked to the financing of terrorism.

1.1 Overview of the Casino Sector

Zambia is a liberalized economy where economic effects have been profound for the country and for both public and foreign investors. One of the private sectors that has shown significant growth in the recent past is the Casino industry which is regulated by the Licensing Committee established under Section 9 of the Tourism and Hospitality Act No. 23 of 2009.

The Centre is aware that Casinos are by definition non-financial institutions. As part of the operation, Casinos offer gaming for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering and terrorist financing. The Centre is cognizant that Casinos in Zambia conduct financial activities similar to financial institutions including but not limited to: accepting funds on account; debit card cashing facilities, cheque cashing; safety deposit boxes. In many cases these financial services are available 24 hours a day. It is this routine exchange of cash for casino chips or plaques and certified cheques, as well as the provision of electronic transactions to and from casino deposit accounts and the movement of funds in and out of the financial sector, which makes Casinos an attractive target for those attempting to launder money and financing terrorism.

1.2 Scope of the Casino Guidelines

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

The STR Guidelines are provided as general information only and as such do not represent all the requirements under the law or the obligations imposed by the Licensing Committee. 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 Supervisory Authority for the Casinos. Therefore, Casinos are advised to also consult with their Supervisory Authority concerning the foregoing.

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.

Casino: As defined in the Tourism and Hospitality Act No 23 of 2007, o means 'any premises kept and managed for gaming'

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.

Gaming: As defined in the Tourism and Hospitality Act No 23 of 2007, means 'the playing of a game of chance for winnings in Money or Money's worth'

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.

Reporting Entity: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report on suspected Money Laundering, Terrorist Financing an other serious offences under the Act. In accordance with Section 2 of the Act, Casinos are designated as Reporting Entities.

Supervisory Authority: For the purpose of these Guidelines, supervisory authority refers to Licensing Committee established under Section 9 of the Tourism and Hospitality Act No 23 of 2007 and designated as such under section 2 of the Act.

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. Establishing a business relationship with or conducting a business transaction 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 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 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 higher-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 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 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 (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 within its organisation 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 as well as a point-of-contact for all employees on issues relating to money laundering and terrorist financing. Every reporting entity shall ensure that the Compliance Officer has access to other information that may be of assistance to the anti-money laundering reporting officer in consideration of a suspicious or unusual transaction.

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

4.1.3 Training

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

4.1.4 Independent Audit

Putting your AML/CFT Compliance programme in place is not enough. The programme must be monitored and evaluated.

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

Monitoring of AML/CFT Compliance programme

The Financial Intelligence Centre will from time to time undertake on 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 IN THE CASINO SECTOR

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. Specific Money Laundering/Terrorist Financing Indicators in the Casino Sector

As Casinos and Personnel working in your entities, there is need to note that there are numerous indicators which may assist you to identify potential money laundering or terrorism financing activities. Although the existence

of a single indicator does not necessarily indicate illicit activity, it should encourage further monitoring and examination.

In most cases, it is the existence of multiple indicators which raises a reporting entity's suspicion of potential criminal activity, and informs their response to the situation. Directors and Senior Management of Casinos should include these money laundering/terrorism financing indicators in staff training and encourage their staff to use these indicators when describing suspicious behaviours for inclusion in suspicious matter reports submitted to the Centre.

ML/TF indicators for Casino Sector

The list below features some of the major indicators of money laundering and terrorist financing in the Casino Sector and should be treated as a non-exhaustive guide:

i. Any casino transaction where an individual receives payment in casino cheques made out to third parties or without a specified payee;
ii. Customer requests a winnings cheque in a third party's name;
iii. Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party;
iv. Multiple cheques being requested or drawn on account;
v. High volume of transactions within a short period;
vi. Multiple chip cash outs on the same day;
vii. Chip cash out is same/similar to chip purchase;
viii. Requests for credit transfers to other casinos;
ix. Customer attempts to avoid the filing of a report for cash by breaking up the transaction;
x. Customer requests cheques that are not for gaming winnings;
xi. Customer enquires about opening an account with the casino and the ability to transfer the funds to other locations when you do not know the customer as a regular, frequent or large volume player;
xii. Customers claiming a high level of gaming machine payouts;
xiii. Supposed winnings do not correspond with recorded winnings;

xiv. Dramatic or rapid increase in size and frequency of transactions for regular account holder;
xv. Detection of chips brought into the casino;
xvi. Customer purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque;
xvii. Customer in possession of large amounts of currency or bills;
xviii. Customer be friending/attempting to befriend casino employees;
xix. Customer puts money into slot machines and claims accumulated credits as a jackpot win;
xx. Customer exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques;
xxi. Customer is known to use multiple names to conduct an activity;
xxii. Customer requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is no effective anti-money-laundering system;
xxiii. Inserting funds into gaming machines and immediately claiming those funds as credits;
xxiv. Customer claiming gaming machine credits/payouts with no jackpot.
xxv. Accumulating gaming credits with minimal play;
xxvi. Customer's intention to win is absent or secondary;
xxvii. Two or more customers frequently wagering against one another on even-money games;
xxviii. Purchasing and cashing out casino chips with little or no gaming activity;
xxix. Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque;
xxx. Use of third parties to purchase casino chips;
xxxi. Use of credit cards to purchase casino chips;
xxxii. Customer due diligence challenges, e.g. refusals, false documents,
xxxiii. Customer purchases chips and leaves casino shortly after;
xxxiv. Large chip purchases;
xxxv. Frequent purchase of casino gift certificates;
xxxvi. Unexplained income inconsistent with financial situation/customer profile.

6.0 HOW TO OBTAIN SUSPICIOUS TRANSACTION FORMS

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

7.0 HOW TO COMPLETE A SUSPICIOUS TRANSACTION REPORT

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

8.0 HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO FIC

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

i. On the FIC e-system (applicable only to reporting institutions with electronic link with the FIC);
ii. Authenticated FIC email address provided for under six (6) of this document;
iii. Registered courier service providers using the address provided for in paragraph nine (9) below; and
iv. To be hand delivered to designated officials of the Monitoring and Analysis department of the Centre 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